



INSTYTUT SPORTU
PAŃSTWOWY INSTYTUT BADAWCZY

Dane osobowe w sporcie

— PRAKTYCZNY PORADNIK —

Monika Trzcńska
Anna Kwiecień
Katarzyna Siemion
Mariusz Andrzejewski



Ministerstwo
Sportu i Turystyki

Dofinansowano ze środków budżetu państwa z części,
której dysponentem jest Minister Sportu i Turystyki.

Autorzy poradnika:

Monika Trzcińska (część I rozdziały 1–15, część II rozdziały 1–3)

Anna Kwiecień (część I rozdziały 18–20, część II rozdziały 6, 7, 10)

dr Katarzyna Siemion (część I rozdziały 1, 15–17, część II rozdziały 8, 9)

Mariusz Andrzejewski (część I rozdział 1, część II rozdziały 2, 4, 5)

Koordynator projektu:

Aneta Lemiesz

Publikacja wydana przez Instytut Sportu – Państwowy Instytut Badawczy w ramach projektu Akademia Zarządzania Sportem dzięki dofinansowaniu ze środków budżetu państwa z części, której dysponentem jest Minister Sportu i Turystyki

Redakcja i korekta: Agata Mościcka / biały-ogród.pl

Projekt makiety i opracowanie graficzne: Agata Mościcka / biały-ogród.pl

(wykorzystane zdjęcia pochodzą z serwisu Freepik)

Projekt okładki: Instytut Sportu - Państwowy Instytut Badawczy

© Copyright by Instytut Sportu – Państwowy Instytut Badawczy, 2025

ISBN 978-83-949509-5-8

Druk i oprawa:

PHU Olejnik Piotr Olejnik

01-318 Warszawa

ul. Eugeniusza Szwanowskiego 2/3

AUTORZY

MONIKA TRZCIŃSKA

radczyni prawna, specjalizuje się w doradztwie dotyczącym prawnych aspektów tworzenia oraz funkcjonowania w zakresie obejmującym m.in. ochronę danych osobowych organizacji zaliczanych do III sektora, w tym podmiotów z branży sportowej. Doświadczona trenerka oraz autorka artykułów tematycznie związanych z danymi osobowymi. Konsultantka prawna poradnika *Wizerunek dziecka w internecie. Publikować czy nie*. Żywo zainteresowana i zaangażowana w tematykę prawa do prywatności dzieci, w szczególności w zakresie kwestii związanych z rozpowszechnianiem ich wizerunku. Autorka poradnika *ngo.pl Ochrona danych osobowych w organizacji pozarządowej. Praktycznie o RODO*.

KATARZYNA SIEMION

radczyni prawna, doktor nauk prawnych, adiunkt w Katedrze Prawa Własności Intelektualnej Wydziału Prawa Uniwersytetu w Białymstoku. Członek Rady Naukowej Instytut Sportu – PIB oraz Polskiego Towarzystwa Prawa Sportowego. Autorka kilkunastu publikacji naukowych z zakresu prawa sportowego, prawa własności intelektualnej, prawa ochrony danych osobowych oraz prawa nowych technologii. W swojej praktyce zawodowej zajmuje się głównie ochroną danych osobowych, prawem medycznym oraz prawem sportowym, prowadzi szkolenia z zakresu ochrony danych osobowych.

ANNA KWIECIEŃ

ekspertka ds. ochrony danych osobowych i audytorka wiodąca międzynarodowej normy ISO/IEC 27001. Absolwentka WPiA UŁ (studia podyplomowe „Ochrona danych osobowych”) oraz WDiKS UŁ. Laureatka nagrody „Top Player” Gazeta.pl za realizację projektów w obszarze nowych technologii i e-commerce. Autorka szkoleń i prelegentka konferencji z zakresu ochrony danych oraz systemów zarządzania sztuczną inteligencją (AIMS). Członkini grupy roboczej przy Instytucie Sportu – PIB opracowującej Kodeks RODO dla branży sportowej, oraz uczestniczka FIFA Data Protection Summit. W praktyce zawodowej wspiera organizacje we wdrażaniu rozwiązań zgodnych z RODO, AI Act oraz normą ISO/IEC 42001 (AIMS), łącząc perspektywę prawną i bezpieczeństwa informacji.

MARIUSZ ANDRZEJEWSKI

radca prawny, absolwent prawa oraz dziennikarstwa i komunikacji społecznej. W zakresie swojej praktyki zawodowej specjalizuje się w ochronie danych osobowych oraz szeroko rozumianym prawie nowych technologii. Autor publikacji o tematyce prawniczej, w tym z zakresu ochrony danych osobowych. Posiada wieloletnie doświadczenie w doradztwie prawnym, świadcząc usługi m.in. dla przedsiębiorstw z branży telekomunikacyjnej. Członek Stowarzyszenia Praktyków Ochrony Danych SPOD, Stowarzyszenia Inspektorów Ochrony Danych – SABI oraz Stowarzyszenia ISSA Polska.

SPIS TREŚCI

Część I. Ogólna.....	11
1. Wstęp	13
2. Regulacje prawne	14
3. Definicja danych osobowych.....	16
3.1. Dane zwykłe	17
3.2. Szczególne kategorie danych osobowych.....	18
3.2.1. Dane biometryczne	18
3.2.2. Dane dotyczące zdrowia.....	19
3.3. Dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa	20
4. Zakres stosowania RODO	22
4.1. W jakich przypadkach nie stosujemy RODO?	23
4.2. Terytorialny zakres stosowania RODO	24
5. Role w procesie przetwarzania danych osobowych	26
5.1. Administrator danych	26
5.1.1. Główne obowiązki administratora	27
5.2. Współadministrator	29
5.3. Podmiot przetwarzający	31
5.3.1. Co to jest dalsze powierzenie?	35
5.4. Odniesienie do działalności związków i klubów sportowych	36
5.5. Jak ustalić rolę pełnioną w procesie przetwarzania danych osobowych?	37
5.6. Strona trzecia	38
5.7. Odbiorca danych	39
6. Ogólne zasady przetwarzania danych osobowych	40
6.1. Zasada zgodności z prawem, rzetelności i przejrzystości	41
6.2. Zasada ograniczenia celu	41
6.3. Zasada minimalizacji danych.....	41
6.4. Zasada prawidłowości	42
6.5. Zasada ograniczenia przechowywania	42
6.5.1. Polityka retencji – przyjmować czy nie?	43
6.5.2. Jak ustalić okres retencji danych osobowych?	43
6.6. Zasada integralności i poufności	45

6.7. Zasada rozliczalności	45
6.7.1. Co administrator powinien dokumentować?	45
7. Podstawy prawne przetwarzania danych osobowych	47
7.1. Podstawy przetwarzania danych zwykłych	48
7.1.1. Zgoda osoby, której dane osobowe są przetwarzane (art. 6 ust. 1 lit a RODO)	48
7.1.2. Wykonanie umowy (art. 6 ust. 1 lit b RODO)	50
7.1.3. Wypełnianie obowiązku prawnego (art. 6 ust. 1 lit c RODO)	51
7.1.4. Ochrona żywotnych interesów osoby (art. 6 ust. 1 lit d RODO)	53
7.1.5. Wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit e RODO)	53
7.1.6. Uzasadniony interes administratora lub strony trzeciej (art. 6 ust. 1 lit f RODO)	54
7.2. Podstawy przetwarzania szczególnych kategorii danych osobowych	58
7.2.1. Wyrażna zgoda osoby, której dane osobowe są przetwarzane (art. 9 ust. 2 lit. a RODO)	59
7.2.2. Wypełnianie obowiązków i praw pracodawcy w dziedzinie prawa pracy (art. 9 ust. 2 lit. b RODO)	60
7.2.3. Ochrona żywotnych interesów zawodnika (art. 9 ust. 2 lit. c RODO)	60
7.2.4. Realizacja zadań w interesie publicznym (art. 9 ust. 2 lit. g RODO)	60
7.2.5. Przetwarzanie niezbędne zgodnie z art. 9 ust. 2 lit h RODO	61
8. Proces licencjonowania zawodników, trenerów i sędziów – podstawa prawna przetwarzania danych osobowych	62
8.1. Zgoda	63
8.2. Wypełnianie obowiązku prawnego ciążącego na administratorze	64
8.3. Uzasadniony interes administratora danych osobowych	64
8.4. Wykonywanie zadania realizowanego w interesie publicznym	65
8.5. Zawarcie i realizacja umowy	66
9. Inspektor ochrony danych (IOD)	67
9.1. Kim jest inspektor ochrony danych?	67
9.2. Obowiązek wyznaczenia IOD	67
9.3. Kwalifikacje inspektora ochrony danych	70
9.4. Obowiązki IOD	71
9.5. Jakie obowiązki wobec inspektora ochrony danych ma organizacja?	73
9.6. Jak wyznaczyć i zgłosić inspektora ochrony danych?	74
9.7. Niezależność i konflikt interesów	74
10. Upoważnienie do przetwarzania danych osobowych	76
11. Powierzenie przetwarzania danych osobowych	78
12. Udostępnienie danych osobowych	81
12.1. Jak powinno się odbywać udostępnienie danych osobowych?	83

13. Różnice między powierzeniem a udostępnieniem danych osobowych.....	84
14. Rejestrowanie czynności i kategorii czynności przetwarzania	86
15. Obowiązek informacyjny	88
15.1. Zakres przekazywanych informacji	88
15.2. Wyłączenia spełniania obowiązku informacyjnego	93
15.3. Termin przekazania informacji	96
15.4. Sposób spełniania obowiązku informacyjnego	97
15.5. Aktualizacja obowiązku informacyjnego.....	99
16. Ochrona danych w fazie projektowania i domyślna ochrona danych	100
16.1. Zasada <i>privacy by design</i>	100
16.2. Zasada <i>privacy by default</i>	102
17. Prawa osób, których dane są przetwarzane	105
17.1. Katalog praw osób, których dane są przetwarzane	105
17.1.1. Prawo dostępu do danych osobowych.....	105
17.1.2. Prawo do sprostowania danych.....	109
17.1.3. Prawo do usunięcia danych („prawo do bycia zapomnianym”).....	111
17.1.4. Prawo do ograniczenia przetwarzania.....	114
17.1.5. Prawo do przenoszenia danych.....	116
17.1.6. Prawo do sprzeciwu wobec przetwarzania danych osobowych.....	118
17.1.7. Prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu	120
17.1.8. Prawo do wycofania zgody na przetwarzanie danych osobowych...	122
17.1.9. Prawo do wniesienia skargi do organu nadzorczego	123
18. Bezpieczeństwo danych osobowych oraz naruszenia ochrony danych osobowych	126
18.1. Bezpieczeństwo danych osobowych	126
18.2. Naruszenia ochrony danych osobowych i związane z tym obowiązki administratorów	127
19. Analiza ryzyka	128
19.1. Obowiązek analizy ryzyka	128
19.2. Przeprowadzenie analizy ryzyka – praktyczne działania	129
19.3. Metody analizy ryzyka	130
19.3.1. Metoda ilościowa analizy ryzyka.....	131
19.3.2. Metoda jakościowa analizy ryzyka	132
19.3.3. Metoda ilościowo-jakościowa analizy ryzyka	133
19.4. Plan postępowania z ryzykiem i jego monitorowanie	135
19.5. Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania	136
19.6. Harmonogram prac zarządzania ryzykiem	136

19.7. Podsumowanie	137
20. Ocena skutków dla ochrony danych.....	138

Część II. Szczegółowa143

1. Przetwarzanie danych osobowych w postaci wizerunku	145
1.1. Definicja wizerunku	145
1.2. Regulacje prawne dotyczące wizerunku.....	145
1.3. Ustawa o prawie autorskim i prawach pokrewnych.....	146
1.4. Wizerunek jako dana osobowa	150
1.4.1. Zgoda (art. 6 ust. 1 lit. a RODO).....	151
1.4.2. Prawnie uzasadniony interes administratora danych (art. 6 ust. 1 lit. f RODO).....	151
1.4.3. Realizacja umowy (art. 6 ust. 1 lit b RODO)	152
1.4.4. Realizacja obowiązku prawnego administratora (art. 6 ust. 1 lit c RODO)	153
1.5. Członkowie kadry narodowej i reprezentacji olimpijskiej	153
1.6. Wizerunek w materiale prasowym	154
1.7. Wizerunek osób niepełnoletnich	155
1.8. Forma zgody	157
1.9. Co należy zrobić i o co zadbać, przetwarzając dane osobowe w postaci wizerunku?.....	157
2. Transfer danych poza Europejski Obszar Gospodarczy (EOG)	160
2.1. Przekazanie na podstawie decyzji KE stwierdzającej odpowiedni stopień ochrony (art. 45 RODO).....	162
2.2. Standardowe klauzule ochrony danych osobowych przyjęte przez KE... 164	
2.3. Przetwarzania w oparciu o jeden z wyjątków wskazanych w art. 49 RODO.....	166
2.4. Transfer danych a obowiązek informacyjny	167
2.5. Transfer danych a inne obowiązki wynikające z RODO.....	168
3. Przetwarzanie danych osobowych a standardy ochrony małoletnich	170
3.1. Przetwarzanie danych osobowych w ramach realizacji obowiązku weryfikacji niekaralności personelu	170
3.2. Przetwarzanie danych osobowych w ramach wdrożonych przez organizację standardów ochrony małoletnich	177
3.2.1. Podstawa prawna przetwarzania danych osobowych	178
3.2.2. Zakres przetwarzanych danych osobowych.....	179
3.2.3. Okres przechowywania danych osobowych	179
3.2.4. Obowiązek informacyjny	179
3.2.5. Poufność i integralność danych osobowych	180

4. Przetwarzanie danych osobowych w celach marketingu	182
4.1. Kluczowe pojęcia w zakresie marketingu	183
4.2. Co warto wziąć pod uwagę?	184
4.3. Pojęcie zgody	185
4.4. Formy marketingu bezpośredniego	187
4.5. Obowiązki informacyjne w marketingu bezpośrednim	189
4.6. Możliwość wycofania zgody	189
5. Newsletter	191
5.1. Wysyłanie newslettera jako usługa świadczona drogą elektroniczną	192
5.2. Prawnie uzasadniony interes organizacji sportowej	193
6. Naruszenia ochrony danych osobowych	195
6.1. Ocena ryzyka naruszenia praw lub wolności osób fizycznych w związku z zaistniałym naruszeniem ochrony danych osobowych	196
6.2. Kiedy musimy zawiadomić osoby o naruszeniu ochrony ich danych osobowych?	198
6.3. Jakie informacje musimy przekazać w zawiadomieniu osoby o naruszeniu ochrony danych osobowych?	198
6.4. Zgłoszenie naruszenia ochrony danych osobowych	202
6.5. A co, jeśli nie dysponujemy jeszcze wszystkimi wymaganymi informacjami?	204
6.6. Dokumentowanie naruszeń	205
6.6.1. Co się stanie, jeżeli nie powiadomimy organu nadzorczego o wszystkich naruszeniach podlegających zgłoszeniu?	206
6.6.2. Dobre praktyki w zapobieganiu naruszeniom ochrony danych osobowych	207
7. Odpowiedzialność i sankcje	208
7.1. Odpowiedzialność administracyjna	208
7.2. Odpowiedzialność cywilna	211
7.3. Odpowiedzialność karna	212
8. Organizacja „małej” imprezy sportowej – zaprojektowanie	213
8.1. Zakres zbieranych danych	214
8.2. Regulamin uczestnictwa w imprezie	215
8.3. Podstawa prawna przetwarzania danych osobowych uczestników imprezy	215
8.4. Zapewnienie realizacji praw osób, których dane są przetwarzane	216
8.5. Obowiązek informacyjny	216
8.6. Uregulowanie zasad dostępu do danych osobowych	216
8.7. Upublicznienie danych osobowych	218
8.8. Okres przechowywania danych osobowych	218

9. Przetwarzanie danych osobowych zawodników przez klub sportowy, związek sportowy i polski związek sportowy	219
9.1. Przetwarzanie danych osobowych przez klub sportowy	219
9.1.1. Podstawa prawna przetwarzania danych osobowych zawodników....	219
9.1.2. Zakres przetwarzanych danych osobowych	222
9.1.3. Okres przechowywania danych osobowych	223
9.1.4. Udostępnienie danych osobowych zawodników	224
9.2. Przetwarzanie danych osobowych zawodników przez polskie związki sportowe	225
9.2.1. Podstawy prawne przetwarzania danych osobowych zawodników	225
9.2.2. Zakres przetwarzanych danych osobowych	227
9.2.3. Okres przechowywania danych osobowych	228
9.3. Przetwarzanie danych osobowych przez związki sportowe	228
9.3.1. Podstawa prawna przetwarzania danych osobowych	228
9.3.2. Zakres przetwarzanych danych osobowych	229
9.3.3. Okres przechowywania danych osobowych	230
9.4. Przekazywanie danych osobowych na różnych szczeblach struktur organizacyjnych (klub sportowy – związek sportowy – polski związek sportowy – międzynarodowa federacja sportowa)	230
10. Szczególne kategorie danych osobowych sportowców. Monitoring zawodników. Nowoczesne technologie	232
10.1. Warunki legalnego przetwarzania danych dotyczących zdrowia sportowca	233
10.2. Warunki legalnego przetwarzania danych biometrycznych sportowca	233
10.3. Komu można udostępniać dane osobowe oraz gdzie i jak należy je przechowywać?	234
10.4. Podanie danych osobowych sportowca na doping do informacji publicznej a RODO	235
10.5. Monitoring zawodników. Nowoczesne technologie.....	236



CZĘŚĆ I OGÓLNA

1. WSTĘP

Niniejszy poradnik został wydany przez Instytut Sportu – Państwowy Instytut Badawczy w ramach projektu „Akademia Zarządzania Sportem”, finansowanego ze środków Ministra Sportu i Turystyki przy wsparciu merytorycznym Prezesa Urzędu Ochrony Danych Osobowych. Poradnik powstał we współpracy z niezależnymi ekspertami specjalizującymi się w ochronie danych osobowych, posiadającymi doświadczenie we wspieraniu organizacji sportowych w zagadnieniach dotyczących przetwarzania danych osobowych. Jego celem jest wsparcie przede wszystkim związków sportowych oraz klubów sportowych w zakresie zgodnego z prawem przetwarzania danych osobowych oraz wykonywania obowiązków prawnych nałożonych przez przepisy. Stanowi on pierwszy krok w realizacji postulatów wspólnej inicjatywy Instytutu Sportu – Państwowego Instytutu Badawczego oraz osiemnastu polskich związków sportowych, dotyczącej opracowania branżowego kodeksu postępowania RODO w sporcie. Poradnik ma służyć jako narzędzie wspierające organizacje sportowe w codziennym stosowaniu przepisów o ochronie danych osobowych oraz jako podstawa do dalszych dyskusji i prac nad kodeksem branżowym w przyszłości.

Poradnik koncentruje się na realnych wyzwaniach i typowych procesach przetwarzania danych, z jakimi mierzą się organizacje sportowe w codziennej działalności. Z uwagi na fakt, że wiele organizacji sportowych – zwłaszcza mniejsze kluby – nie posiada dedykowanego specjalistycznego wsparcia w zakresie ochrony danych osobowych, poradnik ma również na celu podniesienie świadomości prawnej, zmniejszenie ryzyka naruszeń bezpieczeństwa ochrony danych osobowych oraz zapewnienie zgodności z obowiązującymi przepisami prawa. Celem niniejszego opracowania jest ponadto zwrócenie uwagi środowiska sportowego na istotność ochrony danych osobowych w codziennej działalności organizacji.

Poradnik nie obejmuje wszystkich możliwych aspektów związanych z przetwarzaniem danych osobowych, jednak stanowi bazę do wdrożenia najistotniejszych wymagań wynikających z właściwego i legalnego prowadzenia tych procesów w sektorze sportowym. Mamy nadzieję, że publikacja stanie się punktem wyjścia do dalszych działań, rozwijania wiedzy oraz budowania dojrzałości organizacyjnej w zakresie ochrony danych osobowych w polskim sporcie.

Zapraszamy do zapoznania się z treścią poradnika.

Autorzy

2. REGULACJE PRAWNE

Podstawową i zdecydowanie najważniejszą regulacją prawną mającą znaczenie dla kwestii związanych z ochroną danych osobowych jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej jako: ogólne rozporządzenie o ochronie danych, RODO).

Uzupełniającym w stosunku do RODO źródłem prawa regulującym powyższe kwestie jest Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej jako: Ustawa o ochronie danych osobowych)¹. Zagadnienia, które zostały w niej uregulowane, stanowią doprecyzowanie regulacji wynikających z RODO. Ustawa o ochronie danych osobowych wprowadza m.in. wyłączenia i ograniczenia stosowania niektórych przepisów RODO. Z punktu widzenia administratorów szczególne znaczenie mogą mieć zapisy dotyczące odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych (art. 92–100 ustawy), zapisy dotyczące trybu postępowania w sprawie naruszenia przepisów o ochronie danych osobowych (art. 60–74 ustawy), zapisy dotyczące przebiegu postępowania kontrolnego, prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych (art. 78–91 ustawy), przepisy dotyczące administracyjnych kar pieniężnych za naruszenie przepisów o ochronie danych osobowych oraz odpowiedzialności karnej (art. 101–108 ustawy). Ustawa o ochronie danych osobowych określa również, które podmioty obowiązane są do wyznaczenia inspektora ochrony danych osobowych oraz tryb zawiadomienia o jego wyznaczeniu (art. 8–11a ustawy).

Dodatkowo należy również pamiętać, że kwestie dotyczące danych osobowych są uregulowane w różnych przepisach sektorowych. Przykładowo z punktu widzenia każdego pracodawcy przetwarzającego dane osobowe swoich pracowników mają znaczenie przepisy Kodeksu pracy². Główne akty prawne mające znaczenie dla organizacji sportowych niestety nie regulują kwestii związanych z przetwarzaniem danych osobowych przez te podmioty. Wyjątek stanowią przepisy ustawy o bezpieczeństwie imprez masowych³ oraz ustawy o zwalczaniu dopingu w sporcie⁴. Niestety

¹ Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781).

² Ustawa z dnia 26 sierpnia 1974 r. – Kodeks pracy (Dz.U. z 2025 r. poz. 277 z późn. zm).

³ Ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz.U. z 2023 r. poz. 616).

⁴ Ustawa z dnia 21 kwietnia 2017 r. o zwalczaniu dopingu w sporcie (Dz.U. z 2022 r. poz. 1258).

ustawa o sporcie⁵ nadal nie zawiera regulacji, które pozwoliłyby rozwiązać wiele wątpliwości dotyczących podstaw prawnych przetwarzania danych osobowych przez polskie związki sportowe w związku z powierzonymi im w drodze ustawy działaniami (m.in. w zakresie wskazanym w art. 13 ust. 1 ustawy). Powoduje to trudności interpretacyjnych, a w praktyce prowadzi do nadmiarowego opierania się na zgodzie, która powinna być używana jako rozwiązanie ostateczne i wyłącznie w przypadku braku innej podstawy legalizującej przetwarzanie. Doprecyzowanie przepisów ustawy o sporcie o kwestie dotyczące przetwarzania danych osobowych znacznie ułatwiłoby polskim związkom sportowym funkcjonowanie, rozjaśniając wątpliwości i zdejmując z organizacji sportowych część odpowiedzialności interpretacyjnej w obszarze stosowania regulacji dotyczących danych osobowych.

Inne źródła informacji pozwalające na dokonywanie interpretacji regulacji prawnych dostępne na stronie internetowej Urzędu Ochrony Danych Osobowych⁶:

- ▶ decyzje wydane przez Prezesa Ochrony Danych Osobowych;
- ▶ wytyczne Europejskiej Rady Ochrony Danych Osobowych (organu, który po 25 maja 2018 r. zastąpił Grupę Roboczą Art. 29, w skrócie EROD) oraz Grupy Roboczej Art. 29 (tj. Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy 95/46/WE);
- ▶ poradniki branżowe wydawane przez Urząd Ochrony Danych Osobowych;
- ▶ „Biuletyn UODO” umożliwiający otrzymywanie drogą mailową informacji związanych z problematyką ochrony danych;
- ▶ jak również orzeczenia krajowych sądów administracyjnych oraz Trybunału Sprawiedliwości UE.

UWAGA!

Przepisy dotyczące ochrony danych osobowych to nie tylko przepisy wynikające z RODO. To cały zbiór regulacji, który może się wzajemnie uzupełniać i doprecyzowywać. Zapewnienie przetwarzania danych osobowych zgodnie z RODO wymaga znajomości nie tylko treści samego rozporządzenia, ale również regulacji krajowych, w tym przepisów branżowych.

⁵ Ustawa z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2024 r. poz. 1488 z późn. zm).

⁶ www.uodo.pl.

3. DEFINICJA DANYCH OSOBOWYCH

ART. 4 PKT 1 RODO. DEFINICJE

Na użytek niniejszego rozporządzenia:

„1) »dane osobowe« oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”.

Powyższe oznacza, że różne informacje na temat danej osoby, jeżeli zostaną ze sobą połączone, mogą doprowadzić do ustalenia jej tożsamości, w związku z czym mogą stanowić dane osobowe. Katalog informacji, które mogą stanowić dane osobowe, jest otwarty. Zakwalifikowanie danej informacji do tego katalogu zależy od tego, czy pozwoli ona na identyfikację osoby (wprost lub pośrednio). Należy pamiętać, że znaczenie może mieć tutaj kontekst przetwarzania danej informacji – w określonych sytuacjach może stanowić ona daną osobową, a w innych nie. Przykładowo nie zawsze samo imię i nazwisko będzie stanowić dane osobowe (np. Jan Kowalski, Krystyna Kwiatkowska). Identyfikacja kogoś, kto ma powszechnie występujące imię i nazwisko, bez dodatkowych informacji o nim, dotyczących np. miejsca zamieszkania, numeru telefonu, numeru PESEL, nie będzie możliwa. Sama ogólna informacja o wadze i wzroście bez przypisania do konkretnego zawodnika nie będzie stanowiła danej osobowej. Z kolei, kiedy połączymy te informacje nawet z samym imieniem zawodnika, ale również np. jego datą urodzenia i nazwą klubu, w którym trenuje, mogą już jednoznacznie wskazać na daną osobę. Przykładem samodzielnej informacji, która jednocześnie uznawana jest za daną osobową, jest numer PESEL.

PRZYKŁAD

Za dane osobowe można uznać zarówno informacje dotyczące sfery prywatnej, jak i zawodowej (np. służbowy adres mailowy imię.nazwisko@firma.pl). Mogą być one pozyskane z różnych źródeł, przy czym fakt pozyskania ich ze źródeł powszechnie dostępnych, np. ze strony internetowej czy z publicznego rejestru, nie oznacza, że informacje te nie są danymi osobowymi. Za dane osobowe należy również uznać informacje dotyczące osoby fizycznej prowadzącej jednoosobową działalność gospodarczą, pobrane z Centralnej Ewidencji Informacji Działalności Gospodarczej. Zdaniem Prezesa Urzędu Ochrony Danych Osobowych za dane osobowe należy uznać numer tablic rejestracyjnych, numer telefonu czy adres IP.

„Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby [...], w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak **koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny**”⁷.

Dane osobowe dzielimy na:

- ▶ dane zwykłe;
- ▶ szczególne kategorie danych;
- ▶ dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa.

3.1. DANE ZWYKŁE

Dane osobowe zwykłe to wszelkie dane, które nie są szczególną kategorią danych ani danymi dotyczącymi wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa. Katalog danych zwykłych jest otwarty. Dane te mogą być przetwarzane na podstawie przesłanek wskazanych w art. 6 RODO (patrz: Podstawy prawne przetwarzania danych osobowych).

⁷ Motyw 26 RODO.

Dane osobowe zwykle to np. imię i nazwisko zawodnika, nazwa klubu, w którym trenuje, numer licencji, waga, wzrost, numer buta, rozmiar koszulki, wizerunek, numer PESEL czy numer dowodu osobistego.

3.2. SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH

ART. 9 RODO. PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH

„1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby”.

Szczególne kategorie danych to dane osobowe, które ze względu na swój wrażliwy charakter objęte są szczególną ochroną. Co do zasady, przetwarzanie tych danych osobowych jest zakazane, chyba że spełniona zostanie jedna z przesłanek określonych w art. 9 RODO (patrz: Podstawy prawne przetwarzania danych osobowych). Katalog przesłanek legalizujących proces przetwarzania szczególnych kategorii danych osobowych jest zamknięty.

3.2.1. DANE BIOMETRYCZNE

ART. 4 RODO. DEFINICJE

Na użytek niniejszego rozporządzenia:

„14) »dane biometryczne« oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne”.

Dane biometryczne oznaczają dane osobowe, które:

- ▶ wynikają ze specjalnego przetwarzania technicznego;
- ▶ dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej;
- ▶ umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby.

Do danych biometrycznych zaliczamy np. wizerunek twarzy, linie papilarne palców, siatkówkę lub tęczówkę oka, kod DNA, sposób poruszania się, głos czy geometrię twarzy.

Dane biometryczne to dane niezmiennie, pozwalające na jednoznaczne rozróżnienie osób fizycznych. Dlatego, jak wskazuje Prezes UODO, ich przetwarzanie dopuszczone jest tylko wyjątkowo na podstawie art. 9 ust. 2 RODO, gdy m.in. pozwala na to przepis bądź osoba, której dane dotyczą, wyraziła na to zgodę.

Przykładowo kwestie dotyczące wykorzystywania danych biometrycznych uregulowane są w Kodeksie pracy, który wskazuje, że pracodawca może przetwarzać dane biometryczne bez zgody pracownika, ale tylko wtedy, gdy jest to niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony⁸.

UWAGA!

Nie każde przetwarzanie wizerunku twarzy oznacza, że dochodzi do przetwarzania szczególnych kategorii danych osobowych. Aby wizerunek został zakwalifikowany jako dana biometryczna, niezbędne jest zastosowanie specjalnej technologii przetwarzania, np. systemu rozpoznawania twarzy. Samo utrwalanie wizerunku na zdjęciu czy nagraniu (np. przy korzystaniu z monitoringu wizyjnego) nie stanowi przetwarzania danych biometrycznych.

3.2.2. DANE DOTYCZĄCE ZDROWIA

ART. 4 RODO. DEFINICJE

Na użytek niniejszego rozporządzenia:

„15) »dane dotyczące zdrowia« oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia”.

⁸ Art. 221b §2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy.

Dane dotyczące zdrowia to informacje pochodzących zarówno z badań laboratoryjnych, jak i lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych. Dane o zdrowiu to wszelkie informacje o chorobach, kontuzjach, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym czy biomedycznym osoby, niezależnie od ich źródła, którym może być np. lekarz⁹.

3.3. DANE OSOBOWE DOTYCZĄCE WYROKÓW SKAZUJĄCYCH ORAZ CZYNÓW ZABRONIONYCH LUB POWIĄZANYCH ŚRODKÓW BEZPIECZEŃSTWA

ART. 10 RODO. PRZETWARZANIE DANYCH OSOBOWYCH DOTYCZĄCYCH WYROKÓW SKAZUJĄCYCH I CZYNÓW ZABRONIONYCH

„Przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych”.

Dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa nie są kwalifikowane jako szczególne kategorie danych osobowych, jednak mogą być przetwarzane jedynie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii albo prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. **W praktyce oznacza to, że dane te mogą być przetwarzane w sytuacji, w której wynika to z określonego przepisu prawa.**

⁹ Motywu 35 RODO.

PRZYKŁAD

Zgodnie z art. 21 ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym¹⁰ „przed nawiązaniem z osobą stosunku pracy lub przed dopuszczeniem osoby do innej działalności związanej z [...] uprawianiem sportu przez małoletnich, na pracodawcy lub innym organizatorze takiej działalności oraz na osobie, z którą ma być nawiązany stosunek pracy lub która ma być dopuszczona do takiej działalności, ciążyą określone obowiązki, w tym m.in. pracodawca lub inny organizator uzyskuje informacje, czy dane takiej osoby są zamieszczone w Rejestrze Sprawców Przestępstw na Tle Seksualnym (RSPTS) oraz osoba przedkłada pracodawcy lub innemu organizatorowi informację z Krajowego Rejestru Karnego w zakresie wskazanym w ustawie”.

Zgodnie z art. 41 ust. 3 pkt 4 ustawy o sporcie „trenerem lub instruktorem sportu w sportach, w których działają polskie związki sportowe, może być osoba, która: [...] nie była skazana prawomocnym wyrokiem za umyślne przestępstwo, o którym mowa w art. 46–50, lub określone w rozdziałach XIX, XXIII, z wyjątkiem art. 192 i art. 193, rozdziałach XXV i XXVI ustawy z dnia 6 czerwca 1997 r. – Kodeks karny”.

Powyższe dane mogą być przetwarzane na podstawie tych samych przesłanek legalizacyjnych co dane zwykłe, czyli zgodnie z art. 6 RODO (patrz: Podstawy prawne przetwarzania danych osobowych). Przesłanką legalizującą przetwarzanie informacji o karalności najczęściej będzie art. 6 ust. 1 lit. c RODO w oparciu o przepis prawa, który nakłada obowiązek przetwarzania zawartych w niej danych (jak w powyżej wskazanych przypadkach). Dopuszczalne jest również przetwarzanie danych na podstawie innych przesłanek wskazanych w art. 6 RODO, ale pod warunkiem, że prawo przewiduje taką możliwość.

Przykładowo dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa mogą być również przetwarzane w ramach postępowań dyscyplinarnych prowadzonych przez polskie związki sportowe. Choć przepisy ustawy o sporcie nie wskazują wprost na taką możliwość, to przetwarzanie wspomnianych danych osobowych będzie możliwe w oparciu art. 13 ust. 1 pkt. 2¹¹ oraz dalej o treść art. 45b ustawy o sporcie, które stanowią umocowanie polskich związków sportowych do działania w tym zakresie. Tym samym jako podstawę przetwarzania danych osobowych można rozważać art. 6 ust. 1 lit. c) RODO (patrz: Podstawy prawne przetwarzania danych osobowych).

¹⁰ Ustawa z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym (Dz. U. z 2024 r. poz. 560)

¹¹ Polski związek sportowy ma wyłączne prawo do ustanawiania i realizacji reguł sportowych, organizacyjnych i dyscyplinarnych we współzawodnictwie sportowym organizowanym przez związek, z wyjątkiem reguł dyscyplinarnych dotyczących dopingu w sporcie.

4. ZAKRES STOSOWANIA RODO

RODO ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych¹². W praktyce oznacza to, że dane osobowe mogą być przetwarzane:

- ▶ całkowicie lub częściowo w sposób **zautomatyzowany**,
- ▶ ręcznie.

W przypadku ręcznego przetwarzania danych osobowych musi być spełniony dodatkowy warunek, tj. dane osobowe muszą stanowić zbiór lub część zbioru danych. Oznacza to, że dane osobowe muszą być uporządkowane według jakiegoś określonego kryterium. Zbiorem danych jest np. zbiór wydanych licencji sędziowskich, akta osobowe pracownika, lista mailingowa odbiorców newslettera, ewidencja korespondencji, rejestr umów-zleceń. Zbioru danych nie stanowią natomiast np. nieustrukturyzowane notatki.

UWAGA!

Zbiór danych powinien być w taki sposób uporządkowany, aby dostęp do konkretnych danych był możliwy w oparciu o zastosowanie określonego kryterium, np. imienia i nazwiska, daty zamieszczenia w zbiorze, adresu zamieszkania. Jednocześnie zbiór danych nie musi być scentralizowany, zdecentralizowany czy rozproszony – funkcjonalnie lub geograficznie.

Zautomatyzowane przetwarzanie danych z kolei to przetwarzanie z użyciem jakiejś technologii, np. systemów informatycznych.

Przetwarzaniem danych osobowych nazywamy operacje lub zestaw operacji dokonywane na danych osobowych lub zestawach danych osobowych, w tym takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub

¹² Art. 2 ust. 1 RODO.

łączenie, ograniczanie, usuwanie lub niszczenie¹³. Powyższe wyliczenie czynności ma charakter przykładowy.

UWAGA!

Przetwarzanie danych osobowych to nie tylko ich gromadzenie. Organizacja przetwarza dane osobowe, kiedy przechowuje zgłoszenia, deklaracje zawodników, kiedy przekazuje dane zawodnika do ubezpieczyciela czy hotelu, kiedy jej reprezentant naciska migawkę aparatu, robiąc zdjęcia podczas zawodów, kiedy wysyła dokumentację dotyczącą zawodnika mailem, kiedy publikuje zdjęcia z eventu sportowego na swoim profilu w mediach społecznościowych, a także kiedy umieszcza w niszczarce formularze z danymi zawodnika, przegląda listę kontaktową akredytowanych dziennikarzy czy udostępnia dane osobowe uczestników danego wydarzenia swojego grantodawcy.

4.1. W JAKICH PRZYPADKACH NIE STOSUJEMY RODO?

RODO nie ma zastosowania do przetwarzania:

- ▶ informacji anonimowych, czyli takich, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną;
- ▶ danych osobowych zanonimizowanych, czyli poddanych anonimizacji w taki sposób, że osób, których te dane dotyczą, w ogóle nie można zidentyfikować;
- ▶ danych osób zmarłych.

UWAGA!

Co istotne, RODO ma zastosowanie do tzw. danych pseudonimizowanych, czyli takich, których nie można przypisać konkretnej osobie bez użycia dodatkowych informacji. Takie dodatkowe informacje muszą być przechowywane osobno. Muszą być też objęte środkami technicznymi i organizacyjnymi umożliwiającymi ich ponowne przypisanie danej osobie. Pseudonimizacja jest procesem odwracalnym i stosowanym przez administratorów jako środek zabezpieczający dane osobowe przed ich potencjalnym naruszeniem. Innym takim środkiem jest np. szyfrowanie danych osobowych.

¹³ Art. 4 pkt 2 RODO.

Stosowanie RODO jest wyłączone w przypadkach przetwarzania danych osobowych przez osobę fizyczną w ramach czynności **o czysto osobistym lub domowym charakterze**¹⁴, czyli takich, które nie mają związku z działalnością zawodową lub handlową.

Powyższe wyłączenie nie będzie miało zastosowania w przypadku działalności prowadzonej przez klub czy związek sportowy. Nie będzie miało również zastosowania do trenerów lub sędziów, jeżeli będą wykonywać swoje obowiązki zawodowe.

PRZYKŁAD

Działalność osobista lub domowa może polegać m.in. na prowadzeniu korespondencji osobistej i przechowywaniu adresów w celu podtrzymywania więzi społecznych. Dotyczy to również aktywności internetowej podejmowanej w ramach takich czynności (motyw 18 Preambuły RODO).

UWAGA!

RODO nie dotyczy przetwarzania danych osobowych osób prawnych. Dane identyfikacyjne czy rejestrowe (nazwa firmy, NIP, REGON, adres siedziby związku sportowego) oraz dane kontaktowe związku (adres mailowy typu biuro@polskizwiazek.pl, ogólny numer telefonu) nie są objęte zakresem RODO. RODO dotyczy wyłącznie osób fizycznych, w tym również tych, które wykonują określone obowiązki służbowe w ramach struktury związku, m.in. pracowników, zleceniobiorców, członków organów, np. członków zarządu, pełnomocników czy prokurentów.

4.2. TERYTORIALNY ZAKRES STOSOWANIA RODO

ART. 3 RODO. TERYTORIALNY ZAKRES STOSOWANIA

„1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

¹⁴ Art. 2 ust. 2 RODO.

2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego”.

RODO ma zastosowanie do przetwarzania danych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii¹⁵. Oznacza to, że z punktu widzenia zakresu stosowania RODO nie ma znaczenia, czy dane osobowe są przetwarzane na terenie UE czy poza nim. Serwery, na których gromadzone są dane osobowe, mogą być położone poza terenem UE, ale jeżeli przetwarzanie danych osobowych będzie związane z działalnością prowadzoną przez podmiot w ramach jednostki organizacyjnej w miejscu, w którym stosuje się prawo UE, to takie przetwarzanie podlega przepisom UE. Jednocześnie, jeżeli powyższe przesłanki będą spełnione, nie będzie miało znaczenia, jakie obywatelstwo ma osoba, której dane osobowe dotyczą, czy jakie jest jej miejsce zamieszkania¹⁶, np. przepisy RODO będą miały zastosowanie w przypadku, gdy zawodnikiem klubu sportowego będzie osoba mająca obywatelstwo państwa, w którym RODO nie obowiązuje.

¹⁵ Art. 3 ust 1 RODO.

¹⁶ Motyw 14 RODO.

5. ROLE W PROCESIE PRZETWARZANIA DANYCH OSOBOWYCH

5.1. ADMINISTRATOR DANYCH

ART. 4 RODO. DEFINICJE

Na użytek niniejszego rozporządzenia:

„7) »administrator« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania”.

Administrator to właściciel danych osobowych, który podejmuje najważniejsze decyzje dotyczące przetwarzania danych osobowych, m.in. czy określone dane przetwarzać, czemu to służy, jakie dane będą gromadzone i przetwarzane, czy zaprzestać przetwarzania danych, jak długo przetwarzać dane albo czy zlecić przetwarzanie komuś innemu. Administrator sprawuje kontrolę nad procesem przetwarzania danych osobowych. W praktyce może się zdarzyć, że administrator nie gromadzi danych samodzielnie (robią to za niego – na jego zlecenie – inne podmioty). Może dojść również do takiej sytuacji, w której administrator nie przetwarza samodzielnie danych osobowych, a nawet nie ma do nich dostępu. Co ważne, status administratora danych wynika z jego faktycznej roli. Znaczenie mają rzeczywiste działania w konkretnej sytuacji. Nie można formalnie wyznaczyć administratora danych osobowych¹⁷. To, co można zrobić, to bazując na określonym stanie faktycznym, ustalić, jaką rolę w procesie przetwarzania danych osobowych pełni konkretny podmiot lub konkretna osoba. Administrator nie może być wyznaczony w drodze postanowień umownych ani na podstawie jednostronnego oświadczenia.

¹⁷ Wytyczne EROD nr 7/2020 dotyczące pojęć administratora oraz podmiotu przetwarzającego zawartych w RODO.

Administrator może natomiast być wyznaczony w określonych przepisach prawnych. Na przykład art. 36h ustawy o sporcie wskazuje, że administratorem danych gromadzonych w ewidencji „Sportowe talenty” jest minister właściwy ds. kultury fizycznej (wyrażna kompetencja prawna). Przepisy prawa mogą również wskazywać konkretne kryteria jego wyznaczenia. Przetwarzanie może być również niezbędne do wykonywania określonego zadania, za które dany podmiot lub osoba są odpowiedzialni zgodnie z obowiązującymi przepisami prawa (dorożumiana kompetencja prawna).

PRZYKŁAD

Administratorem danych osobowych będzie klub sportowy, związek sportowy, polski związek sportowy czy inny podmiot okołosportowy. Administratorem danych osobowych może być trener prowadzący jednoosobową działalność gospodarczą w zakresie procesów przetwarzania danych osobowych realizowanych w ramach tej działalności. Administratorem danych osobowych może być jednostka organizacyjna klubu sportowego, również taka, która nie posiada odrębnej osobowości prawnej, np. oddział spółki lub stowarzyszenia.

UWAGA!

Kto nie jest administratorem danych?

Administratorami danych nie będą organy ww. podmiotów lub osoby wchodzące w skład tych organów, tj. prezes zarządu czy jego poszczególni członkowie, kolegium sędziów, komisja rewizyjna i jej członkowie, udziałowcy w spółkach, członkowie stowarzyszenia, zgromadzenie członków.

5.1.1. GŁÓWNE OBOWIĄZKI ADMINISTRATORA

Wobec osób, których dane dotyczą, m.in.:

- ▶ spełnianie obowiązku informacyjnego wobec osoby, której dane są gromadzone (patrz: Obowiązek informacyjny);
- ▶ zapewnienie możliwości realizacji praw osób, których dane dotyczą (patrz: Prawa osób);
- ▶ zawiadomienie o naruszeniu ochrony danych osoby, której dane dotyczą, jeżeli wiąże się to dla niej z wysokim ryzykiem naruszenia praw i wolności.

Wobec Prezesa Urzędu Ochrony Danych m.in.:

- ▶ zgłoszenie inspektora ochrony danych, jeżeli był powołany (patrz: Inspektor ochrony danych);
- ▶ zgłoszenie wystąpienia naruszenia ochrony danych osobowych (patrz: Naruszenie ochrony danych osobowych).

Obowiązkiem administratora jest również zapewnienie bezpieczeństwa przetwarzanym danym osobowym poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, które pozwolą przetwarzać dane osobowe zgodnie z przepisami prawa, w tym m.in.:

- ▶ przyjęcie odpowiednich polityk ochrony danych osobowych;
- ▶ zawieranie stosownych umów związanych z przetwarzaniem danych osobowych, w szczególności umów powierzenia przetwarzania danych osobowych (patrz: Powierzenia przetwarzania danych osobowych);
- ▶ nadawanie upoważnień do przetwarzania danych osobowych;
- ▶ szkolenie personelu z zakresie zagadnień związanych z przetwarzaniem danych osobowych;
- ▶ stosowanie odpowiednich zabezpieczeń technicznych, takich jak pseudonimizacja czy szyfrowanie.

Inne obowiązki administratora danych osobowych:

- ▶ powołanie inspektora ochrony danych, jeżeli taki obowiązek wynika z przepisu (patrz: Inspektor ochrony danych);
- ▶ dokonywanie oceny ryzyka związanego z przetwarzaniem danych osobowych i jego monitorowanie (patrz: Analiza ryzyka), a także przeprowadzenie oceny skutków dla ochrony danych, jeżeli zachodzi duże prawdopodobieństwo naruszenia praw i wolności osób, których dane są przetwarzane;
- ▶ kierowanie się podstawowymi zasadami dotyczącymi przetwarzania danych osobowych, w tym m.in. zasadą minimalizacji, zasadą adekwatności czy zasadą ograniczonego przechowywania, oraz możliwość wykazania, że ma to miejsce (patrz: Zasady dotyczące przetwarzania danych osobowych);
- ▶ zapewnienie, aby przetwarzanie danych osobowych odbywało się w oparciu o przesłanki legalizujące takie działanie;
- ▶ prowadzenie rejestru czynności przetwarzania danych osobowych (patrz: Rejestr czynności);
- ▶ stosowanie specjalnych środków bezpieczeństwa w przypadku transferu danych osobowych do państw spoza Europejskiego Obszaru Gospodarczego (EOG);
- ▶ zadbanie o stosowanie zasad *privacy by design* i *privacy by default* (patrz: Zasada *privacy by design* i *privacy by default*).

5.2. WSPÓŁADMINISTRATOR

ART. 26 RODO. WSPÓŁADMINISTRATORZY

„1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

2. Uzgodnienia, o których mowa w ust. 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów”.

Współadministrator to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych¹⁸. Abyśmy mieli do czynienia ze współadministrowaniem, konieczny jest zatem udział w przetwarzaniu danych **co najmniej dwóch administratorów**.

Wspólne zarządzanie danymi osobowymi nie wymaga sztywnych zasad dotyczących ustalania celów i metod przetwarzania przez współadministratorów. Wspólne administrowanie danymi może przybierać formę zarówno ścisłej współpracy, jak i tylko częściowego współdziałania.

Jeżeli strony ustalą, że w ramach prowadzonych przez nie działań dochodzi do współadministrowania, to powinny w sposób przejrzysty uzgodnić zakresy swojej odpowiedzialności dotyczącej wykonywania obowiązków wynikających z RODO. Inaczej mówiąc, strony muszą w sposób prosty i transparentny ustalić, kto co robi i za co odpowiada. Wszystkie obowiązki powinny być przydzielone zgodnie z okolicznościami faktycznymi i w sposób zapewniający, aby cały proces wspólnego

¹⁸ Art. 26 RODO.

przetwarzania był w pełni zgodny z RODO. Jak wskazuje EROD obowiązki nie muszą być rozłożone równo, przy podziale należy brać pod uwagę takie czynniki, jak kompetencje danego współadministratora i jego skuteczność w wywiązywaniu się z nałożonych na niego obowiązków. EROD jednocześnie zaleca udokumentowanie istotnych czynników i wewnętrznej analizy przeprowadzonej w celu podzielenia różnych obowiązków. Analiza ta stanowi część dokumentacji zgodnie z zasadą rozliczalności¹⁹.

Uzgodnienia pomiędzy współadministratorami mogą być dokonane w dowolnej formie, jednocześnie EROD zaleca, żeby były dokonane w formie wiążącego dokumentu, takiego jak umowa lub inny akt prawa na mocy prawa krajowego lub unijnego. W praktyce uzgodnienia najczęściej przyjmują formę umowy lub porozumienia. Nie musi to być dokument, który jest zawierany w formie pisemnej, forma elektroniczna lub dokumentowa również będą dopuszczalne, czyli np. skan dokumentu, dokument podpisany przy użyciu podpisów elektronicznych za pośrednictwem takiej platformy, jak Autenti czy Pergamin, czy nawet wymiana uzgodnień drogą mailową. Jednocześnie uzgodnienia nie muszą stanowić odrębnego dokumentu. Może to być część tzw. umowy głównej lub załącznik do niej.

Uzgodnienia dotyczące współadministrowania powinny w szczególności zawierać:

- ▶ ogólne informacje na temat wspólnego przetwarzania, takie jak określenie przedmiotu i celu przetwarzania, rodzaj danych osobowych oraz kategorię osób, których dane dotyczą;
- ▶ postanowienia dotyczące sposobu, w jaki osoby, których dane dotyczą, będą informowane o przetwarzaniu ich danych, w tym kto będzie odpowiedzialny za dostarczanie tych informacji oraz jak będą one dostarczane;
- ▶ postanowienia dotyczące realizacji praw osób, których dane dotyczą (takich jak np. prawo dostępu, sprostowania, usunięcia danych), w tym jak te prawa będą realizowane i kto będzie za to odpowiedzialny;
- ▶ postanowienia dotyczące podziału innych obowiązków wynikających z RODO – dotyczy to zarówno działań operacyjnych, jak i technicznych środków ochrony danych;
- ▶ postanowienia dotyczące zasad powierzenia przetwarzania danych osobowych innym podmiotom;
- ▶ postanowienia dotyczące organizacji kontaktów z osobami, których dane dotyczą, oraz organem nadzoru;
- ▶ postanowienia dotyczące przyjętych przez strony mechanizmów współpracy i komunikacji, które będą stosowane w celu zarządzania przetwarzaniem danych osobowych.

¹⁹ Wytyczne EROD nr 7/2020 dotyczące pojęć administratora oraz podmiotu przetwarzającego zawartych w RODO.

Współadministratorzy mogą tworzyć wspólny punkt kontaktowy dla podmiotów danych. Wyznaczenie takiego wspólnego punktu nie jest obowiązkowe, jednak zalecane przez EROD. Punktem kontaktowym może być jeden z inspektorów ochrony danych, jeżeli został powołany, lub jakikolwiek inny punkt kontaktowy, w którym można uzyskać informacje.

UWAGA

Osoba, której dane osobowe są przetwarzane, nie jest związana warunkami uzgodnień i może wykonywać swoje prawa wynikające z RODO wobec każdego ze współadministratorów. Nie można zobowiązać takiej osoby do kontaktowania się z wyznaczonym punktem lub konkretnie wskazanym administratorem. W praktyce jednak wyznaczenie punktu kontaktowego powoduje, że w przeważającej liczbie przypadków osoby, których dane dotyczą, będą korzystały ze wskazanych im form komunikacji.

Zasadnicza treść uzgodnień jest udostępniana osobom, których dane dotyczą. EROD zaleca, aby zasadnicza treść uzgodnień obejmowała wszystkie elementy informacji przewidziane dla klauzuli informacyjnej, przy czym dla każdego z tych elementów należy określić, który ze współadministratorów jest odpowiedzialny za zapewnienie zgodności z tymi elementami. Zasadnicza treść uzgodnień musi wskazywać punkt kontaktowy, jeżeli został wyznaczony²⁰. W praktyce oznacza to, że obowiązek udostępnienia zasadniczej treści uzgodnień może być wykonany w ramach tzw. obowiązku informacyjnego (poprzez odpowiednie przygotowanie klauzuli informacyjnej) lub np. poprzez zapisy w politykach prywatności publikowanych na stronie internetowej danej organizacji sportowej.

5.3. PODMIOT PRZETWARZAJĄCY

ART. 4 RODO. DEFINICJE

Na użytek niniejszego rozporządzenia:

„8) »podmiot przetwarzający« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora”.

²⁰ *Ibidem*.

Podmiot przetwarzający to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe na rzecz i w imieniu administratora. Podmiot przetwarzający jest to odrębny podmiot w stosunku do administratora, który działa na podstawie umowy zawartej z administratorem i jest zobowiązany do przetwarzania danych zgodnie z jego instrukcjami oraz przepisami prawa dotyczącymi ochrony danych osobowych.

Uprawnienia i obowiązki podmiotu przetwarzającego powinny zostać precyzyjnie wskazane w umowie powierzenia przetwarzania danych osobowych. Wspomniana umowa musi zawierać elementy wymagane przez art. 28 RODO (patrz: **Powierzenie przetwarzania danych osobowych**). Powinna mieć formę pisemną, w tym elektroniczną, co w polskim porządku prawnym oznacza, że może być zawarta w formie pisemnej (podpisana własnoręcznie lub podpisem kwalifikowanym) albo w formie dokumentowej (tj. takiej, w której złożenie oświadczenia woli następuje w postaci dokumentu, w sposób umożliwiającą ustalenie osoby składającej oświadczenie).

UWAGA!

Obowiązek zawarcia umowy dotyczy zarówno administratora, jak i podmiotu przetwarzającego. Brak zawarcia umowy z podmiotem przetwarzającym w wymaganej formie stanowi podstawę do nałożenia na administratora kary finansowej²¹. Taka kara może być również nałożona na podmiot przetwarzający.

Podobnie jak w przypadku pozostałych uczestników procesów przetwarzania danych osobowych, podmiot przetwarzający nie jest podmiotem, który może zostać w jakiś sposób wskazany. Rola podmiotu przetwarzającego wynika z jego działań podejmowanych w ramach określonej sytuacji. Znaczenie ma charakter świadczonych przez niego usług oraz stopień wpływu, jaki ma dany podmiot na cel i sposób przetwarzania danych osobowych. Jak wskazuje EROD, jeżeli usługa nie jest konkretnie ukierunkowana na przetwarzanie danych osobowych lub jeżeli takie przetwarzanie nie stanowi kluczowego elementu usługi, dostawca usług może być w stanie niezależnie określić cele i sposoby takiego przetwarzania, które są wymagane do świadczenia usługi. W takiej sytuacji dostawca usług powinien być postrzegany jako odrębny administrator, a nie jako podmiot przetwarzający²².

²¹ Decyzja PUODO z dnia 16 sierpnia 2022 r., DKN.5131.29.2022.

²² Wytyczne EROD nr 7/2020 dotyczące pojęć administratora oraz podmiotu przetwarzającego zawartych w RODO.

PRZYKŁAD

Przykładami podmiotów przetwarzających dane osobowe są firmy świadczące usługi hostingowe i dostawcy usług chmurowych, przedsiębiorstwa świadczące usługi kadrowe i płacowe, marketingowe, outsourcingowe IT, archiwizacji, ochrony obiektów, w tym monitorowania, niszczenia dokumentów. Podmiotami przetwarzającymi w określonych sytuacjach mogą być np. firmy rekrutujące pracowników, świadczące usługi fotograficzne.

Ważne, żeby pamiętać, że przepisy RODO nakładają również obowiązki na podmiot przetwarzający, który m.in. zobowiązany jest do prowadzenia rejestru wszystkich kategorii czynności przetwarzania danych osobowych (patrz: **Rejestry czynności i kategorii czynności przetwarzania**), wdrożenia odpowiednich środków technicznych i organizacyjnych, w określonych przypadkach powołania inspektora ochrony danych, stosowania przepisów dotyczących transferu danych do państw trzecich, zapewnienia, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy. W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający ma również obowiązek niezwłocznie poinformować administratora o takim naruszeniu. Jednocześnie, jak wskazuje UODO, podmiot przetwarzający nie jest zobowiązany do dokonania oceny ryzyka wynikającego z naruszenia – to administrator powinien przeprowadzić analizę ryzyka w związku z zaistniałym incydem i podjąć decyzję o ewentualnym zgłoszeniu go organowi nadzorczemu oraz zawiadomieniu osób, których dane dotyczą. W gestii podmiotu przetwarzającego pozostaje ustalenie, czy doszło do naruszenia, a jeśli tak – zgłoszenie tego faktu administratorowi²³.

UWAGA!

Podmiot przetwarzający może zostać pociągnięty do odpowiedzialności odszkodowawczej lub ukarany karą finansową w przypadku niedopełnienia nałożonych na niego obowiązków lub w przypadku, kiedy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

²³ „Biuletyn UODO” nr 1/01/2024. Rola podmiotu przetwarzającego w przypadku naruszenia ochrony danych osobowych na gruncie RODO.

Powierzenie przetwarzania danych osobowych następuje najczęściej przy okazji zlecenia podmiotowi zewnętrznemu realizacji określonej usługi. Często wspomniana usługa związana jest z realizacją czynności, które ze względu na ich charakter stanowią czynności przypisane administratorowi (np. prowadzenie księgowości, prowadzenie strony IT, realizacja działań promocyjnych lub marketingowych), jednak z różnych względów nie są przez niego wykonywane. Administrator, zlecając usługi podmiotowi zewnętrznemu, w wielu przypadkach bada jego kompetencje oraz ocenia proponowane warunki cenowe. Kwestia związana z przetwarzaniem danych osobowych bardzo często w praktyce schodzi na plan dalszy i nie jest oceniana na etapie wyboru kontrahenta. Tymczasem zgodnie z przepisami RODO administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO – w tym w zakresie bezpieczeństwa przetwarzania – i zapewniało ochronę praw osób, których dane dotyczą. Oznacza to zatem, że administrator powinien weryfikować usługodawcę nie tylko pod kątem jakości świadczonych przez niego usług, ale w sytuacji, w której taki usługodawca będzie przetwarzał w imieniu tej organizacji dane osobowe, również pod kątem gwarancji wskazanych powyżej.

Aby ocenić, czy gwarancje usługodawcy są wystarczające, administrator powinien wziąć pod uwagę jego:

- ▶ fachową wiedzę (np. wiedzę techniczną w zakresie środków bezpieczeństwa i naruszeń ochrony danych);
- ▶ wiarygodność;
- ▶ posiadane zasoby;
- ▶ reputację²⁴.

Jak wskazuje PUODO, „brak weryfikacji podmiotu przetwarzającego oraz jego gwarancji dla przetwarzania zgodnie z przepisami o ochronie danych osobowych może wiązać się z konsekwencjami dla osób fizycznych, których dane osobowe zostały powierzone podmiotowi przetwarzającemu, np. w postaci utraty danych osobowych. Zatem decyzja, komu administrator ma powierzyć przetwarzanie danych osobowych, nie może być podejmowana bezpodstawnie. Dopiero po zbadaniu kompetencji i adekwatności wybranego podmiotu przetwarzającego administrator może przystąpić do zawarcia stosownej umowy powierzenia”²⁵.

²⁴ Wytyczne EROD nr 7/2020 dotyczące pojęć administratora oraz podmiotu przetwarzającego zawartych w RODO.

²⁵ UODO, *Powierzenie przetwarzania danych trzeba udokumentować*, <https://uodo.gov.pl/pl/138/2485> [dostęp: 4.07.2025].

UWAGA!

Sposób przeprowadzenia weryfikacji może być różny i będzie zależał od konkretnego przypadku. W szczególności znaczenie będzie miał rodzaj przetwarzania, charakter przetwarzania, jego cele, zakres przetwarzanych danych czy rodzaj mogących wystąpić zagrożeń dla praw i wolności osób fizycznych. Administrator w ramach weryfikacji podmiotu przetwarzającego może prosić podmiot przetwarzający np. o udostępnienie mu konkretnych dokumentów, takich jak polityka ochrony danych osobowych, polityka prywatności czy posiadane certyfikaty. W praktyce weryfikacja często odbywa się poprzez zadawanie konkretnych pytań w formie ankiety, która jest skierowana do podmiotu przetwarzającego. Istotne jest to, żeby dokonanie weryfikacji zostało przez administratora udokumentowane w formie wymiany maili, notatki lub wypełnionej ankiety.

5.3.1. CO TO JEST DALSZE POWIERZENIE?

Dalsze powierzenie przetwarzania danych osobowych (podpowierzenie) to proces, w którym podmiot przetwarzający przekazuje dane osobowe innemu podmiotowi przetwarzającemu (dalszy podmiot przetwarzający) w celu przetwarzania tych danych, pod warunkiem uzyskania uprzedniej zgody administratora i zawarcia odpowiedniej umowy powierzenia.

PRZYKŁAD

Związek sportowy korzysta z usług agencji marketingowej, która świadczy usługi wysyłki newslettera na adresy mailowe przekazane przez związek. Agencja przechowuje otrzymane od związku maile w chmurze, której dostawcą jest zewnętrzna firma.

Dalsze podpowierzenie powinno się odbywać na następujących warunkach:

- ▶ podpowierzenie może mieć miejsce wyłącznie za uprzednią pisemną zgodą administratora danych, która może być wyrażona ogólnie lub w sposób szczególny. Administrator musi mieć prawo do sprzeciwu wobec dodania lub zmiany dalszych podmiotów przetwarzających;

UWAGA!

W praktyce wspomniana zgoda może być zawarta w umowie powierzenia przetwarzania danych osobowych. Jeżeli na etapie jej zawierania strony wiedzą, że część operacji

na danych osobowych będzie wykonywana przez inny podmiot, warto w umowie powierzenia przetwarzania danych osobowych od razu wyrazić zgodę na dalsze powierzenie przetwarzania danych osobowych. Zdarzają się również przypadki, że na etapie zawierania umowy powierzenia przetwarzania danych osobowych kwestie dalszego powierzenia nie są jeszcze przesądzone, w takim wypadku umowa powierzenia powinna precyzować m.in. takie kwestie, jak tryb wystąpienia o zgodę na podpowierzenie, w tym czas jej złożenia oraz termin wyrażenia. Zgoda na podpowierzenie powinna być uzyskana przez podmiot przetwarzającym przed dokonaniem takiego podpowierzenia.

- ▶ podmiot przetwarzający musi zawrzeć z dalszym podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych, która nakłada na dalszy podmiot przetwarzający te same obowiązki ochrony danych, jakie są określone w umowie między administratorem a podmiotem przetwarzającym;
- ▶ podmiot przetwarzający jest w pełni odpowiedzialny wobec administratora za przestrzeganie obowiązków przez dalszy podmiot przetwarzający. Oznacza to, że musi monitorować i zapewniać, że dalszy podmiot przetwarzający spełnia wszystkie wymogi umowy i RODO.

UWAGA!

Administrator powinien posiadać wykaz wszystkich dalszych podmiotów przetwarzających, z których usług korzysta podmiot przetwarzający.

5.4. ODNIESIENIE DO DZIAŁALNOŚCI ZWIĄZKÓW I KLUBÓW SPORTOWYCH

Każdy związek, jak również każdy klub w określonych sytuacjach będzie administratorem danych osobowych. Każdy z tych podmiotów przetwarza dane osobowe zawodników czy trenerów. Nawet jeżeli dany podmiot nie zatrudnia pracowników, to zapewne zawiera umowy zlecenia lub umowy na świadczenie usług z osobami prowadzącymi działalność gospodarczą. Niezależnie od powyższego każdy z tych podmiotów może również występować w relacji współadministrowania, np. przygotowując konkurs razem z kilkoma innymi klubami, organizując wspólnie zawody, turnieje czy mecze, programy szkoleniowe, w tym obozy sportowe, szkolenia, programy rozwojowe, tworząc platformę internetową czy inny system służący np. do rejestracji

zawodników. Relacje te jednak będą zależne od konkretnego stanu faktycznego i określonej sytuacji. Może się jednocześnie zdarzyć, że dany związek lub klub, poza tym, że będzie przetwarzał określone dane osobowe jako administrator lub współadministrator, w szczególnych przypadkach będzie również występował jako podmiot przetwarzający. Na przykład realizacja zadania zleconego przez Ministra Sportu i Turystyki w sytuacji, w której to Minister będzie decydował o celach i sposobach przetwarzania danych osobowych, będzie skutkowałą zawarciem umowy powierzenia przetwarzania danych osobowych. Należy pamiętać również o tym, że dana organizacja może być jednocześnie administratorem i podmiotem przetwarzającym nie tylko w zakresie różnych danych osobowych, różnych kategorii osób. Może się też zdarzyć, że dany klub sportowy jest zarówno administratorem, jak i podmiotem przetwarzającym w zakresie tych samych danych, mogą być one bowiem przetwarzane w ramach różnych procesów, w których dana organizacja pełni różne role.

5.5. JAK USTALIĆ ROLĘ PEŁNIONĄ W PROCESIE PRZETWARZANIA DANYCH OSOBOWYCH?

Ustalenie poszczególnych ról w procesie przetwarzania danych osobowych czasami może nastroczać sporo problemów. To, czy dany podmiot pełni rolę administratora, współadministradora czy podmiotu przetwarzającego będzie uzależnione od konkretnych działań podejmowanych przez te podmioty, w tym od zakresu ich uprawnień i kompetencji. Niektóre przypadki będą wymagały szczegółowej analizy i oceny zaistniałej sytuacji. Aby ustalić rolę pełnioną w procesie przetwarzania danych osobowych:

- ▶ zidentyfikuj konkretny proces przetwarzania danych osobowych i ustal jego cele;
- ▶ ustal, kto decyduje o celach przetwarzania danych osobowych (to zadanie administratora);
- ▶ sprawdź, kto decyduje o sposobie przetwarzania danych, w tym o narzędziach i procedurach (to zadanie administratora);
- ▶ ustal, ile podmiotów zaangażowanych jest w proces przetwarzania danych osobowych, jeżeli jest ich kilka, sprawdź, czy cele i sposoby przetwarzania danych są określane wspólnie (jeżeli odpowiedź jest twierdząca, masz do czynienia ze współadministrowaniem danymi);
- ▶ oceń, czy podmiot działa autonomicznie, czy pod nadzorem innego podmiotu (autonomiczne podejmowanie decyzji w zakresie przetwarzania danych sugeruje rolę administratora);
- ▶ sprawdź, kto decyduje o zakresie i rodzaju przetwarzanych danych osobowych (decyzje te są zazwyczaj podejmowane przez administratora danych);

- oceń relacje i instrukcje między podmiotami (jeśli jeden podmiot przetwarza dane zgodnie z instrukcjami i celami innego podmiotu, pierwszy jest podmiotem przetwarzającym, a drugi – administratorem danych).

5.6. STRONA TRZECIA

ART. 4 RODO. DEFINICJE

Na użytek niniejszego rozporządzenia:

„10) »strona trzecia« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe”.

Innymi słowy, strona trzecia to każdy podmiot, który nie jest bezpośrednio zaangażowany w przetwarzanie danych na mocy relacji administratora lub podmiotu przetwarzającego, ale może mieć dostęp do danych osobowych lub być w jakiś sposób z nimi związany. W momencie, w którym strona trzecia otrzyma dostęp do danych, staje się ich administratorem lub podmiotem przetwarzającym.

PRZYKŁAD

Polski związek sportowy zawiera umowę z firmą sprząającą na usługi sprzątania biura. Osoby sprzątające nie mają dostępu do danych osobowych przetwarzanych przez związek. Polski związek sportowy nie zamierza angażować firmy sprząającej ani jej pracowników w proces przetwarzania danych osobowych. Firma ta i jej pracownicy są zatem postrzegani jako strona trzecia. Polski związek sportowy powinien zastosować odpowiednie środki bezpieczeństwa uniemożliwiające dostęp do danych i wprowadzić obowiązek zachowania poufności na wypadek przypadkowego ujawnienia danych osobowych. Chodzi o sytuacje, w których np. osoba wykonująca czynności sprzątania przypadkowo może mieć wgląd w dokumenty pozostawione na biurku przez pracownika związku²⁶.

²⁶ Przygotowane w oparciu o przykład znajdujący się w Wytycznych EROD 7/2020 dotyczących pojęć administratora oraz podmiotu przetwarzającego zawartych w RODO.

5.7. ODBIORCA DANYCH

ART. 4 RODO. DEFINICJE

Na użytek niniejszego rozporządzenia:

„9) »odbiorca« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania”.

Odbiorcą danych osobowych jest co do zasady każdy, komu są one ujawniane, nie są nim za to organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego.

PRZYKŁAD

Polski związek sportowy w ramach obowiązków sprawozdawczych przekazuje Ministrowi Sportu i Turystyki dane osobowe uczestników wydarzenia organizowanego ze środków finansowanych z budżetu państwa, których dysponentem jest Minister.

Klub sportowy przekazuje dane zawodników polskiemu związkowi sportowemu w celu dokonania ich rejestracji i uzyskania licencji zawodniczej.

Odbiorcę danych należy wskazać w klauzuli informacyjnej oraz rejestrze czynności przetwarzania danych osobowych. Nie trzeba natomiast wskazywać w klauzuli informacyjnej, że w niektórych sytuacjach dane osobowe będą udostępniane policji, prokuraturze, sądom czy ZUS na potrzeby prowadzonych przez te organy postępowań. Część administratorów informuje o tym, nie jest to jednak obowiązkowe, ponieważ podmioty te nie są zgodnie z przepisami RODO odbiorcami danych.

Zgodnie ze stanowiskiem wyrażonym przez PUODO na potrzeby obowiązku prowadzenia rejestrów przetwarzania danych należy przyjąć, że odbiorcami danych nie są podmioty działające z upoważnienia administratora, w jego imieniu i na jego polecenie wewnątrz struktury organizacyjnej, czyli m.in. pracownicy, zleceniobiorcy czy wolontariusze organizacji²⁷.

²⁷ UODO, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, uodo.gov.pl/pl/file/708 [dostęp: 7.08.2025].

6. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

ART. 5 RODO. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

„1. Dane osobowe muszą być:

- a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (»zgodność z prawem, rzetelność i przejrzystość«);
- b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami (»ograniczenie celu«);
- c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (»minimalizacja danych«);
- d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (»prawidłowość«);
- e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą (»ograniczenie przechowywania«);
- f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwoloną lub niezgodną z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (»integralność i poufność«)».

6.1. ZASADA ZGODNOŚCI Z PRAWEM, RZETELNOŚCI I PRZEJRZYSTOŚCI

Przetwarzanie zgodne z prawem: Dane osobowe muszą być przetwarzane zgodnie z obowiązującymi przepisami prawa, czyli powinny być przetwarzane w oparciu o wskazaną w RODO podstawę prawną. Podstawy prawne wynikają z art. 6 (podstawy prawne przetwarzania danych zwykłych) oraz art. 9 (podstawy prawne przetwarzania szczególnych kategorii danych).

Rzetelność: Przetwarzanie danych powinno być prowadzone w sposób uczciwy i z poszanowaniem praw osób, których dane dotyczą.

Przejrzystość: Osoby, których dane są przetwarzane, powinny być informowane w sposób jasny i zrozumiały o przetwarzaniu ich danych osobowych, stąd m.in. konieczność spełnienia wobec tych osób tzw. obowiązku informacyjnego (patrz: **Obowiązek informacyjny**).

6.2. ZASADA OGRANICZENIA CELU

Dane osobowe powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach. Cele przetwarzania danych powinny być wskazane m.in. w klauzuli informacyjnej. Przetwarzanie danych nie może być sprzeczne z pierwotnymi celami, dla których zostały zebrane.

PRZYKŁAD

Rekrutacja pracowników: cel pierwotny – dane osobowe kandydatów (CV, listy motywacyjne, referencje) są zbierane w celu przeprowadzenia procesu rekrutacyjnego; **dalejsze przetwarzanie** – po zakończeniu rekrutacji dane kandydatów, którzy nie zostali zatrudnieni, nie mogą być przechowywane i wykorzystywane do innych celów, np. do innych rekrutacji, bez uzyskania ich zgody.

6.3. ZASADA MINIMALIZACJI DANYCH

Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane²⁸. Danych osobowych nie można gromadzić na zapas ani w zakresie, który byłby nieuzasadniony realizowanym celem.

²⁸ Motyw 39 RODO.

PRZYKŁAD

Formularze kontaktowe na stronach internetowych: formularz kontaktowy powinien wymagać jedynie podstawowych informacji niezbędnych do nawiązania kontaktu, takich jak imię, nazwisko i adres e-mail. Żądanie podawania numeru telefonu, adresu zamieszkania lub innych danych osobowych bez uzasadnionego powodu narusza zasadę minimalizacji danych.

Rekrutacja pracowników: pracodawca zbiera tylko te informacje, które są bezpośrednio związane z oceną kwalifikacji kandydata, takie jak CV, list motywacyjny, kwalifikacje zawodowe. Nie zbiera na etapie rekrutacji szczegółowych informacji medycznych czy danych o rodzinie kandydata.

6.4. ZASADA PRAWIDŁOWOŚCI

Administrator danych powinien dbać o to, aby dane były zgodne z rzeczywistością i odpowiadały aktualnemu stanowi faktycznemu. Jeśli dane mogą się zmieniać (np. adres, nazwisko, stan cywilny), należy zapewnić możliwość ich aktualizacji. Osoba, której dane osobowe są przetwarzane, ma prawo żądać sprostowania danych, które są nieprawidłowe. Administrator powinien weryfikować dane w sposób adekwatny do celu ich przetwarzania.

6.5. ZASADA OGRANICZENIA PRZECHOWYWANIA

Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są przetwarzane. **Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum.** Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. **Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu**²⁹.

²⁹ Motyw 39 RODO.

Okres przechowywania danych osobowych zwany jest **retencją danych osobowych**.

Należy pamiętać o tym, że dane osobowe są przetwarzane w różnych celach, w związku z czym ich okres retencji będzie różny, np. inny będzie okres przechowywania danych osobowych uczestników jednorazowego eventy sportowego, inny stałych zawodników – członków klubu sportowego, a jeszcze inny klientów sklepu internetowego sprzedającego gadżety sportowe.

Okres przechowywania danych osobowych powinien być każdorazowo ustalony przez administratora. Danych osobowych nie można przechowywać w nieskończoność. Każdy administrator musi ustalić niezbędny dla niego okres retencji danych. Okres ten powinien być określony na podstawie celów przetwarzania danych, przepisów prawa oraz zasad minimalizacji danych. Przechowywanie danych tylko przez niezbędny czas zmniejsza ryzyko nieuprawnionego przetwarzania i chroni prywatność osób, których dane są przetwarzane.

6.5.1. POLITYKA RETENCJI – PRZYJMOWAĆ CZY NIE?

Rekomendowane jest stworzenie w ramach organizacji polityki retencji. Jest to wewnętrzny dokument, które określa zasady i okresy przechowywania danych osobowych. Nie jest on obowiązkowy, jednak przyjęcie polityki retencji danych pomaga organizacji zapewnić zgodność z przepisami prawa dotyczącymi ochrony danych osobowych, w tym z RODO. Polityka retencji pomaga w efektywnym zarządzaniu danymi osobowymi. Dodatkowo posiadanie udokumentowanych zasad dotyczących przechowywania i usuwania danych pozwala na szybkie dostarczenie dowodów zgodności z przepisami prawa (patrz: Zasada rozliczalności).

6.5.2. JAK USTALIĆ OKRES RETENCJI DANYCH OSOBOWYCH?

Aby ustalić okres retencji danych osobowych:

- ▶ zdefiniuj, w jakim celu dane osobowe są gromadzone i przetwarzane (powinny być przechowywane tylko tak długo, jak jest to konieczne do osiągnięcia tego celu);
- ▶ sprawdź, czy istnieją jakiegokolwiek przepisy prawne wymagające przechowywania danych przez określony czas, np. przepisy podatkowe, prawa pracy, przepisy rachunkowe;
- ▶ weź pod uwagę potrzeby związane z prowadzoną przez twoją organizację działalnością (potrzeby biznesowe), takie jak promocja organizacji, rozwiązywanie

sporów, prowadzenie postępowań dyscyplinarnych czy archiwizacja (dane powinny być przechowywane tylko tak długo, jak jest to uzasadnione z punktu widzenia biznesowego);

- ▶ pamiętaj o zasadzie minimalizacji danych – powinny być one przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, tylko przez okres nie dłuższy niż jest to niezbędne. Po upływie tego czasu dane powinny zostać zanonimizowane lub usunięte;
- ▶ dokonuj regularnego przeglądu i usuwaj dane, których przetwarzanie jest niezasadne;
- ▶ jeżeli twoja organizacja przyjęła politykę retencji, monitoruj ją i w razie potrzeby aktualizuj w taki sposób, żeby odpowiadała aktualnym potrzebom oraz obowiązującym przepisom prawa.

PRZYKŁAD

Klub sportowy stosuje na swoich obiektach sportowych monitoring wizyjny w celach zapewnienia bezpieczeństwa. Nagrania z monitoringu powinny być przechowywane tylko przez krótki okres (np. 30 dni) i usuwane po upływie tego czasu, chyba że są potrzebne np. do wyjaśnienia incydentów bezpieczeństwa.

Klub sportowy zatrudnia trenerów na umowy-zlecenia. Dane osobowe są w tym przypadku przetwarzane w celu zawarcia i realizacji umowy-zlecenia, jak również w celach podatkowych czy ubezpieczeniowych. Określone dane osobowe mogą być przetwarzane również w celach promocyjnych, np. wizerunek trenera czy e-mail w celu wysyłki newslettera. Dane trenera mogą być również przetwarzane w ramach prowadzonego postępowania dyscyplinarnego. Każdy ze wskazanych celów przetwarzania danych może wiązać się z koniecznością określenia innego terminu retencji danych osobowych przetwarzanych w ramach realizacji tego celu.

Uczestnik szkolenia przekazał związkowi określone dane (np. numer telefonu i adres e-mail) związane z koniecznością kontaktu w związku z organizowanym przez związek szkoleniem. Po przeprowadzeniu szkolenia cel przetwarzania danych osobowych, dla którego dane zostały zebrane, ustaje.

UWAGA!

Dłuższe przechowywanie danych jest dozwolone, jeśli są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, naukowych, historycznych lub statystycznych, pod warunkiem wdrożenia odpowiednich środków technicznych i organizacyjnych.

6.6. ZASADA INTEGRALNOŚCI I POUFNOŚCI

Dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (patrz: *Bezpieczeństwo danych osobowych*).

6.7. ZASADA ROZLICZALNOŚCI

Administrator danych musi być w stanie udowodnić, że przestrzega przepisów RODO, co oznacza, że musi mieć m.in. odpowiednią dokumentację i procedury, które świadczą o zgodnym z prawem przetwarzaniu danych. Zasada rozliczalności nakłada na administratora danych ciężar dowodowy, polegający na konieczności wykazania przez niego, zarówno przed organem nadzorczym (PUODO), jak również przed osobami, których danymi osobowymi dysponuje, że przestrzega wszystkich zasad przetwarzania danych³⁰.

6.7.1. CO ADMINISTRATOR POWINIEN DOKUMENTOWAĆ?

W pierwszej kolejności powinien móc wykazać, że przyjął odpowiednie procedury w postaci m.in. polityki ochrony danych osobowych (lub regulamin dotyczący kwestii związanych z przetwarzaniem danych osobowych w ramach danej organizacji), procedury dotyczącej postępowania w przypadku naruszenia ochrony danych osobowych, w tym zgłaszania incydentów do organów nadzorczych i osób, których dane dotyczą, polityki bezpieczeństwa informacji czy polityki retencji. Dodatkowo administrator musi realizować obowiązki wynikające wprost z RODO, tj. musi prowadzić rejestr czynności przetwarzania danych osobowych i rejestr incydentów ochrony danych osobowych, zawierać umowy powierzenia przetwarzania danych osobowych, upoważniać osoby do przetwarzania w jego imieniu danych osobowych. Administrator powinien również posiadać dokumentację z prowadzonej oceny ryzyka czy oceny skutków dla ochrony danych osobowych. Jeżeli administrator przetwarza dane osobowe na podstawie zgody, powinien móc wykazać, że wspomniane zgody zostały wyrażone, np. poprzez gromadzenie stosowanych formularzy w formie papierowej lub elektronicznej. Jeżeli administrator szkoli swoich pracowników

³⁰ Decyzja PUODO z dnia 18 października 2019 r., ZSPU.421.3.2019.

z zagadnień dotyczących danych osobowych, to powinien móc udowodnić, że takie szkolenia mają miejsce i kto w nich uczestniczy (np. dysponować listą obecności ze szkolenia czy rejestrem osób przeszkolonych). W sytuacji, w której administrator ma wątpliwości, czy jakiś obowiązek go dotyczy, najlepiej sporządzić notatkę, z której będzie wynikało, że przeanalizował temat i doszedł do konkretnych wniosków.

Przykładów działań administratora można wskazać dużo, jednak należy podkreślić, że będą one różne w zależności od tego, kogo będą dotyczyć. To administrator musi przedstawić dowody, które będą wskazywały na działanie adekwatne do sytuacji, zgodne z przepisami o ochronie danych osobowych. Duże polskie związki sportowe nie będą stosowały takich samych rozwiązań jak małe kluby. Podmioty, które przetwarzają dane osobowe regularnie, na dużą skalę, w szerokim zakresie, nie będą stosowały tych samych rozwiązań, co podmioty przetwarzające dane osobowe sporadycznie, na minimalną skalę. Nie wszystkie podmioty są zobowiązane wdrażać skomplikowane, rozbudowane polityki ochrony danych osobowych, które nie będą dostosowane do skali i profilu ich działań. Dokumentacja w przypadku niektórych podmiotów może być bardzo rozbudowana, natomiast w przypadku innych może składać się jedynie z wypunktowania kilku najistotniejszych zasad. Reasumując, każdy przypadek należy oceniać indywidualnie. Jednocześnie należy pamiętać o tym, że przetwarzanie danych osobowych w niewielkim zakresie nie zwalnia z obowiązku stosowania przepisów dotyczących ochrony danych osobowych. RODO ze względu na swój elastyczny charakter pozwala na dobranie pewnych rozwiązań do specyfiki i skali działań, jednak nie zwalnia z obowiązku stosowania omówionych powyżej zasad.

7. PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH

ART. 6 RODO. ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

„1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

- a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem”.

Akapit pierwszy lit. f nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Jedną z podstawowych zasad przetwarzania danych osobowych jest zasada zgodności z prawem (patrz: **Ogólne zasady przetwarzania danych osobowych**). Zgodnie z nią dane osobowe mogą być przetwarzane tylko wtedy, gdy istnieje ku temu jedna z podstaw prawnych wskazanych w RODO. Odrębne podstawy prawne są przewidziane dla danych osobowych zwykłych (art. 6 RODO) oraz dla szczególnych

kategorii danych osobowych (danych wrażliwych) (art. 9 RODO). Dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa wskazane w art. 10 RODO będą przetwarzane na tych samych podstawach prawnych co dane osobowe zwykłe (art. 6 RODO). Każda z przesłanek ma charakter samodzielny. Do legalnego przetwarzania danych osobowych wystarczy spełnienie jednej z nich.

Poniżej przedstawiono podstawy prawne przetwarzania danych najczęściej występujące w podmiotach sportowych wraz z przykładowymi procesami.

7.1. PODSTAWY PRZETWARZANIA DANYCH ZWYKŁYCH

7.1.1. ZGODA OSOBY, KTÓREJ DANE OSOBOWE SĄ PRZETWARZANE (ART. 6 UST. 1 LIT A RODO)

ART. 7 RODO. WARUNKI WYRAŻENIA ZGODY

„1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2. Jeżeli osoba, której dane dotyczą, wyrazi zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy m.in. od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy”.

Przetwarzanie danych jest legalne, jeśli osoba, której dane dotyczą, wyraziła na to zgodę. Zgoda musi być:

- ▶ dobrowolna,
- ▶ świadoma,
- ▶ konkretna,
- ▶ jednoznaczna,
- ▶ możliwa do wycofania w dowolnym momencie.

Zgoda może być wyrażona w formie oświadczenia bądź też wyraźnego działania potwierdzającego przyzwolenie na przetwarzanie danych osobowych. Jeżeli zgoda na przetwarzanie służy różnym celom, powinna dotyczyć odrębnie każdego z tych celów. Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że wyraziła ona zgodę na dany cel przetwarzania³¹ (patrz: Zasada rozliczalności).

UWAGA!

Zgoda musi być zawsze udzielona przez aktywne działanie lub oświadczenie. Musi być oczywiste, że osoba, której dane dotyczą, zgodziła się na określone przetwarzanie. Zgodę można uzyskać np. w formie pisemnego lub (zarejestrowanego) ustnego oświadczenia, w tym drogą elektroniczną. Jednocześnie również inne fizyczne działania można zakwalifikować jako wyraźne działania potwierdzające zgodnie z RODO, np. włożenie wizytówki do specjalnie oznaczonej skrzynki na konferencji sportowej, gdzie wyraźnie informuje się, że złożenie wizytówki oznacza zgodę na przetwarzanie danych kontaktowych w celach networkingowych.

KIEDY ZGODA?

W sytuacji, gdy organizacja (np. klub sportowy):

- ▶ przetwarza dane kandydatów do pracy w przyszłych rekrutacjach;
- ▶ przetwarza dane kandydata do pracy poza zakresem wynikającym z Kodeksu pracy;
- ▶ rozpowszechnia w mediach społecznościowych na swoich profilach wizerunek niepełnoletnich uczestników organizowanych wydarzeń;

³¹ Motyw 42 RODO: „Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych”. Mówiąc inaczej, w przypadku przetwarzania danych na podstawie zgody klauzula informacyjna oznacza nie tylko samo spełnienie obowiązku informacyjnego aktualnego dla każdej z podstaw przetwarzania, lecz dodatkowo stanowi element mogący nawet decydować o tym, czy w konkretnym przypadku w ogóle dysponujemy podstawą prawną przetwarzania (jeśli zgoda nie jest świadoma, to nie wiąże, a jeśli nie wiąże, to nie może stanowić podstawy prawnej przetwarzania danych). Dlatego przy okazji formułowania treści zgody tak ważna jest jednoczesna i uważna realizacja obowiązku informacyjnego. Jego zaniedbanie może udaremnić skuteczne oparcie przetwarzania danych na zgodzie osoby, której dane dotyczą.

- ▶ przeprowadzi konkurs (w tym wypadku w zależności od stanu faktycznego można również rozważać podstawę prawną w postaci wykonania umowy lub uzasadnionego interesu administratora danych osobowych);
- ▶ korzysta z prywatnych danych kontaktowych swojego pracownika (np. numeru telefonu, adresu mailowego) w celu kontaktowania się z nim w sprawach służbowych.

PRZYKŁAD

Zgoda przedstawiciela ustawowego (rodzica bądź opiekuna prawnego) na udział niepełnoletniego zawodnika we współzawodnictwie nie jest tym samym co zgoda na przetwarzanie jego danych osobowych. Konieczność uzyskania zgody przedstawiciela ustawowego niepełnoletniego zawodnika na udział we współzawodnictwie wynika z przepisów Kodeksu rodzinnego i opiekuńczego (w szczególności art. 92, art. 95 i art. 96), to bowiem przedstawiciel ustawowy sprawuje władzę rodzicielską nad niepełnoletnim zawodnikiem i to on podejmuje decyzje w sprawach jego dotyczących. Udział zawodnika we współzawodnictwie będzie wiązał się z przetwarzaniem danych osobowych, jednak przesłanką przetwarzania danych osobowych w tym wypadku nie będzie zgoda. W zależności od konkretnej sytuacji przetwarzanie danych osobowych może odbywać się w tym wypadku np. na podstawie art. 6 ust. 1 lit e RODO (realizacja zadania w interesie publicznym w przypadku organizowania współzawodnictwa przez polski związek sportowy), art. 6 ust. 1 lit b RODO (udział w zawodach po akceptacji regulaminu), art. 6 ust. 1 lit f RODO (organizowanie zawodów sportowych zgodnie z przyjętymi wewnętrznymi regulacjami danego związku sportowego, m.in. statutem, uchwałami).

Nieprawidłowe jest odbieranie zgody na przetwarzanie naszych danych osobowych w przypadku istnienia innej przesłanki legalizacyjnej, która upoważnia administratora do przetwarzania danych osobowych w tym samym celu i zakresie. Przesłanka zgody powinna być traktowana jako ostateczna i stosowana wyłącznie w przypadku, w którym brakuje innej podstawy przetwarzania danych osobowych. W praktyce przesłanka zgody będzie wykorzystywana raczej rzadko.

7.1.2. WYKONANIE UMOWY (ART. 6 UST. 1 LIT B RODO)

W przypadku, gdy przetwarzanie jest niezbędne do wykonania umowy, gdzie stroną jest osoba, której dane dotyczą, lub do podjęcia działań na jej żądanie przed zawarciem umowy, na szczególną uwagę zasługują dwa elementy:

- ▶ przesłanka ta stanowi podstawę przetwarzania danych osobowych osoby fizycznej, **będącej stroną umowy**;
- ▶ na podstawie tej przesłanki mogą być przetwarzane wyłącznie dane **niezbędne** do wykonywania tej umowy.

KIEDY UMOWA?

W sytuacji, gdy organizacja (np. klub sportowy):

- ▶ korzysta ze wsparcia wolontariusza (zarówno w przypadku zawarcia porozumienia wolontariackiego w formie pisemnej, jak i ustnej);
- ▶ zatrudnia osoby na umowę cywilnoprawną lub zleca świadczenie osobie prowadzącej jednoosobową działalność gospodarczą (np. umowy z trenerami, sędziami, animatorami);
- ▶ otrzymuje darowiznę od osoby fizycznej;
- ▶ umożliwia użytkownikom swojej strony internetowej zapisanie się na newslettera zgodnie z dostępnym tam regulaminem newslettera (regulamin newslettera może stanowić umowę na świadczenie usług drogą elektroniczną);
- ▶ przetwarza dane uczestników organizowanych przez siebie kursów, seminariów czy szkoleń (np. imię, nazwisko, certyfikaty, dane kontaktowe);
- ▶ gromadzi dane osobowe zawodników, trenerów w celu organizacji i zarządzania zawodami sportowymi (na podstawie zaakceptowanego przez te osoby regulaminu zawodów);
- ▶ przyjmuje zawodnika (np. w drodze zawarcia umowy lub podpisania deklaracji przystąpienia zgodnie z przyjętymi regulacjami wewnętrznymi klubu – statutem, regulaminem);
- ▶ zawiera ze sportowcem kontrakt zawodniczy;
- ▶ gromadzi dane osobowe kibiców (np. imię, nazwisko, dane kontaktowe, dane płatności) w związku ze sprzedażą biletów na imprezy sportowe;
- ▶ sprzedaje gadzety sportowe w sklepie internetowym i w związku z tym gromadzi dane osobowe klientów;
- ▶ przeprowadza konkurs wśród swoich członków (pod warunkiem wcześniejszej akceptacji warunków tego konkursu).

7.1.3. WYPEŁNIANIE OBOWIĄZKU PRAWNEGO (ART. 6 UST. 1 LIT C RODO)

Przetwarzanie jest wymagane, aby wypełnić obowiązek prawny ciążyący na administratorze, wynikający z przepisów prawa krajowego lub unijnego. W tym wypadku podstawa prawna przetwarzania jest określona w konkretnych przepisach prawa, które wskazują na cel przetwarzania danych.

KIEDY PRZEPIS PRAWA?

W sytuacji, gdy organizacja (np. klub sportowy):

- ▶ prowadzi rekrutację do pracy (art. 22¹ Kodeksu pracy określa konkretny katalog danych osobowych, których przedstawienia można żądać od kandydata do pracy);
- ▶ spełnia obowiązki wynikające z przepisów o rachunkowości oraz przepisów podatkowych w przypadku zatrudniania osoby na umowę-zlecenia;
- ▶ spełnia obowiązki wynikające z ustawy o działalności pożytku publicznego i wolontariacie³² w przypadku zawierania umowy z wolontariuszem, np. konieczność ubezpieczenia wolontariusza;
- ▶ spełnia obowiązki wynikające z przepisów ubezpieczeniowych w sytuacji zatrudniania osoby na umowę-zlecenia;
- ▶ spełnia obowiązki wynikające z przepisów podatkowych w sytuacji wydania nagrody w organizowanym przez klub sportowy konkursie;
- ▶ rozpoznaje zgłoszenia wewnętrzne zgodnie z przepisami ustawy o ochronie sygnalistów;
- ▶ dokonuje weryfikacji w Rejestrze sprawców przestępstw na tle seksualnym oraz odbiera zaświadczenia zawierające informację z Krajowego Rejestru Karnego zgodnie z zapisami ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich³³;
- ▶ wypełnia obowiązek identyfikacji uczestników meczu piłki nożnej³⁴;
- ▶ wypełnia obowiązek utrwalania przebiegu imprezy masowej za pomocą urządzeń rejestrujących obraz i dźwięk, odbywającej się na stadionie, obiekcie czy terenie wskazanym w wykazie wojewody³⁵;
- ▶ przetwarza dane osobowe w związku z nadawaniem przez polski związek sportowy określonych uprawnień, np. patentu strzeleckiego³⁶, patentu żeglarskiego³⁷;
- ▶ spełnia obowiązek ubezpieczenia od następstw nieszczęśliwych wypadków zawodnika uczestniczącego we współzawodnictwie sportowym organizowanym przez polski związek sportowy oraz zawodnika kadry narodowej³⁸.

³² Art. 46 ust. 3 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i wolontariacie (Dz.U. z 2020 r. poz. 1057 z późn. zm.).

³³ Art. 21 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich.

³⁴ Art. 13 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych.

³⁵ Art. 11 ust. 4 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych.

³⁶ Art. 10.b. ustawy z dnia 21 maja 1999 r. o broni i amunicji.

³⁷ Art. 37a ustawy z dnia 21 grudnia 2000 r. o żegludze lądowej.

³⁸ Art. 38 ustawy z dnia 25 czerwca 2010 r. o sporcie.

7.1.4. OCHRONA ŻYWOTNYCH INTERESÓW OSOBY (ART. 6 UST. 1 LIT D RODO)

Przetwarzanie jest niezbędne w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. Zazwyczaj przesłanka ta odnosi się do sytuacji zagrażających życiu lub zdrowiu np. w przypadku nagłej kontuzji lub wypadku na boisku, kiedy zawodnik wymaga natychmiastowej pomocy medycznej.

7.1.5. WYKONANIE ZADANIA REALIZOWANEGO W INTERESIE PUBLICZNYM LUB W RAMACH SPRAWOWANIA WŁADZY PUBLICZNEJ (ART. 6 UST. 1 LIT E RODO)

Przesłanka wykonywania zadania w interesie publicznym odnosi się do sytuacji, w których przetwarzanie danych osobowych jest niezbędne do realizacji zadań określonych prawem, mających na celu dobro ogółu, a nie interes prywatny, które są realizowane przy użyciu form niewładczych. Przesłanka ta dotyczy zadań, które zostały zlecone podmiotowi przez przepisy prawa, ale wskazuje się, że art. 6 ust. 1 lit. e RODO znajdzie zastosowanie również tam, gdzie konkretne zadania nie wynikają wprost z aktów powszechnie obowiązujących, lecz np. z programów rządowych, których celem jest realizacja określonych polityk lub celów publicznych. Nie ma zamkniętego katalogu zadań realizowanych w interesie publicznym ani podmiotów, które mogłyby pełnić funkcję administratora. Przesłanka ta nie dotyczy wyłącznie podmiotów publicznych.

KIEDY INTERES PUBLICZNY?

W sytuacji, gdy organizacja (np. klub sportowy, polski związek sportowy) realizuje zadania zlecone:

- ▶ na podstawie ustawy o działalności pożytku publicznego i wolontariacie³⁹;
- ▶ w oparciu o art. 29 ust. 7 ustawy o sporcie⁴⁰.

³⁹ Wytyczne EROD nr 1/2024 dotyczące przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit f RODO (konsultacje publiczne zamknięte 20 listopada 2024 r.).

⁴⁰ Art. 29 ust. 7 ustawy z dnia 25 sierpnia 2010 r. o sporcie. Minister właściwy do spraw kultury fizycznej w zakresie dofinansowania zadań związanych z przygotowywaniem kadry narodowej do udziału w igrzyskach olimpijskich, igrzyskach paraolimpijskich, igrzyskach głuchych, mistrzostwach świata lub mistrzostwach Europy może zlecać polskiemu związkowi sportowemu, Polskiemu Komitetowi Olimpijskiemu i Polskiemu Komitetowi Paraolimpijskiemu realizację zadań publicznych z pominięciem otwartego konkursu ofert, o którym mowa w art. 11 ust. 2 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie. Przepisy art. 47 i art. 151 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych stosuje się odpowiednio (Dz.U. z 2009 r. nr 157 poz. 1240).

UWAGA!

Zastosowanie powyżej przesłanki mogą rozważać polskie związki sportowe w zakresie realizowanych przez nie zadań wynikających z przepisów ustawy o sporcie. Polskie związki sportowe są tworzone w celu organizowania i prowadzenia współzawodnictwa w danej dyscyplinie sportu. Do ich powołania niezbędna jest zgoda ministra właściwego ds. kultury fizycznej. Minister zatwierdza również statut polskiego związku sportowego oraz wprowadzane do niego zmiany. Związki sportowe mają monopol w realizacji zadań określonych w art. 13 ustawy o sporcie. Zadania te są wykonywane zgodnie z wewnętrznymi regulacjami przyjęty przez polskie związki sportowe, również w oparciu o regulacje przyjęte przez międzynarodowe organizacje sportowe. Charakter wspomnianych działań może przemawiać za uznaniem, iż stanowią one wykonywanie zadań realizowanych w interesie publicznym, a tym samym przetwarzanie danych osobowych w celu ich wykonania może być oparte na przesłance z art. 6 ust. 1 lit. e RODO.

7.1.6. UZASADNIONY INTERES ADMINISTRATORA LUB STRONY TRZECIEJ (ART. 6 UST. 1 LIT F RODO)

Przetwarzanie jest niezbędne do realizacji prawnie uzasadnionych interesów administratora lub strony trzeciej, chyba że nadrzędny charakter mają interesy lub prawa osób, których dane dotyczą. Oparcie przetwarzania danych osobowych na wskazanej przesłance wymaga⁴¹:

- ▶ zidentyfikowania uzasadnionego interesu;
- ▶ potwierdzenia konieczności przetwarzania danych osobowych;
- ▶ przeprowadzenia testu równowagi.

ZIDENTYFIKOWANIE UZASADNIONEGO INTERESU

Uzasadniony interes administratora danych osobowych to ustalony przez organizację interes w kontekście prowadzonych przez nią działań. Mogą to być interesy komercyjne, społeczne, gospodarcze, prawne, ekonomiczne czy inne interesy, pod warunkiem że są one zgodne z prawem i zasadami ochrony danych osobowych. Interesy, na które powołuje się administrator, muszą być realne, aktualne oraz wystarczająco istotne, aby uzasadnić przetwarzanie danych osobowych. Nie ma zamkniętego katalogu interesów, które mogą być uzasadnione. Jednocześnie należy pamiętać, że nie każdy interes może wypełniać przesłankę uzasadnionego interesu, np. interes

⁴¹ Wytyczne EROD nr 1/2024 dotyczące przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit f RODO (konsultacje publiczne zamknięte 20 listopada 2024 r.).

hipotetyczny, zbyt ogólnikowy czy niezgodny z obowiązującymi przepisami prawa nie będzie mógł być uznany za interes uzasadniony. Uzasadniony interes organizacji sportowej może wynikać z przyjętych przez nią regulacji wewnątrzorganizacyjnych, np. uchwał organów, które będą regulowały kwestie dotyczące działań prowadzonych przez te organizacje, takie jak zarządzanie członkostwem, uczestnictwo w wydarzeniach sportowych czy weryfikacja uprawnień.

Uzasadniony interes administratora danych osobowych może stanowić podstawę przetwarzania np. wtedy, gdy:

- ▶ zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem (np. stałe relacje z członkami klubu sportowego);
- ▶ osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się dalszego przetwarzania⁴².

POTWIERDZENIE KONIECZNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Po zidentyfikowaniu interesu należy ocenić, czy przetwarzanie danych osobowych jest niezbędne do realizacji celu wynikającego z prawnie uzasadnionego interesu. Należy sprawdzić, czy nie istnieją inne środki, przy użyciu których można osiągnąć wspomniany cel, jednocześnie w mniejszym stopniu ograniczając prawa i wolności innych osób. Przy dokonywaniu wspomnianej oceny należy uwzględnić zasadę minimalizacji danych osobowych (patrz: *Zasada minimalizacji danych*).

PRZEPROWADZENIE TESTU RÓWNOWAGI

UWAGA!

Na uzasadniony interes nie można się powołać w sytuacji, w której charakter nadrzędny wobec interesów organizacji mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, w szczególności, gdy ta osoba jest dzieckiem (patrz: *Przetwarzanie danych osobowych w postaci wizerunku*).

⁴² Motyw 47 RODO. Taki prawnie uzasadniony interes może istnieć np. w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, np. gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania.

Przesłanka prawnie uzasadnionego interesu wymaga od organizacji przeprowadzenia tzw. **testu równowagi interesów**, tj. analizy korzyści dla organizacji oraz zagrożeń dla praw i wolności osoby, której dane dotyczą. Jeśli test wykaże, że interesy osoby, której dane dotyczą, mają charakter nadrzędny, przetwarzanie na tej podstawie jest niedopuszczalne.

JAK PRZEPROWADZIĆ TEST RÓWNOWAGI?

1. Identyfikacja uzasadnionego interesu administratora

Określ, jaki jest prawnie uzasadniony interes administratora lub strony trzeciej, np. potrzeba ochrony mienia w obiekcie sportowym, prowadzenie działań marketingowych klubu, relacjonowanie danego wydarzenia sportowego na profilu klubu w mediach społecznościowych, publikacja na stronie internetowej imienia i nazwiska najlepszych strzelców turnieju piłki nożnej.

2. Ocena konieczności przetwarzania danych

Oceń, czy przetwarzanie danych jest konieczne do realizacji określonego celu. Ustal, czy istnieją inne, mniej inwazyjne środki, które umożliwiają jego realizację bez przetwarzania danych osobowych.

3. Ocena wpływu przetwarzania na osoby, których dane dotyczą

Przeanalizuj, w jakim stopniu przetwarzanie danych wpływa na osoby, których dane są przetwarzane. Bierz pod uwagę zarówno pozytywne, jak i negatywne skutki przetwarzania.

4. Wyważenie interesów

Porównaj uzasadniony interes administratora danych z prawami i wolnościami osób, których dane dotyczą. W sytuacji, gdy wpływ na prywatność osób jest minimalny, a interes administratora znaczący, przetwarzanie może być uznane za zgodne z RODO. **Szczegółowo przeanalizuj sytuację, w której w oparciu o przesłankę uzasadnionego interesu chcesz przetwarzać dane osobowe dzieci, np. niepełnoletnich zawodników.**

5. Środki ochrony i minimalizacji ryzyka

Aby zapewnić równowagę, należy wdrożyć środki ochrony minimalizujące ryzyko dla prywatności osoby, której dane dotyczą. Mogą to być np. ograniczenia dostępu do nagrań, ograniczenia czasu przechowywania danych, anonimizacja danych, publikacja relacji na zamkniętej grupie, zablokowanie możliwości nagrywania przez uczestników spotkania online.

DOKUMENTOWANIE TESTU RÓWNOWAGI

Przeprowadzenie testu równowagi powinno być udokumentowane. Administrator musi być w stanie wykazać, że przetwarzanie danych osobowych na podstawie uzasadnionego interesu było poprzedzone testem i że interesy administratora faktycznie przeważały nad interesami osób, których dane dotyczą (patrz: *Zasada rozliczalności*).

KIEDY UZASADNIONY INTERES?

W sytuacji, gdy organizacja (np. klub sportowy, polski związek sportowy):

- ▶ dochodzi roszczeń i broni się przed konkretnymi roszczeniami;
- ▶ przesyła podziękowania za wpłatę dokonaną przez darczyńcę na rzecz klubu;
- ▶ prowadzi monitoring wizyjny obiektu sportowego (jeżeli nie wynika on z obowiązku określonego w ustawie o bezpieczeństwie imprez masowych)⁴³;
- ▶ wykonuje obowiązki sprawozdawcze i rozliczeniowe wynikające z zawartych umów dotacyjnych czy grantowych, o ile ich wykonanie nie jest obowiązkiem prawnym;
- ▶ prowadzi fanpage na portalach społecznościowych i w serwisach internetowych na warunkach określonych przez regulaminy dostawców mediów społecznościowych, w tym komunikuje się z użytkownikami tych mediów;
- ▶ opublikuje relacje z danego wydarzenia sportowego na profilu w mediach społecznościowych;
- ▶ przyznaje akredytacje fotografom i dziennikarzom (uzasadniony interes administratora danych osobowych polega m.in. na konieczności zapewnienia odpowiedniego kontaktu z mediami i osobami relacjonującymi przebieg wydarzenia, bezpieczeństwa podczas wydarzenia, wyboru osób zapewniający najwyższy poziom realizowanych usług – zgodnie z ewentualnie przyjętymi zasadami wewnętrznymi);
- ▶ przesyła oferty do osób, które wyraziły zgodę na przysyłanie im drogą mailową informacji handlowych zgodnie z ustawą o świadczeniu usług drogą elektroniczną oraz ustawą Prawo telekomunikacyjne;
- ▶ prowadzi inne działania o charakterze marketingowym.

UWAGA!

Zgodnie ze stanowiskiem PUODO uzasadniony interes, o którym mowa w art. 6 ust. 1 lit. f RODO, powinien wynikać z realnie istniejącej sytuacji, w której przetwarzanie danych jest rzeczywiście niezbędne do dochodzenia konkretnego roszczenia lub obrony przed nim. Nie może natomiast stanowić podstawy przetwarzania danych wyłącznie w celu potencjalnego, hipotetycznego zabezpieczenia się przed nieokreślonymi, przyszłymi i niepewnymi roszczeniami. Takie przetwarzanie danych osobowych stanowi przetwarzanie „na zapas”, co jest niezgodne z przepisami RODO. Stanowisko to znajduje potwierdzenie w orzecznictwie, m.in. w wyrokach Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Naczelnego Sądu Administracyjnego⁴⁴.

⁴³ Art. 11 ust. 4 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych.

⁴⁴ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13 stycznia 2021 r., sygn. akt II SA/Wa 607/20, wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 marca 2021 r., sygn. akt II SA/Wa 1340/20, wyrok Naczelnego Sądu Administracyjnego z dnia 8 stycznia 2025 r., sygn. akt III OSK 4868/21.

7.2. PODSTAWY PRZETWARZANIA SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH

ART. 9 RODO. PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH

„2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

- a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
- b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
- i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
- j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą”.

Przetwarzanie szczególnych danych osobowych jest co do zasady zakazane. Jednocześnie w przypadku działalności klubów czy związków sportowych dochodzi do sytuacji, w których wspomniane dane będą przetwarzane. Nie budzi zapewne wątpliwości, że wszystkie organizacje sportowe, które występują w roli pracodawców, przetwarzają szczególne kategorie danych osobowych swoich pracowników, w przeważającej mierze dotyczy to danych osobowych dotyczących stanu zdrowia. Poza wspomnianymi kategoriami osób organizacje sportowe mogą również przetwarzać dane szczególnych kategorii swoich zawodników. Najczęściej będą to dane dotyczące stanu zdrowia (w tym np. niepełnosprawność), ale też dane genetyczne czy biometryczne (patrz: Dane biometryczne).

7.2.1. WYRAŻNA ZGODA OSOBY, KTÓREJ DANE OSOBOWE SĄ PRZETWARZANE (ART. 9 UST. 2 LIT. A RODO)

W przypadku przetwarzania szczególnych kategorii danych osobowych zgoda oprócz przesłanek wskazanych powyżej powinna dodatkowo spełniać przesłankę „wyraźnej” zgody. Oznacza to, że powinna być wyrażona w sposób niebudzący wątpliwości, a nie w jakikolwiek sposób dorozumiany, np. poprzez zaznaczenie odpowiednia pola, podpisanie stosownego oświadczenia.

PRZYKŁAD

Wyrażna zgoda osoby, której dane osobowe są przetwarzane, wymagana jest w przypadku przetwarzania danych dotyczących zdrowia zawodników (np. badań lekarskich, raportów medycznych, wyników testów fizjologicznych), aby monitorować ich stan i wydolność fizyczną celem optymalizacji treningów i przygotowań do zawodów.

7.2.2. WYPEŁNIANIE OBOWIĄZKÓW I PRAW PRACODAWCY W DZIEDZINIE PRAWA PRACY (ART. 9 UST. 2 LIT. B RODO)**PRZYKŁAD**

Klub sportowy lub związek sportowy jako pracodawca może przetwarzać dane dotyczące zdrowia pracownika, np. zawarte w zwolnieniach lekarskich, zgodnie z przepisami prawa pracy czy przepisami ubezpieczeń społecznych.

7.2.3. OCHRONA ŻYWOTNYCH INTERESÓW ZAWODNIKA (ART. 9 UST. 2 LIT. C RODO)**PRZYKŁAD**

Przetwarzanie danych osobowych zawodnika dotyczących jego stanu zdrowia będzie uzasadnione, jeśli jest to konieczne do ochrony jego żywotnych interesów, a zawodnik nie jest w stanie wyrazić zgody, np. w przypadku nagłej kontuzji lub wypadku na boisku, kiedy wymaga natychmiastowej pomocy medycznej.

7.2.4. REALIZACJA ZADAŃ W INTERESIE PUBLICZNYM (ART. 9 UST. 2 LIT. G RODO)**PRZYKŁAD**

Przetwarzanie danych o niepełnosprawności zawodnika może być uzasadnione, gdy jest ono konieczne do realizacji celów leżących w interesie publicznym, np. w ramach programów sportowych dla osób z niepełnosprawnościami finansowanych ze środków publicznych.

7.2.5. PRZETWARZANIE NIEZBĘDNE ZGODNIE Z ART. 9 UST. 2 LIT H RODO

Przetwarzanie danych osobowych będzie również uzasadnione w sytuacji, gdy jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego. Zastosowanie ma wówczas art. 9 ust. 2 lit h RODO.

PRZYKŁAD

Przesłanka ta będzie miała zastosowanie w przypadku gromadzenia przez polski związek sportowy zaświadczeń lekarskich o stanie zdrowia zawodników uczestniczących we współzawodnictwie sportowym organizowanym przez polski związek sportowy. Odbieranie orzeczeń lekarskich jest konieczne ze względu na profilaktykę zdrowotną i posiada konkretną podstawę w prawie polskim, tj. m.in. w art. 37 ust. 1 ustawy o sporcie⁴⁵, który nakłada na zawodnika obowiązek uzyskania takiego orzeczenia. **W takim przypadku nie ma potrzeby odbierać od zawodnika osobnej zgody na przetwarzanie danych o zdrowiu zawartych w orzeczeniu lekarskim.**

⁴⁵ Art. 37 ust. 1 ustawy z dnia 25 sierpnia 2010 r. o sporcie. Zawodnik uczestniczący we współzawodnictwie sportowym organizowanym przez polski związek sportowy jest obowiązany do uzyskania orzeczenia lekarskiego o stanie zdrowia umożliwiającym bezpieczne uczestnictwo w tym współzawodnictwie.

8. PROCES LICENCJONOWANIA ZAWODNIKÓW, TRENERÓW I SĘDZIÓW – PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

ART. 13 USTAWY O SPORCIE. PRAWA POLSKIEGO ZWIĄZKU SPORTOWEGO⁴⁶

„1. Polski związek sportowy ma wyłączne prawo do:

- 1) organizowania i prowadzenia współzawodnictwa sportowego o tytuł Mistrza Polski oraz o Puchar Polski w danym sporcie;
- 2) ustanawiania i realizacji reguł sportowych, organizacyjnych i dyscyplinarnych we współzawodnictwie sportowym organizowanym przez związek, z wyjątkiem reguł dyscyplinarnych dotyczących dopingu w sporcie;
- 3) powołania kadry narodowej oraz przygotowania jej do igrzysk olimpijskich, igrzysk paralimpijskich, igrzysk głuchych, mistrzostw świata lub mistrzostw Europy;
- 4) reprezentowania tego sportu w międzynarodowych organizacjach sportowych”.

System licencjonowania zawodników, sędziów i instruktorów w polskich związkach sportowych to formalny proces, który ma na celu nadanie uprawnień do wykonywania określonych czynności w ramach danej dyscypliny sportowej. System ten funkcjonuje w oparciu o regulacje ustawowe (art. 13 ust. 1 pkt 2 ustawy o sporcie) oraz wewnętrzne regulacje poszczególnych związków sportowych (m.in. statuty, regulaminy, uchwały). W doktrynie wskazuje się, że regułami organizacyjnymi, ustanowionymi przez polskie związki sportowe na podstawie art. 13 ust. 1 pkt 2 ustawy o sporcie, są m.in. normy określające obowiązujący w danym sporcie system licencjonowania⁴⁷. Powyższe twierdzenie znajduje również oparcie w treści uzasadnienia do

⁴⁶ Ustawa z dnia 25 sierpnia 2010 o sporcie (Dz.U. z 2024 r. poz. 1488 z późn. zm.).

⁴⁷ E. Krześniak, *Ustawa o sporcie. Komentarz*, Warszawa 2020.

ustawy o sporcie⁴⁸. Nadawanie licencji należy wyłącznie do kompetencji polskich związków sportowych.

W ramach prowadzonych przez polskie związki sportowe procesów licencjonowania przetwarzane są różnego rodzaju dane osobowe. Zakres tych danych najczęściej zależy od specyfiki danej dyscypliny sportowej, jednak większość polskich związków sportowych pozyskuje dane identyfikacyjne, takie jak: imię i nazwisko, numer PESEL czy data urodzenia. Do tego dochodzą dane kontaktowe, takie jak adres zamieszkania i adres e-mail, a w przypadku sędziów lub instruktorów – dane dotyczące kwalifikacji: wykształcenie, dyplomy i certyfikaty potwierdzające kwalifikacje trenerskie lub instruktorskie.

UWAGA!

Zakres przetwarzanych danych w procesie licencjonowania powinien być adekwatny i niezbędny do realizacji tego procesu (patrz: Zasada minimalizacji).

Kwestia doboru przesłanki (patrz: Przesłanki przetwarzania danych osobowych), na podstawie której polskie związki sportowe przetwarzają dane osobowe w procesie licencjonowania, może nastroić sporo wątpliwości. Ze względu na wiele niejasności dotyczących statusu polskiego związku sportowego, charakteru wydawanych przez niego regulacji wewnętrznych, a także realizowanych przez niego zadań ustalenie podstawy prawnej przetwarzania danych osobowych wymaga przyjęcia określonej interpretacji co do bazowych regulacji prawnych odnoszących się do funkcjonowania tej organizacji. Przyjęcie podstawy prawnej przetwarzania danych osobowych będzie pochodną przyjęcia określonych rozwiązań prawnych. Poniższe opracowanie nie daje jednoznacznej odpowiedzi na pytanie, która z przesłanek będzie właściwa, a jedynie wskazuje możliwe do przyjęcia rozwiązania.

8.1. ZGODA

Przesłanką, która **nie** będzie miała zastosowania w procesie licencjonowania, jest **zgoda** (art. 6 ust. 1 lit a RODO). Przede wszystkim zgoda na przetwarzanie danych

⁴⁸ Z uzasadnienia do projektu ustawy o sporcie: Wyłączne uprawnienia przyznane polskiemu związkowi sportowemu są ściśle związane z autonomią tego związku w zakresie ustanawiania i egzekwowania norm sportowych, porządkowych, organizacyjnych i dyscyplinarnych w danym sporcie (art. 13 pkt 2 projektu), co wynika z uznania, że organizowanie i uprawianie sportu jest wolne, również w ramach funkcjonowania polskiego związku sportowego. Powyższe uprawnienia dotyczyć będą także spraw użytkowania licencji, które w chwili obecnej są uregulowane w ustawie o sporcie kwalifikowanym. Również w tym przypadku przyjęto, że jest to sfera wyłącznych uprawnień polskiego związku sportowego.

osobowych ma charakter dobrowolny. W procesie licencjonowania zawodników, sędziów czy instruktorów przetwarzanie danych osobowych jest warunkiem koniecznym do uzyskania licencji. Oznacza to, że osoba zainteresowana uzyskaniem licencji nie może odmówić wyrażenia zgody bez ponoszenia negatywnych konsekwencji, takich jak brak możliwości udziału w zawodach lub ich prowadzenia. W procesie licencjonowania niemożliwe byłoby również skuteczne wycofanie zgody. Musiałoby to się wiązać z daleko idącymi konsekwencjami, m.in. utratą licencji, a tym samym niemożliwością udziału we współzawodnictwie sportowym organizowanym przez polski związek sportowy. Tym samym zgoda odbierana w ramach procesu licencjonowania nie spełnia podstawowych wymogów określonych przez RODO. Warto również pamiętać, że zgoda stanowi przesłankę, która powinna być wykorzystywana wyłącznie w sytuacji braku innych podstaw prawnych przetwarzania danych osobowych, tymczasem specyfika procesu licencjonowania daje podstawy do przyjęcia innych przesłanek.

8.2. WYPEŁNIANIE OBOWIĄZKU PRAWNEGO CIAŻĄCEGO NA ADMINISTRATORZE

Trudno w tym wypadku powoływać się również na przesłankę wynikającą z art. 6 ust. 1 lit. c RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze). Przesłanka ta legalizuje przetwarzanie danych osobowych w przypadku istnienia po stronie administratora obowiązku określonego przepisami prawa, który dla jego realizacji wymaga przetwarzania danych osobowych. Biorąc pod uwagę treść przepisów ustawy o sporcie oraz wątpliwości i kontrowersje występujące w doktrynie odnośnie do charakteru prawnego tworzonych przez polskie związki sportowe wewnętrznych regulacji (nie są to bowiem regulacje mające charakter przepisów prawa powszechnie obowiązującego), uznać należy, że skorzystanie z powyższej przesłanki jest dalece dyskusyjne.

8.3. UZASADNIONY INTERES ADMINISTRATORA DANYCH OSOBOWYCH

Warto natomiast rozważyć zastosowanie przesłanki wynikającej z art. 6 ust. 1 lit. f RODO, czyli **uzasadnionego interesu** administratora danych osobowych, polegającego na konieczności zarządzania współzawodnictwem sportowym na zasadach wynikających z wewnętrznych regulacji związkowych. Polskie związki sportowe, działające w oparciu o art. 13 ust. 1 pkt 2 ustawy o sporcie, mają wyłączne prawo

do ustanawiania i realizacji reguł sportowych, organizacyjnych i dyscyplinarnych we współzawodnictwie sportowym w danym sporcie, a co za tym idzie – prawnie uzasadniony interes w zarządzaniu współzawodnictwem sportowym. Obejmuje to m.in. uprawnienie do wydawania licencji zawodnikom, sędziom oraz instruktorom, zgodnie z przyjętymi przez siebie wewnątrzwiązkowymi regulacjami. Zarządzanie tymi procesami wymaga przetwarzania danych osobowych i odbywa się na zasadach określonych w wewnętrznych regulacjach związkowych, m.in. uchwałach przyjętych przez uprawnione do tego organy. Ponadto osoby ubiegające się o udzielenie licencji łączy określona relacja z polskim związkiem sportowym, bowiem występują one o nadanie im uprawnień do udziału we współzawodnictwie sportowym w danym sporcie. W związku z tym są świadome tego, że ich dane osobowe będą w tym zakresie przetwarzane przez polski związek sportowy.

8.4. WYKONYWANIE ZADANIA REALIZOWANEGO W INTERESIE PUBLICZNYM

Dodatkowo warto rozważyć zastosowanie przesłanki wynikającej z art. 6 ust. 1 lit. e RODO, czyli przetwarzania danych **w celu wykonania zadania realizowanego w interesie publicznym**. Zgodnie z art. 7 ust. 1 ustawy o sporcie polski związek sportowy może być utworzony w celu organizowania i prowadzenia współzawodnictwa w danej dyscyplinie sportu. Utworzenie polskiego związku sportowego wymaga uzyskania zgody ministra właściwego ds. kultury fizycznej. W sprawach nieuregulowanych w ustawie o sporcie do polskiego związku sportowego stosuje się przepisy ustawy z dnia 7 kwietnia 1989 r. – Prawa o stowarzyszeniach. Wydaje się, że można byłoby przyjąć, iż monopol przyznany polskim związkom sportowym w zakresie uprawnień wynikających z art. 13 ustawy stanowi swego rodzaju delegowanie na polskie związki sportowe zadań, których realizacja służy interesowi publicznemu. Argumentem przemawiającym za przyjęciem tego rozwiązania może być również fakt sprawowania szczególnego nadzoru nad działalnością polskiego związku sportowego przez ministra właściwego ds. kultury fizycznej. Podkreślenia wymaga, że tego typu nadzorem nie są objęte inne organizacje sportowe, takie jak kluby sportowe czy związki sportowe działające na poziomie regionalnym. Polski związek sportowy jako jedyna organizacja została wyposażona w określone uprawnienia i jednocześnie jako jedyna organizacja podlega specjalistycznemu nadzorowi. Stosownie do treści art. 29 ust. 1 ustawy o sporcie minister właściwy ds. kultury fizycznej może dofinansować uprawianie lub organizowanie sportu oraz jego promocję. Fakt wykonywania zadań publicznych przez polski związek sportowy został potwierdzony w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 6 marca 2013 r. Zgodnie z nim polski związek

sportowy jest podmiotem wykonującym zadania publiczne, o których mowa w art. 4 ust. 1 pkt 5 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej⁴⁹.

8.5. ZAWARCIE I REALIZACJA UMOWY

Ostatnią przesłanką, która może być również rozważana w procesie licencjonowania, jest przesłanka wynikająca z art. 6 ust. 1 lit b RODO, tj. **zawarcie i realizacja umowy**. Oparcie przetwarzania danych osobowych na tej przesłance wymagałoby jednak przyjęcia koncepcji, że wydawane przez polskie związki sportowe licencje mają charakter umowy, w której polski związek sportowy zobowiązuje się do organizowania współzawodnictwa w danej dziedzinie sportu i umożliwia w nim udział określonym osobom, natomiast osoby te zobowiązują się do spełnienia określonych zasad, przestrzegania wymagań określonych w stosowanych regulacjach wewnętrznych polskiego związku sportowego, w tym w wielu wypadkach do uiszczenia stosownej opłaty z tym związanej. Ponieważ przyjęcie powyższego rozwiązania może powodować daleko idące konsekwencje prawne, zarówno dla polskich związków sportowych, jak i osób ubiegających się o licencję lub ją otrzymujących, skorzystanie z powyższego rozwiązania wymaga pogłębionej analizy prawnej w zakresie możliwości zakwalifikowania licencji jako umowy.

⁴⁹ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 6 marca 2013 r., sygn. akt II SAB/Wa 1/13.

9. INSPEKTOR OCHRONY DANYCH (IOD)

9.1. KIM JEST INSPEKTOR OCHRONY DANYCH?

Inspektor ochrony danych to osoba wyznaczona przez organizację, której głównym zadaniem jest dbanie o zgodność przetwarzania danych osobowych z przepisami dotyczącymi ochrony danych, takimi jak RODO. Inspektor pełni funkcję doradczą i nadzorczą w zakresie ochrony danych osobowych, wspierając organizację w przestrzeganiu odpowiednich przepisów oraz zapewniając, że prawa osób, których dane dotyczą, są chronione. IOD zobowiązany jest do zachowania tajemnicy lub poufności co do wykonywanych przez siebie zadań. Inspektorem ochrony danych nie może być osoba prawna, np. spółka. Zawsze musi to być konkretna osoba fizyczna.

9.2. OBOWIĄZEK WYZNACZENIA IOD

ART. 37 RODO. WYZNACZENIE INSPEKTORA OCHRONY DANYCH

„1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

- a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
- c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.
4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.
5. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 39.
6. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
7. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy”.

Obowiązek wyznaczenia inspektora ochrony danych nie dotyczy wszystkich podmiotów przetwarzających dane osobowe. Jest on ograniczony do konkretnych grup podmiotów wskazanych w RODO oraz ustawie o ochronie danych osobowych. Istotne jest to, że obowiązek ten dotyczy zarówno administratorów danych, jak i podmiotów przetwarzających dane. Co do zasady związki i kluby sportowe nie są zobowiązane do wyznaczenia inspektora ochrony danych osobowych. RODO przewiduje powołanie takiego inspektora w sytuacji, w której przetwarzania danych dokonuje organ lub podmiot publiczny. Związki i kluby sportowe nie są takim organem, co oznacza, że wspomniany obowiązek ich nie dotyczy. Warto jednak wspomnieć, że nie jest to jedyny katalog podmiotów, które muszą wyznaczyć inspektora.

Inspektor musi być powołany również w przypadkach, gdy główna działalność administratora lub podmiotu przetwarzającego polega na:

- ▶ operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
- ▶ przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO) oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych (art. 10 RODO).

Główna działalność administratora danych lub podmiotu przetwarzającego oznacza działalność kluczową z punktu widzenia osiągnięcia celów administratora

lub podmiotu przetwarzającego dane, która jest nierozzerwalnie związana z przetwarzaniem danych osobowych. Zatem, jeżeli główną działalnością klubu sportowego jest organizowanie i prowadzenie zajęć sportowych, uczestnictwo w zawodach i turniejach, szkolenie i rozwój zawodników, a prowadzenie tej działalności nie jest możliwe bez przetwarzania danych osobowych, to potencjalnie należałoby uznać, że taki klub jest zobowiązany do powołania inspektora ochrony danych. Co jednak istotne, aby taki obowiązek istniał, konieczne jest spełnienie dodatkowych kryteriów, tj. musi być spełniona przesłanka przetwarzania danych osobowych na tzw. dużą skalę, jak również musi dochodzić do tzw. regularnego i systematycznego monitorowania osób, których dane są przetwarzane.

RODO nie zawiera definicji „dużej skali”. Przetwarzanie danych osobowych na dużą skalę odnosi się do sytuacji, w której przetwarzanie obejmuje dużą liczbę danych lub dotyczy znacznej liczby osób. Czynniki, które mogą wskazywać na przetwarzanie danych osobowych na dużą skalę, to:

- ▶ **ilość przetwarzanych danych** (przetwarzanie dotyczy dużych ilości danych osobowych, np. milionów rekordów);
- ▶ **zakres geograficzny przetwarzania** (dane przetwarzane są w wielu różnych lokalizacjach geograficznych, np. w ramach ogólnopolskiej organizacji sportowej);
- ▶ **liczba osób, których dane dotyczą** (przetwarzanie obejmuje dane bardzo dużej liczby osób, np. dane zawodników grających w piłkę nożną w klubach zrzeszonych w ramach struktury polskiego związku piłki nożnej w całej Polsce);
- ▶ **czas trwania przetwarzania** (przetwarzanie, które odbywa się przez dłuższy okres, może również być uznane za przetwarzanie na dużą skalę)⁵⁰.

Podobnie RODO nie zawiera definicji „regularnego i systematycznego monitorowania” osób, których dane dotyczą. Regularne i systematyczne monitorowanie odnosi się do procesu ciągłego lub powtarzającego się obserwowania, śledzenia lub nadzorowania zachowań, działań lub lokalizacji osób. Działanie to może mieć miejsce zarówno w świecie cyfrowym (np. monitorowanie w sieci), jak i fizycznym.

PRZYKŁADY

Monitorowanie zdrowia i wydolności fizycznej zawodników – w klubach sportowych, zwłaszcza tych profesjonalnych, zawodnicy są często monitorowani pod kątem parametrów zdrowotnych i wydolnościowych. Regularnie zbierane są dane na temat ich tętna, poziomu tlenu we krwi, prędkości biegu, regeneracji po wysiłku.

⁵⁰ Zgodnie z Wytycznymi dotyczącymi inspektorów ochrony danych przyjętymi w dniu 13 grudnia 2016 r.; ostatnio zmienionymi i przyjętymi w dniu 5 kwietnia 2017 r.

Monitorowanie frekwencji i wyników treningów – kluby sportowe mogą regularnie monitorować obecność zawodników na treningach oraz ich postępy. Dane te mogą być wykorzystywane do planowania treningów, oceniania zawodników oraz dostosowywania indywidualnych programów treningowych.

Monitoring wideo w obiektach sportowych – w obiektach sportowych, takich jak stadiony czy hale sportowe, mogą być zainstalowane kamery, które monitorują zachowanie i bezpieczeństwo uczestników. Tego rodzaju monitoring może być uważany za regularny i systematyczny, jeśli obejmuje dużą liczbę osób i jest prowadzony na stałe.

Obowiązek powołania inspektora ochrony danych może zatem dotyczyć konkretnego podmiotu spełniającego wyżej omówione przesłanki. Jeżeli określony związek lub klub sportowy w ramach prowadzonych przez siebie głównych działań będzie przetwarzał dane osobowe na dużą skalę, a przetwarzanie to będzie polegało na 1) systematycznym i regularnym monitorowaniu osób, których dane osobowe są przetwarzane, albo 2) będzie dotyczyło szczególnych danych osobowych (np. danych dotyczących stanu zdrowia zawodników) lub danych dotyczących wyroków skazujących i czynów zabronionych, to taki podmiot będzie miał obowiązek powołania inspektora ochrony danych. W praktyce dotyczy to dużych związków i klubów sportowych. W pozostałych przypadkach powołanie inspektora będzie miało charakter fakultatywny i nie będzie obowiązkowe.

UWAGA!

Nawet jeśli powołanie inspektora ochrony danych nie jest obowiązkowe, warto rozważyć podjęcie takich działań z uwagi na wiele korzyści, jakie może to przynieść organizacji, takich jak wzrost zaufania wśród zawodników i opiekunów prawnych niepełnoletnich zawodników, zapewnienie profesjonalnego wsparcia w zakresie zgodności z przepisami prawa, zapewnienie skutecznej reakcji na incydenty bezpieczeństwa. Powołanie inspektora ochrony danych jest więc strategiczną decyzją, która może przyczynić się do lepszego zarządzania ryzykiem, poprawy procesów wewnętrznych oraz budowania pozytywnego wizerunku organizacji.

9.3. KWALIFIKACJE INSPEKTORA OCHRONY DANYCH

Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie

ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Poziom wiedzy inspektora powinien być ustalany w kontekście konkretnych potrzeb administratora danych i procesora⁵¹. Jak wskazuje Grupa Robocza Art. 29, wymagany poziom wiedzy fachowej nie jest jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach organizacji.

Fachowa wiedza IOD obejmuje m.in. znajomość:

- ▶ przepisów prawa dotyczących danych osobowych (RODO, przepisów krajowych oraz innych przepisów unijnych) oraz praktyk dotyczących jego stosowania;
- ▶ branży sportowej i podmiotów działających w tym sektorze, w tym m.in. przepisów ustawy o sporcie, wewnętrznych regulacji ustanowionych przez międzynarodowe organizacje sportowe i polskie związki sportowe w danej dyscyplinie sportowej;
- ▶ procesów przetwarzania danych osobowych oraz technologii informacyjnych i bezpieczeństwa danych.

UWAGA!

RODO nie zabrania powołania jednego inspektora ochrony danych dla kilku podmiotów. Może to być dobre rozwiązanie, w szczególności w przypadku mniejszych klubów (np. zrzeszonych w ramach jednego wojewódzkiego związku sportowego), które chcą skorzystać ze wsparcia jednego profesjonalisty, jednocześnie dzieląc między siebie koszty jego zatrudnienia. Taka osoba musi mieć rzeczywistą możliwość pełnienia przydzielonej jej funkcji i realizacji przypisanych zadań we wszystkich podmiotach, które ją powołały.

9.4. OBOWIĄZKI IOD

ART. 39 RODO. ZADANIA INSPEKTORA OCHRONY DANYCH

„1. Inspektor ochrony danych ma następujące zadania:

- a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

⁵¹ Motyw 97 RODO.

- b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
 - c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
 - d) współpraca z organem nadzorczym;
 - e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
2. Inspektor ochrony danych wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania”.

Jak widać, zakres obowiązków IOD bywa bardzo szeroki, nie może on jednak wyręczać administratora w realizacji jego zadań. Oznacza to, że obowiązki przypisane administratorowi nie powinny być cedowane na IOD. Przykładowo, to nie IOD powinien wystawiać upoważnienia do przetwarzania danych osobowych, zawierać umowy powierzenia przetwarzania danych osobowych, decydować o zgłoszeniu naruszeń do UODO i prowadzić rejestru czynności przetwarzania danych osobowych (choć w praktyce bardzo często taki obowiązek jest na niego nakładany). Ustalając zakres obowiązków IOD, należy pamiętać o tym, że nie może on dokonywać czynności, które następnie będą podlegały jego monitorowaniu albo będą stanowiły przedmiot podejmowanych przez niego decyzji, co z kolei może powodować konflikt interesów.

UWAGA!

IOD nie ponosi odpowiedzialności osobistej za niezgodność z wymogami RODO. Zapewnienie zgodności z przepisami prawa w zakresie przetwarzania danych osobowych spoczywa na administratorze i podmiocie przetwarzającym.

9.5. JAKIE OBOWIĄZKI WOBEC INSPEKTORA OCHRONY DANYCH MA ORGANIZACJA?

ART. 38 RODO. STATUS INSPEKTORA OCHRONY DANYCH

- „1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów”.

Podstawowym obowiązkiem organizacji powołującej IOD jest zapewnienie mu wsparcia w realizowanych przez niego zadaniach. W zależności od wielkości i struktury organizacji podmiot, który powołuje IOD, powinien wyposażyć go w odpowiednie zasoby, które umożliwią mu realizację przypisanych zadań. IOD powinien mieć zapewniony odpowiedni czas na wykonywanie swojej pracy, powinien być wyposażony w odpowiednią infrastrukturę i posiadać odpowiednie wsparcie innych osób zatrudnionych w organizacji. Podmiot powołujący IOD powinien zapewnić mu udział we wszystkich zagadnieniach związanych z ochroną danych osobowych. Pracownicy oraz współpracownicy organizacji powinni zostać powiadomieni o powołaniu IOD oraz o konieczności wsparcia jego działań, m.in. poprzez udzielanie

stosownych informacji. Realizacja obowiązków IOD wymaga współpracy w ramach organizacji. IOD nie jest odpowiedzialny za zarządzanie poszczególnymi procesami przetwarzania danych osobowych. Jego działania mają charakter wspierający i doradczy, a świadczenie profesjonalnego doradztwa bardzo często łączy się z koniecznością uzyskiwania szczegółowych danych i informacji dotyczących określonych stanów faktycznych, ale również planów i założeń.

9.6. JAK WYZNACZYĆ I ZGŁOSIĆ INSPEKTORA OCHRONY DANYCH?

Inspektorem ochrony danych może być zarówno pracownik administratora/podmiotu przetwarzającego, jak i tzw. osoba z zewnątrz, zatrudniona np. na podstawie umowy-zlecenia lub umowy na świadczenie usług. Podmiot, który wyznaczył inspektora ochrony danych, zobowiązany jest do udostępnienia imienia i nazwiska oraz adresu poczty elektronicznej lub numeru telefonu inspektora na swojej stronie internetowej. Jeżeli administrator lub podmiot przetwarzający nie prowadzi własnej strony, udostępnia informacje o IOD w sposób ogólnie dostępny w miejscu prowadzenia działalności. Dane inspektora w powyższym zakresie muszą być przekazane również Prezesowi UODO⁵².

Zgłoszenia inspektora dokonuje się w formie elektronicznej poprzez stronę internetową Urzędu Ochrony Danych Osobowych. Należy to zrobić w terminie 14 dni od powołania. Wskazówki dotyczące zgłoszenia oraz linki do formularzy zgłoszeniowych dostępne są pod adresem: <https://uodo.gov.pl/pl/499/2443>.

Wyznaczanie IOD może odbywać się na podstawie oświadczenia złożonego zgodnie z zasadami reprezentacji danego klubu lub związku sportowego, np. poprzez zarządzenie lub uchwałę zarządu. Nic nie stoi na przeszkodzie, aby wyznaczenie IOD nastąpiło poprzez zawarcie umowy o pracę, umowy-zlecenia lub umowy cywilnoprawnej.

9.7. NIEZALEŻNOŚĆ I KONFLIKT INTERESÓW

Bez względu na to, czy inspektorem ochrony danych jest pracownik, czy osoba z zewnątrz, IOD powinien być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny⁵³. Podlega on bezpośrednio najwyższemu kierownictwu organizacji,

⁵² UODO, *Czy można powołać więcej niż jednego IOD?*, <https://uodo.gov.pl/pl/495/2401> [dostęp: 7.07.2025].

⁵³ Motyw 97 RODO.

czyli członkom zarządu. IOD nie może otrzymywać instrukcji co do wykonywania przypisanych mu zadań. Istnieje zakaz odwołania lub karania IOD za realizację przypisanych mu zadań.

Zgodnie z RODO IOD może wykonywać „inne zadania i obowiązki” z zastrzeżeniem, że nie powodują one konfliktu interesów. Konflikt interesów występuje, jeśli nie można pogodzić prawidłowego wykonywania zadań IOD z realizacją innych zadań, gdyż pomiędzy nimi występuje sprzeczność uniemożliwiająca ich odpowiednią realizację. Konflikt interesów może być również rezultatem nadmiaru obowiązków przydzielonych do wykonania IOD, jeśli musi on wybierać między obowiązkami, które będzie realizował, a tymi, którym nie podoła z powodu braku czasu koniecznego na ich wykonanie⁵⁴. IOD nie powinien pełnić żadnej funkcji, która bezpośrednio wpływa na decyzje dotyczące przetwarzania danych osobowych, aby mógł działać w sposób niezależny i zgodny z zasadami RODO.

PRZYKŁAD

Inspektor Ochrony Danych nie powinien być zatrudniony na następujących stanowiskach:

- ▶ dyrektor, np. sportowy,
- ▶ kierownik działu IT,
- ▶ dyrektor finansowy lub główny księgowy,
- ▶ kierownik działu HR,
- ▶ kierownik działu prawnego,
- ▶ menedżer ds. marketingu,
- ▶ członek zarządu,

oraz na innych niższych stanowiskach, jeśli przypisany im zakres obowiązków wiąże się z udziałem w określaniu celów i sposobów przetwarzania danych⁵⁵.

⁵⁴ UODO, Czy można łączyć funkcję IOD z zadaniami związanymi z obsługą wniosków od sygnalistów?, <https://uodo.gov.pl/pl/495/2415> [dostęp: 7.07.2025].

⁵⁵ Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r.; zmienione i przyjęte w dniu 5 kwietnia 2017 r.

10. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

ART. 29 RODO. PRZETWARZANIE Z UPOWAŻNIENIA ADMINISTRATORA LUB PODMIOTU PRZETWARZAJĄCEGO

„Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego”.

Upoważnienie do przetwarzania danych osobowych oznacza formalne nadanie uprawnień konkretnej osobie do przetwarzania danych w imieniu administratora danych. Osoby działające na podstawie upoważnienia mogą wykonywać operacje na danych osobowych, takie jak zbieranie, modyfikowanie czy odczytywanie, zgodnie z wytycznymi i poleceniami administratora.

Przepisy RODO nie wskazują wprost na obowiązek nadawania upoważnień, jednakże nie ulega wątpliwości, że dane osobowe mogą być przetwarzane wyłącznie na polecenie administratora. Takie polecenie może być wyrażone właśnie w formie upoważnienia do przetwarzania danych osobowych. Obowiązek nadawania upoważnień może również wynikać z określonych przepisów prawa, np. Kodeksu pracy.

Zasadniczo forma upoważnienia może być dowolna, z wyjątkiem sytuacji, w których przepisy prawa wymagają zachowania formy pisemnej. Zgodnie z Kodeksem pracy do przetwarzania szczególnych kategorii danych osobowych, takich jak dane o stanie zdrowia pracownika lub osoby ubiegającej się o pracę, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez pracodawcę (art. 22^{1b} § 3 Kodeksu pracy). Jednocześnie jednak zgodnie ze stanowiskiem UODO nadawanie upoważnień w postaci elektronicznej należy uznać za spełnienie obowiązku nadania upoważnień w formie pisemnej.

Pozostałe upoważnienia mogą przyjąć formę pisemną, elektroniczną, a nawet ustną, chociaż w praktyce, ze względu na zasadę rozliczalności, najczęściej stosuje się formę pisemną lub rodzaj formy elektronicznej. Upoważnienie może być odrębnym dokumentem lub stanowić część umowy, np. umowy zawartej ze zleceniobiorcą. Ważne jest,

aby organizacja ewidencjonowała wydawane przez siebie upoważnienia i wiedziała, komu i w jakim zakresie zostały one wydane (patrz: Zasada rozliczalności).

W upoważnieniu powinien być określony zakres oraz czas, w jakim osoba będzie uprawniona do przetwarzania danych osobowych. Zakres upoważnienia powinien być dostosowany do roli i obowiązków danej osoby w organizacji, np. osoba odpowiedzialna za zatrudnienie może mieć dostęp do danych kadrowych, podczas gdy osoba realizująca eventy sportowe będzie miała dostęp do danych kontrahentów realizujących usługi w ramach eventu lub uczestników wydarzenia. Zakres upoważnienia może wynikać z zakresu obowiązków danej osoby albo być wprost wskazany w upoważnieniu, np. poprzez wymienienie procesów przetwarzania danych osobowych, w które dana osoba jest zaangażowana, takich jak zawieranie umów na świadczenie usług z podwykonawcami, albo poprzez wskazanie konkretnego zbioru danych, np. dane osobowe zawodników, uczestników eventów, rodziców i opiekunów prawnych niepełnoletnich zawodników. Upoważnienie nadaje się na czas trwania stosunku prawnego (np. umowy o pracę, umowy współpracy) albo realizacji konkretnych obowiązków służbowych.

11. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

ART. 28 RODO. PODMIOT PRZETWARZAJĄCY

Powierzenie przetwarzania danych osobowych polega na przekazaniu danych osobowych innemu podmiotowi, który przetwarza je na polecenie administratora, w celach przez niego określonych, zgodnie z przekazanymi przez niego instrukcjami.

Uprawnienia i obowiązki podmiotu przetwarzającego (patrz: Podmiot przetwarzający) powinny zostać wskazane w umowie powierzenia przetwarzania danych osobowych, która musi zawierać elementy wymagane przez art. 28 RODO. Jednocześnie – jak wskazuje EROD – umowa o powierzeniu danych nie powinna ograniczać się do powtórzenia przepisów RODO: powinna zawierać bardziej szczegółowe, konkretne informacje na temat sposobu spełnienia wymogów i poziomu ochrony wymaganego do przetwarzania danych osobowych, które jest przedmiotem umowy o przetwarzaniu⁵⁶.

UWAGA!

Umowa może być zawarta w formie pisemnej (podpisana własnoręcznie lub podpisem kwalifikowanym) lub dokumentowej (tj. takiej, w której złożenie oświadczenia woli następuje w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie).

Główne elementy umowy powierzenia przetwarzania danych osobowych to⁵⁷:

- ▶ przedmiot przetwarzania, np. dokumentacja pracownicza, lista mailingowa odbiorców newslettera, rejestr zawodników;

⁵⁶ Wytyczne EROD nr 7/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO.

⁵⁷ Opracowano w oparciu o Wytyczne EROD nr 7/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO.

- ▶ czas trwania przetwarzania, np. przez okres obowiązywania umowy głównej na świadczenie usługi hostingu;
- ▶ charakter przetwarzania, czyli rodzaj operacji wykonywanych w ramach przetwarzania, np. zbieranie danych, nagrywanie, tworzenie kopii zapasowych, i cel, np. w celu realizacji usługi określonej w umowie głównej;
- ▶ rodzaj danych, np. dane kontaktowe;
- ▶ kategorie osób, których dane dotyczą, np. zawodnicy, pracownicy;
- ▶ obowiązki i prawa administratora;
- ▶ administrator danych powinien być uprawniony do wydawania instrukcji dotyczących przetwarzania danych przez podmiot przetwarzający. Umowa powinna jasno określać, że podmiot przetwarzający może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora. Instrukcje mogą być przekazywane w umówiony sposób. Instrukcje mogą być zawarte w umowie powierzenia przetwarzania danych osobowych. Mogą być również w trakcie obowiązywania umowy dodatkowo przesyłane mailem czy w każdej innej udokumentowanej formie. Powinny być również archiwizowane (patrz: Zasada rozliczalności).

UWAGA!

Jeżeli podmiot przetwarzający wykracza poza instrukcje administratora, w tym decyduje o celach i sposobach przetwarzania powierzonych mu danych osobowych, oprócz tego, że narusza swoje obowiązki, to dodatkowo może być uznany za odrębnego administratora.

- ▶ administrator danych powinien mieć prawo do przeprowadzenia audytu lub inspekcji w celu sprawdzenia zgodności działań podmiotu przetwarzającego z umową i przepisami dotyczącymi ochrony danych osobowych;
- ▶ obowiązki podmiotu przetwarzającego:
- ▶ podmiot przetwarzający zobowiązuje się do zapewnienia, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub są objęte odpowiednim ustawowym obowiązkiem zachowania poufności;
- ▶ podmiot przetwarzający musi zapewnić odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych. Środki wdrożone przez podmiot przetwarzający powinny być zgodne instrukcjami administratora. Umowa powinna zawierać obowiązek podmiotu przetwarzającego uzyskania zgody administratora na ich zmianę oraz obowiązek regularnego ich przeglądu w taki sposób, żeby były one adekwatne w odniesieniu do występującego ryzyka;

- ▶ podmiot przetwarzający powinien zobowiązać się do wspierania administratora danych w wywiązywaniu się z obowiązków dotyczących praw osób, których dane dotyczą. Zakres wsparcia może być różny (w zależności od działalności powierzonej podmiotowi przetwarzającemu) i może polegać np. na niezwłocznym przekazywaniu każdego żądania, udzielaniu niezbędnych informacji czy nawet zarządzaniu indywidualnymi żądaniami.

UWAGA!

Niezależnie od zakresu wsparcia podmiotu przetwarzającego to administrator ponosi odpowiedzialność za realizację praw osób, których dane dotyczą (patrz: Prawa osób).

- ▶ podmiot przetwarzający powinien zobowiązać się do niezwłocznego informowania administratora danych o wszelkich naruszeniach ochrony danych osobowych, które mogą mieć wpływ na przetwarzane dane. Podmiot przetwarzający zobowiązany jest również do pomocy administratorowi w realizacji innych jego obowiązków (m.in. powiadamianiu organu nadzorczego i osób, których dane dotyczą o naruszeniu ochrony danych, przeprowadzeniu oceny skutków dla ochrony danych osobowych);
- ▶ podmiot przetwarzający ma ponadto obowiązek informować administratora, jeżeli jego zdaniem wydane przez administratora instrukcje dotyczące przetwarzania danych osobowych naruszają obowiązujące w tym zakresie przepisy prawa;
- ▶ podpowierzenie przetwarzania danych – umowa powinna określać zasady dotyczące angażowania innych podmiotów przetwarzających (patrz: Podmiot przetwarzający);
- ▶ zasady poufności – umowa powinna zawierać zapisy dotyczące obowiązku zachowania w poufności zarówno przekazanych podmiotowi przetwarzającemu danych osobowych, jak również stosowanych środków bezpieczeństwa;
- ▶ zakończenie umowy i usunięcie danych – umowa powinna zawierać zapisy dotyczące usunięcia lub zwrócenia danych po zakończeniu realizacji umowy. Podmiot przetwarzający musi usunąć lub zwrócić wszystkie kopie danych, chyba że co innego wynika z przepisów prawa.

12. UDOŚTĘPNIENIE DANYCH OSOBOWYCH

Udostępnienie danych osobowych polega na przekazaniu tych danych innemu podmiotowi, który będzie je przetwarzał we własnym celu i zgodnie z własnymi zasadami. W przeciwieństwie do powierzenia przetwarzania danych, gdzie przetwarzający działa na zlecenie administratora i zgodnie z jego instrukcjami, w przypadku udostępnienia podmiot, który otrzymuje dane, staje się **samodzielnym administratorem** tych danych. Oznacza to, że nowy administrator ponosi pełną odpowiedzialność za przetwarzanie danych, w tym za spełnienie wszelkich obowiązków prawnych, takich jak realizacja obowiązku informacyjnego czy zapewnienie odpowiednich środków ochrony danych. Udostępnienie danych osobowych może również nastąpić na rzecz strony trzeciej, np. osoby fizycznej, która nie stanie się administratorem danych osobowych, bo będzie je przetwarzała w celu czysto osobistym lub domowym (np. udostępnienie nagrania z monitoringu wizyjnego na wniosek osoby, której samochód został zniszczony na parkingu należącym do klubu).

Udostępnienie danych osobowych stanowi jedną z form przetwarzania danych osobowych i może nastąpić, gdy istnieje odpowiednia podstawa prawna do dokonania takiego powierzenia (patrz: **Podstawy prawne przetwarzania danych osobowych**). Najczęściej występujące podstawy to:

- ▶ zgoda osoby, której dane dotyczą, np. zgoda zawodnika na udostępnienie przez klub jego danych osobowych sponsorowi klubu celem opublikowania ich w mediach społecznościowych sponsora;
- ▶ wymóg prawny, np. udostępnienie przez klub danych osobowych pracownika celem zgłoszenia go do Zakładu Ubezpieczeń Społecznych;
- ▶ uzasadniony interes administratora danych albo strony trzeciej, np. udostępnienie nagrania z monitoringu wizyjnego na wniosek osoby fizycznej, gdy uszkodzono jej samochód stojący w zasięgu kamery należącej do klubu, chyba że działanie to dotyczyło czynu zabronionego;
- ▶ realizacja zadania w interesie publicznym, np. przekazanie danych osobowych w ramach obowiązków sprawozdawczych w przypadku realizacji zadań finansowanych ze środków z budżetu państwa, w szczególności zadań zleconych.

Obowiązek udostępnienia danych osobowych będzie wynikał z przepisów prawa, które nakazują administratorowi przekazanie określonych danych lub informacji. Udostępnienie danych w praktyce będzie odbywało się na wniosek (np. uprawnionego

organu) lub z własnej inicjatywy administratora m.in. z związku z prowadzoną przez niego działalnością.

W sytuacji, w której organ publiczny zwraca się do organizacji o udostępnienie określonych danych osobowych, co do zasady powinien wprost wskazać przepis prawa, który uprawnia go do żądania określonego rodzaju informacji, np. dokumentów, i który tym samym zobowiązuje administratora do ich udostępnienia. Praktyka w tym zakresie bywa różna. Zdarza się, że organy publiczne albo nie przywołują żadnej podstawy prawnej, albo wskazują podstawę, która co prawda uprawnia te organy do przetwarzania określonych danych, ale nie nakłada na administratora obowiązku udostępnienia takich danych. Organizacja sportowa każdorazowo przed udostępnieniem danych powinno zweryfikować otrzymany wniosek i ustalić, czy jest on zasadny.

PRZYKŁAD

Udostępnienie danych na żądanie sądu⁵⁸, udostępnienie danych na żądanie organów ścigania⁵⁹, udostępnienie danych organom podatkowym⁶⁰, udostępnienie danych Zakładowi Ubezpieczeń Społecznych⁶¹

UWAGA!

W niektórych przypadkach (takich jak stała współpraca z usługodawcą, np. hotelem, umowa sponsoringowa), zwłaszcza gdy przekazywanie danych odbywa się regularnie lub na większą skalę, warto zawrzeć umowę między administratorami. Powinna ona precyzować warunki udostępnienia danych, zakres danych, cel ich przetwarzania przez nowego administratora, a także obowiązki dotyczące ochrony danych osobowych.

Udostępnienie danych osobowych to nie to samo co prawo dostępu do danych osobowych przysługujące osobie, której dane osobowe są przetwarzane (patrz: Prawa osób). Udostępnienie danych osobowych innemu administratorowi to przekazanie danych w celu ich dalszego, niezależnego przetwarzania przez inny podmiot, natomiast prawo dostępu to prawo osoby, której dane są przetwarzane, do uzyskania informacji na temat tego, jak jej dane są przetwarzane, co służy ochronie jej prywatności i zapewnieniu zgodności z przepisami RODO.

⁵⁸ Art. 248 Kodeksu postępowania cywilnego.

⁵⁹ Art. 15 Kodeksu postępowania karnego.

⁶⁰ Art. 155 Ordynacji podatkowej.

⁶¹ Art. 88 ustawy o systemie ubezpieczeń społecznych.

12.1. JAK POWINNO SIĘ ODBYWAĆ UDOSTĘPNIENIE DANYCH OSOBOWYCH?

Udostępniając dane osobowe, należy się kierować następującymi zasadami:

- ▶ przed udostępnieniem danych należy się upewnić, że istnieje odpowiednia podstawa prawna do takiego działania (*patrz: Podstawy prawne przetwarzania danych osobowych*);
- ▶ należy dokładnie zweryfikować, komu dane mają być udostępnione, w tym sprawdzić, czy odbiorca istnieje i jest uprawniony do przetwarzania tych danych;
- ▶ udostępniane powinny być jedynie te dane, które są niezbędne do realizacji celu przetwarzania albo zgodnie z zakresem wynikającym z przepisów prawa (w przypadku kiedy udostępnienie danych wynika z obowiązku prawnego);
- ▶ udostępnienie danych powinno się odbywać w sposób zapewniający ich bezpieczeństwo, co można zrobić poprzez:
 - ▷ szyfrowanie plików zawierających dane osobowe przed ich przekazaniem drogą elektroniczną;
 - ▷ przekazywanie haseł do zaszyfrowanych plików za pośrednictwem innego kanału komunikacji, np. SMS-em lub telefonicznie;
 - ▷ używanie bezpiecznych metod przesyłania danych, np. zaufanego kuriera, systemów szyfrowanej poczty elektronicznej;
 - ▷ w przypadku przekazywania danych w formie papierowej dokumenty powinny być odpowiednio zapakowane, np. w koperty zabezpieczone przed otwarciem przez osoby nieuprawnione;
- ▶ należy prowadzić ewidencję każdego przypadku udostępnienia danych, w tym komu, w jakim zakresie i na jakiej podstawie prawnej dane zostały przekazane. W przypadku przekazywania danych mailowo, treść wiadomości oraz odpowiedź powinny być archiwizowane (*patrz: Zasada rozliczalności*);
- ▶ w przypadku braku możliwości udostępnienia danych, należy przygotować odpowiedź odmowną z uzasadnieniem.

UWAGA!

Przydatne jest przyjęcie procedury dotyczącej udostępniania danych osobowych. Formalna procedura zapewnia jasne wytyczne dla pracowników dotyczące tego, jak postępować w przypadku konieczności udostępnienia danych. Eliminuje to niepewność i zmniejsza ryzyko błędów.

13. RÓŻNICE MIĘDZY POWIERZENIEM A UDOSTĘPNIENIEM DANYCH OSOBOWYCH

UDOSTĘPNIENIE

- ▶ Przekazanie danych odrębnemu administratorowi, który będzie je przetwarzał we własnych celach, na własną odpowiedzialność, zgodnie z ustalonymi przez siebie zasadami.
- ▶ Podstawą udostępnienia jest jedna z podstaw prawnych wynikających z RODO (art. 6 lub art. 9 RODO), dodatkowo może być zawarta umowa na udostępnienie danych osobowych, nie jest to jednak obowiązek.
- ▶ Utrata kontroli nad danymi osobowymi

POWIERZENIE

- ▶ Przekazanie danych osobowych podmiotowi, który będzie je przetwarzał na zlecenie administratora, w celach przez niego ustalonych, zgodnie z jego instrukcjami.
- ▶ Podstawą przekazania jest umowa powierzenia przetwarzania danych.
- ▶ Kontrola nad danymi osobowymi – prawo żądania zwrotu danych osobowych lub ich usunięcia po zakończeniu trwania umowy powierzenia ich przetwarzania.

PRZYKŁAD

Związek sportowych w związku z zorganizowanym zgrupowaniem przekazuje dane osobowe zawodników do hotelu, w którym będą oni nocować.

Klub kieruje pracownika na wstępne, okresowe czy kontrolne badania lekarskie do jednostki służby medycyny pracy.

Klub przekazuje firmie kurierskiej informacje o odbiorcy przesyłki⁶².

PRZYKŁAD

Klub korzysta z usług:

- ▶ firmy świadczącej usługi hostingowe i dostawcy usług chmurowych;
- ▶ firmy świadczącej usługi kadrowe i płacowe;
- ▶ agencji marketingowej, która realizuje dla niego kampanie mailingowe, przetwarzając dane fanów klubu.

⁶² Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 lipca 2022 r., sygn. akt II SA/Wa 4143/21.

Polski związek sportowy udostępnia dane osobowe zawodnika do międzynarodowej organizacji sportowej w związku z organizowaniem jego udziału w międzynarodowym współzawodnictwie sportowym.

Klub sportowy udostępnia dane osobowe swoich zawodników do odpowiedniego związku sportowego w celu rejestracji zawodników, zgłaszania ich do zawodów czy przeprowadzania klasyfikacji sportowej.

Klub sportowy udostępnia dane osobowe zawodników i trenerów sponsorom, którzy wymagają takich danych w ramach umowy sponsoringowej (np. do celów marketingowych, promocyjnych czy organizacyjnych).

Związek sportowy korzysta z usług:

- ▶ firmy świadczącej usługi w zakresie bezpieczeństwa IT;
- ▶ firmy analitycznej, która oferuje usługi analizy danych dotyczących wyników sportowych i wydolności zawodników.

14. REJESTROWANIE CZYNNOŚCI I KATEGORII CZYNNOŚCI PRZETWARZANIA

ART. 30 RODO

Rejestr to dokument, w którym administrator danych lub podmiot przetwarzający dokumentuje wszystkie czynności związane z przetwarzaniem danych osobowych, które przeprowadza w swojej organizacji. Jest to forma wewnętrznej ewidencji, która służy jako narzędzie zarządzania i monitorowania procesami związanymi z przetwarzaniem danych w organizacji. Zgodnie z wymogami RODO administratorzy danych osobowych mają obowiązek prowadzić **rejestr czynności przetwarzania danych osobowych**, natomiast podmioty przetwarzające muszą prowadzić **rejestr kategorii czynności przetwarzania**.

Rejestr czynności przetwarzania oraz rejestr kategorii czynności muszą być prowadzone przez organizacje, które spełniają przynajmniej jedno z poniższych kryteriów:

- ▶ zatrudniają ponad 250 osób;
- ▶ w ich przypadku przetwarzanie danych wiąże się z ryzykiem naruszenia praw i wolności osób, których dane dotyczą;
- ▶ w ich przypadku przetwarzanie danych nie jest sporadyczne;
- ▶ w ich przypadku przetwarzane są szczególne kategorie danych osobowych lub dane dotyczące wyroków skazujących i czynów zabronionych.

W praktyce oznacza to, że nawet jeśli organizacja zatrudnia mniej niż 250 osób, może być zobowiązana do prowadzenia rejestru, jeżeli spełnia jedno z powyższych kryteriów. Jeśli organizacja przetwarza dane osobowe pracowników, zleceniobiorców, wolontariuszy lub członków, proces ten ma zazwyczaj charakter ciągły i systematyczny, co wyklucza sporadyczność. Jeśli jednak niektóre czynności przetwarzania mają charakter jednorazowy (np. jednorazowa organizacja konkursu czy eventu), mogą nie być objęte rejestrem, pod warunkiem że ryzyko naruszenia praw osób fizycznych jest mało prawdopodobne i nie obejmują one

szczególnej kategorii danych ani danych dotyczących wyroków skazujących i czynów zabronionych⁶³.

Rejestry czynności powinny zawierać m.in. następujące informacje:

- ▶ kto przetwarza dane osobowe;
- ▶ w jakim celu są one przetwarzane;
- ▶ czyje dane są przetwarzane i jaki jest ich zakres;
- ▶ komu dane są ujawniane;
- ▶ czy dane są przekazywane do państwa trzeciego lub organizacji międzynarodowych i jak są zabezpieczone (w przypadku określonej podstawy prawnej transferu);
- ▶ jak długo dane będą przetwarzane;
- ▶ jak dane są zabezpieczane.

Zakres obligatoryjnych informacji w przypadku rejestru kategorii czynności jest nieco węższy niż w rejestrze czynności, i obejmuje wskazanie:

- ▶ administratora danych;
- ▶ procesów, które są podejmowane w ramach przetwarzania danych;
- ▶ czy dane są przekazywane do państwa trzeciego lub organizacji międzynarodowych i jak są zabezpieczone (w przypadku określonej podstawy prawnej transferu).

Najczęściej rejestry te prowadzone są w formie elektronicznej (głównie w postaci tabel), co umożliwia bieżące aktualizowanie dokumentu zgodnie ze stanem faktycznym. Aktualizacja rejestrów jest konieczna w przypadku pojawienia się nowych procesów przetwarzania danych lub w sytuacji, gdy zachodzą zmiany w informacjach już umieszczonych w rejestrze. Możliwe jest także prowadzenie rejestru w formie papierowej, choć jest to mniej wygodne. Na rynku dostępne są również specjalistyczne programy i aplikacje, które ułatwiają zarządzanie danymi osobowymi zgodnie z RODO, w tym prowadzenie rejestrów.

UWAGA!

Brak prowadzenia rejestru czynności przetwarzania czy kategorii czynności przetwarzania stanowi przesłankę do nałożenia na organizację administracyjnej kary pieniężnej.

Wskazówki i wyjaśnienia dotyczące ww. rejestrów oraz przykładowe szablony rejestrów dostępne są na stronie internetowej Urzędu Ochrony Danych Osobowych⁶⁴.

⁶³ Zgodnie ze stanowiskiem Grupy Roboczej Art. 29 w sprawie wyjątków od obowiązku prowadzenia rejestru czynności przetwarzania.

⁶⁴ UODO, *Rejestrowanie czynności przetwarzania*, <https://uodo.gov.pl/pl/123/214> [dostęp: 7.07.2025].

15. OBOWIĄZEK INFORMACYJNY

ART. 13–14 RODO

Jednym z głównych obowiązków nałożonych na administratora danych osobowych przez RODO jest obowiązek informacyjny względem osoby, której dane przetwarza. Obowiązek informacyjny ma służyć temu, aby osoba, której dane są przetwarzane, wiedziała o tym, kto dlaczego i w jakim zakresie wykorzystuje jej dane osobowe, a także jakie w związku z tym przysługują jej prawa. Stanowi to gwarancję spełnienia przez administratora danych osobowych obowiązku dotyczącego realizacji uprawnień kontrolnych przyznanych osobie, której dane osobowe są przetwarzane. Można stwierdzić, że jest ono nawet kluczowe, aby osoby te mogły skorzystać z przysługujących im praw⁶⁵. Jeżeli bowiem nie wiedziałyby, przez kogo ich dane są przetwarzane i w jakim celu, to nie mogłyby skorzystać z gwarantowanych im przez przepisy RODO uprawnień.

15.1. ZAKRES PRZEKAZYWANYCH INFORMACJI

Art. 13 i 14 RODO wskazują zakres informacji, które administrator danych osobowych jest zobowiązany przekazać osobie, której dane przetwarza. Różni się on w zależności od tego, skąd dane pochodzą – czy podała je osoba, której te dane dotyczą (niezależnie od tego, w jaki sposób to się odbyło, tj. w bezpośredniej fizycznej obecności, przez formularz zgłoszeniowy, rozmowę telefoniczną itd.)⁶⁶, czy też pochodzą one z innego źródła (tj. nie bezpośrednio od osoby, której dane dotyczą, np. przez osobę trzecią, ze źródła publicznie dostępnego, z rejestrów, baz internetowych itd.).

⁶⁵ P. Litwiński, *Kara – komentarz do decyzji o nałożeniu kary finansowej na spółkę Bisnode*, „Magazyn ODO” 2019, nr 8, s. 14.

⁶⁶ E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, Komentarz do art. 13.

Jeżeli dane zostały pozyskane przez administratora danych osobowych bezpośrednio od osoby, której dotyczą, musi on przy pozyskaniu danych poinformować o:

- ▶ swojej tożsamości (tj. podać imię i nazwisko, nazwę, formę prawną oraz adres siedziby) oraz danych kontaktowych (takich jak adres korespondencyjny, adres e-mailowy, telefon kontaktowy, faks itp.);
- ▶ danych kontaktowych inspektora ochrony danych (jego adresie, adresie e-mailowym, numerze telefonu itd.), gdy został on w organizacji sportowej powołany (patrz: *Inspektor ochrony danych*), o przy czym nie jest konieczne wskazywanie jego imienia i nazwiska⁶⁷;
- ▶ celach przetwarzania danych osobowych, które powinny być wyraźne, uzasadnione i ustalone w momencie zbierania danych⁶⁸;
- ▶ podstawie prawnej przetwarzania danych osobowych – w tym zakresie wskazuje się, że podstawa prawna przetwarzania danych osobowych powinna zostać podana zgodnie z przepisami RODO, tj. z powołaniem się na odpowiednią przesłankę legalizującą przetwarzanie, wskazaną w art. 6 ust. 1 RODO (w przypadku danych zwykłych) lub art. 9 ust. 2 RODO (w przypadku szczególnych kategorii danych), ewentualnie art. 10 RODO (w przypadku przetwarzania danych o wyrokach skazujących i naruszeniach prawa)⁶⁹ (patrz: *Podstawy prawne przetwarzania danych osobowych*);
- ▶ okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu – wskazuje się, że jeżeli administrator danych osobowych jest w stanie podać konkretny okres przechowywania danych osobowych (np. dwa, trzy lata, pięć lat), to powinien to wyrazić wprost w treści obowiązku informacyjnego; jeżeli natomiast nie jest w stanie określić konkretnego terminu, powinien wskazać kryteria jego ustalenia⁷⁰ (patrz: *Zasada ograniczenia przechowywania*);
- ▶ prawach osoby, której dane dotyczą, do żądania dostępu do danych osobowych jej dotyczących, sprostowania jej danych osobowych, usunięcia jej danych osobowych, ograniczenia przetwarzania jej danych osobowych, przeniesienia jej danych osobowych, przy czym należy wskazać, że prawo do usunięcia, ograniczenia przetwarzania, a także przeniesienia danych osobowych nie przysługuje osobie w każdej sytuacji, ale w przypadkach wskazanych w przepisach prawa, w szczególności przepisach RODO (patrz: *Prawa osób, których dane są przetwarzane*);
- ▶ prawie do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych – zgodnie z przepisami RODO osoba, której dane dotyczą,

⁶⁷ Tak też: *ibidem*.

⁶⁸ Motyw 39 RODO.

⁶⁹ E. Bielak-Jomaa, D. Lubasz (red.), *RODO...*, *op.cit.*

⁷⁰ Decyzja PUODO z dnia 6 kwietnia 2019 r., ZSPU.421.2.2018.

może wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim stanowiącym miejsce jej zwykłego pobytu (miejsce zamieszkania), miejsca pracy lub miejsca popełnienia zarzucanego naruszenia ochrony danych;

- ▶ tym, czy podanie danych osobowych jest wymogiem ustawowym (obowiązek prawny podania/przetwarzania danych został wskazany w przepisach prawa, np. Kodeksie pracy odnośnie do danych zbieranych w kwestionariuszu osobowym pracownika) lub umownym (tj. niezbędnym do realizacji umowy pomiędzy administratorem danych osobowych a osobą, której dane dotyczą) albo warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania, a także jakie są ewentualne konsekwencje niepodania danych (np. niemożliwość zawarcia lub realizacji umowy itd.); w przypadku wykorzystywania przez administratorów danych osobowych formularzy internetowych powinny one w sposób jednoznaczny wskazywać, które pola są obowiązkowe, a które fakultatywne;
- ▶ jeżeli istnieją – prawnie uzasadnionych interesach realizowanych przez administratora lub stronę trzecią, jeżeli przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit. f RODO (patrz: *Uzasadniony interes administratora lub strony trzeciej*);
- ▶ jeżeli istnieją – odbiorcach danych osobowych lub kategoriach odbiorców (patrz: *Odbiorca danych*); chodzi tutaj o wszystkich innych administratorów danych osobowych, którym dane zostaną ujawnione, pozostałych współadministratorów, podmioty przetwarzające; informacje te powinny być jak najbardziej szczegółowe (np. dotyczyć rodzaju prowadzonej przez taki podmiot działalności, sektora, w którym odbiorca działa, jego lokalizacji, a nawet nazwy lub imienia i nazwiska);
- ▶ jeżeli ma zastosowanie – przekazywaniu danych osobowych do odbiorców z państw trzecich lub organizacji międzynarodowych, tj. zamiarze przekazywania danych osobowych do odbiorców z państwa trzeciego lub organizacji międzynarodowej, stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony, wzmiance o odpowiednich lub właściwych zabezpieczeniach – w przypadku przekazania danych osobowych na podstawie art. 46 RODO (standardowe klauzule ochrony danych) lub art. 49 ust. 1 akapit drugi RODO (wyjątki dopuszczające przekazanie danych) oraz informacji o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia (patrz: *Część szczegółowa. Transfer danych poza Europejski Obszar Gospodarczy*),
- ▶ w przypadku, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody – prawie do wycofania zgody w dowolnym momencie bez wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem; EROD stoi na stanowisku, że informacja ta powinna również zawierać sposób, w jaki zgoda może zostać wycofana⁷¹; w tym zakresie należy pamiętać,

⁷¹ WP-260 – Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, s. 44.

że wycofanie zgody musi być równie łatwe, jak jej wyrażenie (np. jeżeli wyrażenie zgody nastąpiło poprzez zaznaczenie checkboxa, to również poprzez odznaczenie checkboxa taka zgoda powinna móc być wycofana;

- ▶ jeżeli ma zastosowanie – zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, tj. o tym, że takie zautomatyzowane podejmowanie decyzji ma miejsce, o zasadach, zgodnie z którymi się to odbywa, oraz znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (patrz: **Prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu**);
- ▶ jeżeli dotyczy – prawie do wniesienia sprzeciwu wobec przetwarzania danych osobowych; należy również zwrócić uwagę na to, że informacja o prawie sprzeciwu wobec przetwarzania danych osobowych powinna zostać przekazana osobie, której dane dotyczą, najpóźniej przy pierwszym z nią kontakcie oraz w sposób jasny i odrębny od wszystkich innych informacji (np. poprzez wyraźne graficzne wyodrębnienie takiego komunikatu).

W przypadku, gdy dane zostały pozyskane z innego źródła (np. od kontrahenta, agenta, klubu sportowego, ze źródeł powszechnie dostępnych, takich jak KRS, CEIDG czy rejestry zawodników), należy podać informacje dotyczące:

- ▶ swojej tożsamości (tj. imię i nazwisko, nazwę, formę prawną oraz adres siedziby) oraz danych kontaktowych (np. adres korespondencyjny, adres e-mailowy, telefon kontaktowy, faks itp.);
- ▶ danych kontaktowych inspektora ochrony danych (adres, adres e-mailowy, numer telefonu itd.), gdy został on w organizacji powołany (patrz: **Inspektor ochrony danych**), przy czym nie jest konieczne wskazywanie jego imienia i nazwiska⁷²;
- ▶ celów przetwarzania danych osobowych, które powinny być wyraźne, uzasadnione i ustalone w momencie zbierania danych⁷³;
- ▶ podstawy prawnej przetwarzania danych osobowych – w tym zakresie wskazuje się, że podstawa prawna przetwarzania danych osobowych powinna zostać podana zgodnie z przepisami RODO, tj. z powołaniem się na odpowiednią przesłankę legalizującą przetwarzanie, wskazaną w art. 6 ust. 1 RODO (w przypadku danych zwykłych) lub art. 9 ust. 2 RODO (w przypadku szczególnych kategorii danych), ewentualnie art. 10 RODO (w przypadku przetwarzania danych o wyrokach skazujących i naruszeniach prawa⁷⁴ (patrz: **Podstawy prawne przetwarzania danych osobowych**);
- ▶ okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu; wskazuje się, że jeżeli administrator danych osobowych jest w stanie podać konkretny okres ich przechowywania (np. dwa,

⁷² Tak też: E. Bielak-Jomaa, D. Lubasz (red.), *RODO...*, *op.cit.*

⁷³ Motyw 39 RODO.

⁷⁴ E. Bielak-Jomaa, D. Lubasz (red.), *RODO...*, *op.cit.*

trzy lata, pięć lat), to powinien to wyrazić wprost w treści obowiązku informacyjnego; jeżeli natomiast nie jest w stanie określić konkretnego terminu, powinien wskazać kryteria jego ustalenia⁷⁵;

- ▶ kategorii danych osobowych, które zostały pozyskane; w związku z tym, że dane osobowe zostały pozyskane nie bezpośrednio od osoby, której dotyczą, może ona nie wiedzieć, jakie dotyczące jej dane osobowe administrator danych osobowych przetwarza, w związku z tym administrator danych osobowych powinien w tym zakresie udzielić stosownych informacji;
- ▶ źródła pochodzenia danych osobowych (skąd, od kogo administrator pozyskał dane), a także, gdy ma to zastosowanie, czy pochodzą one ze źródeł powszechnie dostępnych (np. baz internetowych, rejestrów publicznych itd.); administrator danych osobowych powinien podać konkretne źródło pozyskania danych, a w przypadku braku takiej możliwości, co najmniej charakter źródła – publiczne czy prywatne, a także rodzaj podmiotu/organizacji/organu/branży/sektora;
- ▶ prawa osoby, której dane dotyczą, do żądania dostępu do danych osobowych jej dotyczących, sprostowania jej danych osobowych, usunięcia jej danych osobowych, ograniczenia przetwarzania jej danych osobowych, przeniesienia jej danych osobowych, przy czym należy wskazać, że prawo do usunięcia, ograniczenia, przetwarzania, a także przeniesienia danych osobowych nie przysługuje osobie w każdej sytuacji, ale w przypadkach wskazanych w przepisach prawa, w szczególności przepisach RODO;
- ▶ prawa do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych; zgodnie z przepisami RODO osoba, której dane dotyczą, może wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim stanowiącym miejsce jej zwykłego pobytu (miejsce zamieszkania), miejsca pracy lub miejsca popełnienia zarzucanego naruszenia ochrony danych;
- ▶ prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, jeżeli przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit. f RODO;
- ▶ jeżeli istnieją – odbiorców danych osobowych lub kategorii odbiorców; chodzi tutaj o wszystkich innych administratorów danych osobowych, którym dane zostaną ujawnione, pozostałych współadministratorów, podmioty przetwarzające; informacje te powinny być jak najbardziej szczegółowe (np. dotyczyć rodzaju prowadzonej przez taki podmiot działalności, sektora, w którym odbiorca działa, jego lokalizacji, a nawet nazwy lub imienia i nazwiska);
- ▶ jeżeli ma zastosowanie – przekazywania danych osobowych do odbiorców z państw trzecich lub organizacji międzynarodowych, tj. zamiaru przekazywania danych osobowych do odbiorców z państwa trzeciego lub organizacji międzynarodowej,

⁷⁵ Decyzja PUODO z dnia 6 kwietnia 2019 r., ZSPU.421.2.2018.

stwierdzenia lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony, wzmianki o odpowiednich lub właściwych zabezpieczeniach – w przypadku przekazania danych osobowych na podstawie art. 46 RODO (standardowe klauzule ochrony danych), lub art. 49 ust. 1 akapit drugi RODO (wyjątki dopuszczające przekazanie danych) oraz sposobach uzyskania kopii tych zabezpieczeń lub miejscu ich udostępnienia (patrz: *Część szczegółowa. Transfer danych poza Europejski Obszar Gospodarczy*);

- ▶ w przypadku, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody – prawa do wycofania zgody w dowolnym momencie bez wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem; EROD stoi na stanowisku, że informacja ta powinna również zawierać sposób, w jaki zgoda może zostać wycofana⁷⁶; w tym zakresie należy pamiętać, że wycofanie zgody musi być równie łatwe, jak jej wyrażenie (np. jeżeli wyrażenie zgody nastąpiło poprzez zaznaczenie checkboxa, to również poprzez odznaczenie checkboxa taka zgoda powinna móc być wycofana);
- ▶ jeżeli ma zastosowanie – zautomatyzowanego podejmowania decyzji, w tym profilowania, o którym mowa w art. 22 ust. 1 i 4 RODO, tj. tego, że takie zautomatyzowane podejmowanie decyzji ma miejsce, zasad, zgodnie z którymi się to odbywa, oraz znaczenia i przewidywanych konsekwencji takiego przetwarzania dla osoby, której dane dotyczą (patrz: *Prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu*);
- ▶ jeżeli dotyczy – prawa do wniesienia sprzeciwu wobec przetwarzania danych osobowych; należy również zwrócić uwagę na to, że informacja o prawie sprzeciwu wobec przetwarzania danych osobowych powinna zostać przekazana osobie, której dane dotyczą, najpóźniej przy pierwszym z nią kontakcie oraz w sposób jasny i odrębny od wszystkich innych informacji (np. poprzez wyraźne graficzne wyodrębnienie takiego komunikatu).

15.2. WYŁĄCZENIA SPEŁNIANIA OBOWIĄZKU INFORMACYJNEGO

Przepisy RODO wskazują sytuacje, w których nie ma zastosowania obowiązek przekazania informacji o przetwarzaniu danych osobowych osobie, której dane dotyczą. Należy jednak pamiętać, że jak każdy wyjątek od reguły powinien być on interpretowany zawężająco, aby nie doszło do naruszenia praw i wolności osób, których dane dotyczą.

⁷⁶ WP-260 – Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, s. 44.

W przypadku, gdy dane osobowe pochodzą bezpośrednio od osoby, której dotyczą, spełnienie obowiązku informacyjnego jest wyłączone w przypadku i zakresie, w jakim osoba ta dysponuje tymi informacjami. A zatem administrator danych osobowych jest zwolniony z obowiązku przedstawienia osobie, której dane dotyczą, informacji, które osoba ta już posiada. Wskazuje się przy tym, że administrator danych osobowych może powołać się na to wyłączenie jedynie w przypadku, gdy ma pewność, że osoba, której dane dotyczą, posiada wszystkie wymagane prawem informacje.

Mając na uwadze zasadę rozliczalności, administrator danych osobowych powinien jednak być w stanie wykazać, jakie informacje i w jaki sposób osoba ta już otrzymała, czy są one kompletne, a także, czy nie nastąpiły w tym zakresie żadne zmiany. Osoba, której dane dotyczą, powinna posiadać wszystkie wymagane informacje oraz powinny być one aktualne. Jeżeli osoba posiada jedynie część wymaganych przez art. 13 informacji, administrator danych osobowych przy ich pozyskaniu powinien poinformować o pozostałych informacjach, tak aby były one kompletne.

Jednocześnie należy wskazać na wyłączenia spełniania obowiązku informacyjnego, gdy dane pochodzą z innego źródła. Przekazanie przez administratora danych osobowych wyżej wymienionych informacji nie jest konieczne w takim przypadku i zakresie, w jakim:

- ▶ osoba, której dane dotyczą, dysponuje już tymi informacjami;
- ▶ udzielenie tych informacji:
- ▶ okazuje się niemożliwe (w szczególności przy przetwarzaniu danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, do celów statystycznych); w tym zakresie administrator danych osobowych musi wskazać czynniki, które uniemożliwiają mu obiektywnie udzielenie informacji o przetwarzaniu danych osobowych osobom, których dotyczą; w przypadku, gdy stan „niemożliwości” ustanie, administrator danych osobowych powinien niezwłocznie spełnić obowiązek informacyjny;
- ▶ wymagałoby niewspółmiernie dużego wysiłku (w szczególności przy przetwarzaniu danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, do celów statystycznych)⁷⁷; w tym zakresie należy mieć na uwadze wytyczne zawarte w motywie 62 RODO, zgodnie z którym przy ocenie niewspółmiernie dużego wysiłku uwzględnić należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie

⁷⁷ Warto wskazać tutaj na jedną z bardzo głośnych spraw dotyczącą pierwszej kary nałożonej przez Prezesa Urzędu Ochrony Danych Osobowych za niespełnienie obowiązku informacyjnego przez podmiot, który zajmował się przygotowaniem raportów handlowych dotyczących przedsiębiorców. Podmiot ten powołał się na wyłączenie wynikające z art. 14 ust. 5 pkt 2 RODO, który mówi, że spełnienie tego obowiązku informacyjnego wymagałoby niewspółmiernie dużego wysiłku polegającego na ogromnych kosztach z tym związanych. Prezes Urzędu Ochrony Danych Osobowych stoi na stanowisku, że wyłączenie to nie ma w tej sprawie zastosowania. Zob.: Decyzja PUODO z dnia 15 marca 2019 r., ZSPR.421.3.2018.

przyjęte odpowiednie zabezpieczenia; EROD proponuje, aby w takim przypadku przeprowadzić test równowagi – porównać wysiłek, który musi włożyć administrator danych osobowych w spełnienie obowiązku informacyjnego ze skutkami dla osoby, której dane przetwarza, w przypadku nieprzekazania tych informacji; aby zapewnić rozliczalność, administrator danych osobowych powinien udokumentować przeprowadzoną w ten sposób ocenę⁷⁸. Wskazuje się, że „niewspółmiernie duży wysiłek” oznacza, iż wysiłek włożony w przekazanie informacji jest nieproporcjonalny i nieuzasadniony w porównaniu z celem, któremu włożony wysiłek miałby służyć⁷⁹. Wątpliwości budzi to, czy można powoływać się na przesłankę „niewspółmiernie dużego wysiłku” w przypadku kosztów, które niesie za sobą spełnienie obowiązku informacyjnego⁸⁰. Jeśli administrator danych osobowych powoła się na to wyłączenie, musi wdrożyć odpowiednie środki, aby zapewnić należytą ochronę praw i wolności osób, których dane przetwarza. W szczególności może informacje te udostępnić publicznie. Dodatkowo, mogą to być takie środki, jak: cykliczne dokonywanie oceny skutków dla ochrony danych, wprowadzenie dodatkowych zabezpieczeń, minimalizacja zakresu zbieranych danych oraz okresu ich przechowywania⁸¹; EROD stoi na stanowisku, że powołanie się na to wyłączenie jest możliwe przy spełnieniu łącznie następujących przesłanek: administrator danych osobowych musi wykazać, że samo spełnienie obowiązku informacyjnego może uniemożliwić lub poważnie utrudnić realizację celów przetwarzania, a po drugie przetwarzanie danych osobowych jest zgodne z zasadami określonymi w art. 5 RODO, a przede wszystkim – jest w całości rzetelne i ma podstawę prawną⁸²;

- ▶ mogłoby uniemożliwić lub poważnie utrudnić realizację celów przetwarzania danych osobowych;
- ▶ pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane w prawie Unii Europejskiej lub prawie danego państwa członkowskiego, któremu podlega administrator danych osobowych, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; a zatem skorzystanie z tego wyłączenia jest uzależnione od spełnienia łącznie dwóch przesłanek:

⁷⁸ WP-260 – Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, s. 13–14.

⁷⁹ M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 226–227.

⁸⁰ Sprawy tej dotyczyła pierwsza kara pieniężna nałożona przez Prezesa Urzędu Ochrony Danych Osobowych za niespełnienie obowiązku informacyjnego. Podmiot, na który została nałożona kara, powoływał się na wyłączenie obowiązku informacyjnego z uwagi na ogromne koszty realizacji tego obowiązku, a zatem „niewspółmiernie duży wysiłek” (Decyzja PUODO z dnia 15 marca 2019 r., ZSPR.421.3.2018). Zob.: P. Litwiński, *Kara...*, *op.cit.*, s. 13–17.

⁸¹ WP-260 – Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, s. 13–14.

⁸² *Ibidem*.

pozyskanie lub ujawnienie danych osobowych wynika wprost z przepisów prawa europejskiego lub przepisów prawa krajowego danego państwa członkowskiego (tj. przewiduje wprost obowiązek prawny przetwarzania określonych danych osobowych przez administratora danych osobowych), a ponadto przepisy te przewidują odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane są przetwarzane;

- ▶ dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy (np. tajemnica lekarska, tajemnica adwokacka itd.).

15.3. TERMIN PRZEKAZANIA INFORMACJI

W przypadku, gdy organizacja sportowa pozyskała dane osobowe bezpośrednio od osoby, której dane dotyczą (np. poprzez wypełnienie przez nią formularza, podanie ustnie danych, wpisanie danych w formularzu lub zgłoszeniu elektronicznym), podanie informacji powinno nastąpić **przy pozyskaniu danych osobowych**, np. poprzez wskazanie ich pod formularzem, przekazanie w formie papierowej bezpośrednio po podaniu ustnie danych osobowych, załączenie do regulaminu konkursu, regulaminu zawodów, w stopce e-maila.

W przypadku, gdy administrator pozyskał dane osobowe nie bezpośrednio od osoby, której one dotyczą, tj. z innego źródła, informacje powinny zostać przekazane w określonych terminach:

- ▶ co do zasady – w rozsądnym terminie po pozyskaniu danych osobowych, nie później niż w ciągu miesiąca od ich pozyskania;
- ▶ jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dotyczą (np. komunikacją mailową, telefoniczną, korespondencyjną) – administrator danych powinien spełnić obowiązek informacyjny przy pierwszym kontakcie, nawet jeżeli nie upłynął miesiąc od momentu pozyskania danych; w przypadku, gdy komunikacja nastąpi później, zastosowanie ma zasada ogólna, a zatem informacje o przetwarzaniu danych osobowych powinny zostać przekazane nie później niż w terminie miesiąca od pozyskania danych;
- ▶ jeżeli planuje się ujawnić dane osobowe innemu odbiorcy (**patrz: Odbiorca danych**) – najpóźniej przy ich pierwszym ujawnieniu; w tym zakresie należy wskazać, że ogólny termin miesiąca od pozyskania danych nie będzie miał zastosowania, gdy ujawnienie danych nastąpi w krótszym terminie niż termin ogólny (tj. przed upływem miesiąca), w tym przypadku, informacje powinny zostać przekazane najpóźniej przy pierwszym ujawnieniu danych.

15.4. SPOSÓB SPEŁNIANIA OBOWIĄZKU INFORMACYJNEGO

Mając na uwadze zasadę przejrzystości, organizacja sportowa jako administrator danych powinna przekazać informacje o przetwarzaniu danych osobowych osobom, których dane wykorzystuje, przy uwzględnieniu następujących kwestii:

- ▶ informacje muszą zostać podane w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie;
- ▶ informacje powinny być konstruowane za pomocą w miarę możliwości jasnego i prostego języka, w szczególności jeżeli kierowane są do dzieci;
- ▶ należy unikać niezrozumiałych sformułowań oraz zbyt skomplikowanego, specjalistycznego języka, zdań wielokrotnie złożonych;
- ▶ informacje powinny zostać wyodrębnione od innych informacji, np. postanowień umownych, ogólnych warunków umów, treści pism itd. Najlepszym rozwiązaniem jest zaznaczenie wprost, że dane informacje stanowią informacje o przetwarzaniu danych, np. poprzez nadanie odpowiedniego tytułu typu „Informacje dotyczące przetwarzania danych osobowych”, „Klauzula informacyjna związana z przetwarzaniem danych osobowych”, „Obowiązek informacyjny”, oraz wyodrębnienie tych informacji graficznie od innych postanowień;
- ▶ informacje powinny być łatwo dostępne dla osób, do których są kierowane. Taka osoba nie powinna być zobowiązana do poszukiwania tych informacji. Może to nastąpić poprzez bezpośrednie przekazanie jej wszystkich informacji (np. w formie pisemnego oświadczenia, wiadomości e-mail), podanie linka do tych danych, warstwowej informacji o polityce prywatności czy też – w przypadku elektronicznego pozyskiwania danych – bezpośrednio na stronie, na której dane są zbierane, za pomocą wyskakującego okienka, z którym dana osoba powinna się zapoznać, lub potwierdzenia zapoznania się z informacjami przed dokonaniem zakupu, zarejestrowaniem się do panelu użytkownika itd. W tym zakresie kluczowe znaczenie ma wyrażenie zawarte w art. 13 i 14 RODO, zgodnie z którym administrator danych osobowych „podaje” osobie, której dane dotyczą, określone w przepisach informacje. A zatem to administrator danych osobowych powinien podjąć aktywne działanie, aby przekazać informacje o przetwarzaniu danych osobowych. Należy więc uznać za nieprawidłowe zamieszczanie informacji o przetwarzaniu danych osobowych jedynie na stronie internetowej, bez poinformowania osób, których dane dotyczą, o tym, że mogą tam te informacje znaleźć. W szczególności dana osoba może nie spodziewać się, że jej dane osobowe są przetwarzane przez określony podmiot, a co za tym idzie, trudno oczekiwać, żeby tych informacji poszukiwała na jego stronie internetowej.

W tym zakresie warto podkreślić możliwość warstwowego spełniania obowiązku informacyjnego⁸³. Najważniejsze informacje, takie jak tożsamość i dane kontaktowe administratora danych osobowych, cele przetwarzania oraz informacja o prawach przysługujących osobie, której dane dotyczą, powinny być spełnione w pierwszej warstwie informacyjnej⁸⁴. Pozostałe informacje mogą zostać zamieszczone w drugiej lub kolejnej warstwie informacyjnej, jednak łatwo dostępnej, np. na stronie internetowej w określonej zakładce czy też pod określonym linkiem. W przypadku komunikacji prowadzonej za pomocą poczty elektronicznej dobrym rozwiązaniem jest zamieszczenie pierwszej podstawowej warstwy informacyjnej w stopce maila wraz z odnośnikiem do pozostałych informacji. W tym zakresie należy wskazać dokładną ich lokalizację tak, aby była ona łatwo dostępna dla osób, które chcą się z nią zapoznać. W przypadku komunikacji telefonicznej możliwe jest przekazanie podczas rozmowy jedynie najważniejszych informacji, o których mowa powyżej, a w pozostałym zakresie odesłanie do polityki prywatności zamieszczonej na stronie internetowej, przesłanie informacji na adres e-mailowy lub linka odsyłającego do tych informacji. Spotykaną praktyką jest również nagranie lub zapewnienie możliwości odsłuchania nagranej wcześniej informacji o przetwarzaniu danych osobowych.

Należy również wskazać, że często to nie sam administrator danych osobowych realizuje obowiązek informacyjny, ale ktoś w jego imieniu, np. członkowie zarządu (działający w imieniu spółki), upoważnieni pracownicy⁸⁵, jeden ze współadministratorów, który został do tego zobowiązany w drodze wspólnych uzgodnień, ale również inny podmiot (np. kontrahent), który na podstawie zawartej z administratorem danych osobowych umowy zobowiązał się do zrealizowania w jego imieniu obowiązku informacyjnego np. w stosunku do swoich pracowników, których dane administrator posiada w celu realizacji umowy z tym kontrahentem.

Mając na uwadze zasadę rozliczalności, administrator danych osobowych powinien być w stanie wykazać, że spełnił w określony sposób obowiązek informacyjny (np. poprzez wskazanie treści polityki prywatności zamieszczonej na stronie internetowej, archiwizacji informacji mailowych, archiwizacji dokumentacji i oświadczeń w tym zakresie, wykorzystywanych formularzy itd.).

⁸³ Tak również: D. Karwala, A. Szczygieł, *Podejście warstwowe sposobem na realizację obowiązku informacyjnego*, „Magazyn ODO” 2019, nr 6, s. 49–52.

⁸⁴ Ministerstwo Cyfryzacji, *RODO. Poradnik dla sektora FinTech*, <https://www.gov.pl/documents/31305/0/RODO+-+FinTech-ma%C5%82y.pdf/372bd1d0-feb6-3473-9ea1-3c7de0a001b7> [dostęp: 21.10.2024].

⁸⁵ P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Komentarz do art. 13.

15.5. AKTUALIZACJA OBOWIĄZKU INFORMACYJNEGO

Przepisy RODO wskazują wprost sytuację, w której konieczne jest ponowne spełnienie obowiązku informacyjnego. Dotyczy to zmiany celu przetwarzania w stosunku do celu, w którym dane zostały pierwotnie zebrane. W takim przypadku administrator danych osobowych **przed przystąpieniem do takiego dalszego przetwarzania** powinien poinformować osobę, której dane dotyczą, o tym innym celu (np. dane zebrane w celach realizacji umowy mają być wykorzystywane do celów marketingu bezpośredniego).

Analogiczna sytuacja będzie miała miejsce w sytuacji, gdy zdezaktualizuje się którakolwiek z informacji, które zostały wcześniej przekazane. Może to dotyczyć przykładowo danych kontaktowych, tożsamości administratora danych osobowych (np. w przypadku zmiany nazwy, przekształcenia itd.), podstawy prawnej przetwarzania, okresu przechowywania danych osobowych itd.

16. OCHRONA DANYCH W FAZIE PROJEKTOWANIA I DOMYŚLNA OCHRONA DANYCH

ART. 25 RODO

„1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać m.in. poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42”.

16.1. ZASADA *PRIVACY BY DESIGN*

Przepisy RODO nakładają na administratora obowiązki związane z tym, aby uwzględniać kwestie dotyczące ochrony danych osobowych nie tylko na etapie, kiedy już są przetwarzane, ale także przed rozpoczęciem danego przetwarzania.

Głównym obowiązkiem z tym związanym jest wdrożenie odpowiednich środków i niezbędnych zabezpieczeń tak, aby zapewnić skuteczną realizację zasad przetwarzania danych osobowych (patrz: *Ogólne zasady przetwarzania danych osobowych*) oraz praw i wolności osób, których dane są przetwarzane.

Administrator powinien uwzględniać aspekty związane z ochroną danych osobowych w fazie projektowania, tj. przed wprowadzeniem nowego procesu przetwarzania, nowej usługi, produktu czy programu, a także w ramach monitorowania i przeglądu skuteczności już istniejących procesów przetwarzania danych osobowych⁸⁶. Obowiązek ten dotyczy wszystkich organizacji sportowych, które są administratorami, niezależnie od ich wielkości oraz tego, jak skomplikowane i złożone są procesy przetwarzania, które realizują.

Co ważne, należy przy tym uwzględnić:

- ▶ stan wiedzy technicznej i postępu w zakresie technologii (jakie są obecnie systemy i zabezpieczenia stosowane na rynku, które zapewnią bezpieczeństwo przetwarzanych danych osobowych, jakie nowe rozwiązania są wprowadzane w związku z postępowaniem technologicznym, jakie nowe zagrożenia pojawiają się w związku z przetwarzaniem danych osobowych; przy czym nie jest konieczne, aby organizacja sportowa korzystała z najnowszych, innowacyjnych środków bezpieczeństwa, ponieważ ich dostępność może być ograniczona lub może być to poza możliwościami finansowymi organizacji, ale powinno to skłaniać organizację do tego, aby nie korzystać z rozwiązań przestarzałych, które nie odpowiadają aktualnym zagrożeniom dla ochrony danych⁸⁷);
- ▶ koszt wdrożenia tych środków (czy można wdrożyć rozwiązania mniej kosztowne, ale które zapewnią odpowiednie bezpieczeństwo danych osobowych, przy czym sam koszt wdrożenia nie może być podstawą do odstąpienia od wdrożenia danego zabezpieczenia⁸⁸);
- ▶ charakter, zakres, kontekst i cele przetwarzania (czyje oraz jakie dane będą przetwarzane, czy dotyczy to też danych szczególnych kategorii, jak dużo danych będzie przetwarzanych, w jakim celu dane będą przetwarzane);
- ▶ ryzyko naruszenia praw lub wolności osób, których dane dotyczą, o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania danych osobowych, co wiąże się z koniecznością przeprowadzenia analizy ryzyka dla danego procesu przetwarzania (patrz: *Analiza ryzyka*).

⁸⁶ Decyzja PUODO z dnia 19 stycznia 2022 r., DKN.5130.2215.2020.

⁸⁷ P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022, Komentarz do art. 25.

⁸⁸ Wytyczne EROD nr 4/2019 dotyczące art. 25. Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych, wersja 2.0, s. 9.

Na tej podstawie administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, które będą adekwatne i skuteczne⁸⁹ (takie jak np. pseudonimizacja, przeszkolenie pracowników, wdrożenie systemów wykrywających złośliwe oprogramowanie).

PRZYKŁADY WPROWADZANIA NOWYCH PROCESÓW, KTÓRE WYMAGAJĄ UWZGLĘDNIENIA OCHRONY DANYCH W FAZIE PROJEKTOWANIA

Organizacja sportowa:

- ▶ wprowadza nowy system księgowy, kadrowy, poczty elektronicznej;
- ▶ postanawia stworzyć sklep internetowy do sprzedaży gadżetów i produktów sportowych;
- ▶ zamierza wprowadzić internetową sprzedaż biletów na mecze lub organizowane turnieje;
- ▶ postanawia korzystać z przechowywania danych i informacji w chmurze;
- ▶ organizuje wraz z innymi organizacjami turniej, którego wyniki będą udostępniane w internecie, a obsługą będzie zajmować się zewnętrzny podmiot;
- ▶ postanawia wprowadzić newsletter;
- ▶ tworzy program lojalnościowy dla swoich kibiców.

UWAGA!

W przypadku, gdy organizacja sportowa zamierza skorzystać z gotowego rozwiązania, np. systemu informatycznego dostępnego na rynku, powinna zweryfikować, czy dostawca uwzględnił przy jego tworzeniu kwestie dotyczące ochrony danych osobowych. Administrator powinien bowiem korzystać z takich usług i systemów, które zapewniają realizację obowiązków wynikających z ochrony danych osobowych. Ważne jest również, czy dostawca zapewnia aktualizacje systemu tak, aby odpowiadały one aktualnej wiedzy technicznej i spełniały wymogi prawne.

16.2. ZASADA *PRIVACY BY DEFAULT*

Administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Obowiązek ten ma zapewnić

⁸⁹ Zob. decyzja PUODO z dnia 16 maja 2023 r., DKN.5131.56.2022.

zasadę minimalizacji danych (patrz: *Ogólne zasady przetwarzania danych osobowych*). Organizacja sportowa, decydując się na wprowadzenie danego procesu przetwarzania, powinna zastanowić się, jakie i czyje dane muszą zostać zebrane, żeby zrealizować zamierzony cel przetwarzania, jak długo muszą być przechowywane, a także kto powinien mieć do nich dostęp. Przyjmuje się, że co do zasady dane osobowe nie powinny być udostępniane nieokreślonej liczbie osób (np. poprzez publikację w internecie, w szczególności gdy chodzi o dzieci) bez wyraźnej interwencji ze strony osoby, której dane dotyczą.

W tym kontekście pomocne mogą być wytyczne EROD nr 4/2019 dotyczące art. 25 – Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych. Wskazują one kwestie, które należy wziąć pod uwagę przy realizacji zasady ochrony danych w fazie projektowania i domyślnej ochrony danych pod kątem zasad przetwarzania danych osobowych⁹⁰.

Organizacja sportowa powinna zatem przeprowadzić analizę projektowanego procesu i uwzględnić przede wszystkim to:

- ▶ jaki proces jest wdrażany;
- ▶ jaki jest cel wdrażanego procesu, co organizacja chce osiągnąć;
- ▶ jakie dane osobowe będą zbierane i dalej przetwarzane w ramach procesu (rodzaje danych, kategorie osób);
- ▶ jaki jest cel przetwarzania danych osobowych w ramach procesu;
- ▶ czy wszystkie dane, które mają być zbierane, są niezbędne do tego, żeby zrealizować zamierzony cel, dlaczego jest to konieczne;
- ▶ w jaki sposób dane osobowe będą pozyskiwane, skąd będą pochodzić (bezpośrednio od osoby, z innego źródła, ze źródeł publicznie dostępnych);
- ▶ na jakiej podstawie prawnej dane będą przetwarzane (patrz: *Podstawy prawne przetwarzania danych osobowych*);
- ▶ w jaki sposób dane będą przetwarzane, przy pomocy jakich narzędzi, systemów, czy też będą przetwarzane w formie papierowej;
- ▶ jakie zabezpieczenia danych osobowych będą stosowane;
- ▶ kto będzie miał dostęp do danych osobowych, czy przy przetwarzaniu będą uczestniczyć inne, zewnętrzne podmioty, jeżeli tak, to jaka będzie ich rola (patrz: *Powierzenie przetwarzania danych osobowych, Współadministrator, Udostępnienie danych osobowych*);
- ▶ w jaki sposób będą realizowane prawa osób, których dane będą przetwarzane, w tym jak będzie spełniany obowiązek informacyjny (patrz: *Obowiązek informacyjny*);
- ▶ jeżeli przetwarzanie danych osobowych będzie odbywać się na podstawie zgody, to jaka powinna być jej treść, w jaki sposób zgoda ta będzie zbierana, czy za pośrednictwem formularzy papierowych, czy poprzez narzędzia elektroniczne,

⁹⁰ Wytyczne EROD nr 4/2019 dotyczące art. 25. Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych, wersja 2.0, s. 16–32.

np. wyrażenie zgody poprzez zaznaczenie checkboxa, przy zakładaniu konta w sklepie internetowym itp.;

- ▶ jak długo dane będą potrzebne organizacji, jaki będzie okres ich przechowywania, jak potem organizacja będzie usuwać dane osobowe, czy w ogóle możliwe jest trwałe usunięcie danych osobowych (patrz: **Okres przechowywania danych osobowych**);
- ▶ czy w ramach tego procesu będzie dochodzić do przekazywania danych osobowych do państw spoza EOG, jeżeli tak, to na jakiej podstawie (patrz: **Transfer danych poza Europejski Obszar Gospodarczy**);
- ▶ w jaki sposób będą rozwiązywane sprawy związane z naruszeniem ochrony danych osobowych, jaki będzie schemat działania przy naruszeniu ochrony danych (patrz: **Naruszenia ochrony danych**);
- ▶ kto będzie odpowiedzialny za weryfikację przebiegu procesu pod kątem przepisów o ochronie danych osobowych, jak często należy monitorować i weryfikować wprowadzany proces.

W przypadku gdy w organizacji sportowej został powołany inspektor ochrony danych (patrz: **Inspektor ochrony danych**), należy pamiętać, że powinien on być włączony w prace nad wdrożeniem nowego procesu przetwarzania danych osobowych.

Z uwagi na zasadę rozliczalności (patrz: **Zasada rozliczalności**) administrator powinien w jakiś sposób udokumentować przeprowadzenie procesu projektowania i domyślnej ochrony danych poprzez np. sporządzenie raportu lub notatki z odpowiedziami na wskazane powyżej pytania.

UWAGA!

Prawidłowe zastosowanie zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych może zabezpieczyć interesy organizacji sportowej. Z uwagi na to, że już na etapie wprowadzania nowego procesu przetwarzania danych osobowych zostaną uwzględnione kwestie i wymogi wynikające z przepisów o ochronie danych osobowych, organizacja uchroni się przed koniecznością zmiany już istniejących procesów lub systemów, z których korzysta, a które nie spełniają wymogów wynikających z przepisów. Może to bowiem wiązać się z trudnościami we wprowadzeniu takich zmian, a także koniecznością ponoszenia kosztów z tym związanych⁹¹.

⁹¹ *Ibidem*, s. 11.

17. PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

17.1. KATALOG PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Przepisy RODO wprowadzają szeroki zakres praw dla osób, których dane osobowe są przetwarzane przez organizację sportową. To zaś wiąże się z koniecznością zapewnienia możliwości wykonania przez te osoby przysługujących im praw.

Podstawowe prawa osób, których dane dotyczą, to:

- ▶ prawo dostępu do danych osobowych;
- ▶ prawo do sprostowania danych;
- ▶ prawo do usunięcia danych („prawo do bycia zapomnianym”);
- ▶ prawo do ograniczenia przetwarzania;
- ▶ prawo do przenoszenia danych;
- ▶ prawo do sprzeciwu wobec przetwarzania danych osobowych;
- ▶ prawo do niepodlegania decyzjom podjętym w warunkach zautomatyzowanego przetwarzania danych, w tym profilowania;
- ▶ prawo do wycofania zgody na przetwarzanie danych osobowych;
- ▶ prawo do złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

17.1.1. PRAWO DOSTĘPU DO DANYCH OSOBOWYCH

ART. 15 RODO

„1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

- a) cele przetwarzania;
- b) kategorie odnośnych danych osobowych;

- c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
 - d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
 - e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
 - f) informacje o prawie wniesienia skargi do organu nadzorczego;
 - g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
 - h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem.
3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.
4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych”.

Przepisy RODO przyznają osobie, której dane dotyczą, prawo dostępu do jej danych. W ramach tego prawa możliwe jest żądanie:

- ▶ udzielenia stosownych informacji;
- ▶ otrzymania kopii danych.

ŻĄDANIE UDZIELENIA STOSOWNYCH INFORMACJI

Osoba, której dane dotyczą może żądać uzyskania informacji o:

- ▶ celach przetwarzania (w jakim celu jej dane są przetwarzane);
- ▶ kategoriach danych osobowych (jakie jej dane są przetwarzane, np. imię, nazwisko, adres zamieszkania, PESEL);

- ▶ odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych (komu jej dane są przekazywane) (patrz: Odbiorca danych osobowych);
- ▶ planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalenia tego okresu (jak długo dane będą przechowywane w odniesieniu do celów, w których są przetwarzane);
- ▶ prawie do żądania od administratora danych osobowych sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- ▶ prawie wniesienia skargi do organu nadzorczego;
- ▶ w przypadku zbierania danych osobowych nie od osoby, której dotyczą – wszelkich dostępnych informacji o ich źródle (skąd organizacja sportowa pozyskała jej dane);
- ▶ jeżeli ma to zastosowanie – zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, które wywierają skutki prawne, w szczególności o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
- ▶ jeżeli ma to zastosowanie – odpowiednich zabezpieczeniach związanych z przekazywaniem danych do państw trzecich lub organizacji międzynarodowych.

UWAGA!

Jeżeli dana osoba zwróci się o udzielenie informacji w ramach realizacji prawa dostępu do danych osobowych, organizacja sportowa ma obowiązek ich udzielenia, jeżeli przetwarza dane osobowe tej osoby. Prawo to obowiązuje niezależnie od podstawy prawnej przetwarzania czy źródła pozyskania danych osobowych. Należy jednak zawsze zweryfikować, w jakim zakresie dana osoba żąda prawa dostępu (czy tylko w określonym zakresie, np. odnośnie do danego procesu przetwarzania, czy też w pełnym zakresie – odnośnie do wszystkich danych jego dotyczących). W ramach realizacji prawa dostępu do danych osobowych możliwe jest żądanie tylko tego zakresu informacji, który został wskazany powyżej.

PRZYKŁADY

Kibic posiadający konto w sklepie internetowym klubu sportowego wnosi o uzyskanie prawa dostępu do danych osobowych przetwarzanych w sklepie internetowym.

Zawodnik zwraca się do polskiego związku sportowego o przekazanie mu informacji o wszystkich jego danych osobowych, które przetwarza polski związek sportowy.

Rodzice małoletniego zawodnika żądają od organizatora zawodów informacji o przetwarzanych danych osobowych ich dziecka.

PRAWO DO UZYSKANIA KOPII DANYCH OSOBOWYCH

Na prawo dostępu do danych osobowych składa się również prawo do otrzymania od administratora danych osobowych kopii danych osobowych we wskazanym przez siebie formacie. A zatem osoba może żądać, żeby organizacja sportowa przekazała jej kopię danych osobowych jej dotyczących. Może też wskazać, czy dotyczy to wszystkich danych osobowych, które posiada o niej organizacja sportowa, czy tylko danych w określonym zakresie (np. w zakresie udziału zawodnika w danych zawodach).

Jeżeli osoba zwróciła się o kopię danych drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną⁹² (jeżeli np. osoba zwróciła się o przesłanie kopii w formie e-mailowej, administrator danych osobowych powinien przesłać kopię przetwarzanych danych w tej samej formie).

PRZYKŁADY

Formy przekazania kopii danych:

- ▶ kopia dokumentu;
- ▶ wydruk z systemu informatycznego;
- ▶ przekazanie zrzutu ekranowego;
- ▶ zapewnienie samodzielnego elektronicznego dostępu poprzez pobranie kopii danych bezpośrednio z systemu informatycznego⁹³.

UWAGA!

Należy zweryfikować, jakie dane osobowe żądającego organizacja sportowa przetwarza, a także gdzie się one znajdują. Jeżeli dana osoba zażądała uzyskania kopii wszystkich danych jej dotyczących, należy sprawdzić posiadaną dokumentację, systemy informatyczne, konta pocztowe, dyski chmurowe, w których mogą znajdować się dane osobowe tej osoby.

⁹² P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 394.

⁹³ M. Sakowska-Baryła, *Prawo dostępu przysługujące osobie, której dane dotyczą*, [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie RODO*, Wrocław 2017, s. 167.

OPŁATA ZA REALIZACJĘ PRAWA DO KOPII DANYCH

Administrator danych osobowych nie powinien pobierać opłaty za przekazanie kopii danych. Przepisy RODO wskazują jednak, że może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych w przypadku żądania każdej kolejnej kopii danych (np. gdy konieczne jest skserowanie dużej liczby dokumentów zawierających dane osobowe)⁹⁴.

PRZYKŁADY

Zawodnik żąda ponownego przesłania wcześniej przekazanych już przez klub sportowy kopii danych w tym samym zakresie.

Kibic składa kilkakrotnie takie same żądania odnośnie do przekazania kopii jego danych, gdy zakres tych danych się nie zmienił w porównaniu do wcześniejszego żądania i jego zrealizowania przez organizację sportową⁹⁵.

UWAGA!

Prawo do otrzymania kopii danych nie może wpływać na prawa i wolności innych osób, w tym np. tajemnice handlowe, prawo własności intelektualnej, w tym prawa autorskie chroniące oprogramowanie. Jeżeli takie zagrożenie istnieje, administrator danych osobowych powinien w jasny i przejrzysty sposób poinformować osobę występującą z żądaniem o powodach niemożności zrealizowania prawa w tym zakresie lub o ograniczonym zakresie przekazanych kopii danych.

Niezależnie od powyższego należy wskazać, że żądanie prawa dostępu do danych osobowych jest prawem niezależnym od np. prawa wglądu do akt postępowania, np. dyscyplinarnego, żądania udostępniania odpisów dokumentów, zaświadczeń regulowanych przez poszczególne przepisy prawa powszechnego.

17.1.2. PRAWO DO SPROSTOWANIA DANYCH

ART. 16 RODO

„Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem

⁹⁴ Zob. szerzej: K. Kozieł, *Sposoby ustalania opłat za realizację praw podmiotów danych*, „Magazyn ODO” 2018, nr 6, s. 10–13.

⁹⁵ Por. *ibidem*, s. 10.

celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia”.

Prawo do sprostowania danych przyznaje osobie, której dane dotyczą, następujące uprawnienia:

- ▶ prawo do sprostowania nieprawidłowych danych osobowych;
- ▶ prawo do uzupełnienia niekompletnych danych osobowych.

Osoba, której organizacja sportowa przetwarza dane osobowe, może zażądać sprostowania danych osobowych, jeżeli wykaże w zgłoszonym żądaniu, że dane te są nieprawidłowe lub niekompletne.

Dane nieprawidłowe to takie, które nie odzwierciedlają rzeczywistego stanu rzeczy (tj. dane nieprawdziwe). Dane niekompletne to takie, które są prawidłowe, ale niepełne w określonym zakresie.

PRZYKŁADY

- ▶ błędnie wskazane nazwisko, numer telefonu, adres e-mail itd. zawodnika lub kibica;
- ▶ zmiana danych po zawarciu związku małżeńskiego i zmianie nazwiska przez zawodniczkę;
- ▶ aktualizacja danych nieaktualnych, jak np. zmiana numeru telefonu, adresu zamieszkania przez zawodnika, trenera, sędziego.

UWAGA!

Należy pamiętać, że kompletność danych osobowych powinna być oceniana pod względem zasady minimalizacji danych osobowych (powinno zbierać się tylko tyle danych, ile jest niezbędnych z uwagi na cel, w jakim dane są zbierane). Jeżeli osoba żąda, żeby uzupełnić jej dane osobowe, bo uważa, że są niekompletne, organizacja sportowa powinna się upewnić, czy faktycznie te dane są jej niezbędne.

POINFORMOWANIE ODBIORCÓW DANYCH O SPROSTOWANIU DANYCH

Administrator danych osobowych jest zobowiązany do poinformowania o sprostowaniu danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe (czyli podmioty przetwarzające, podmioty, którym dane zostały udostępnione, organy i inne podmioty, którym ujawniono dane), chyba że okaże się to niemożliwe

lub będzie wymagać niewspółmiernie dużego wysiłku. Ma to zapewnić zgodność z prawem przetwarzania danych osobowych osób fizycznych. Konieczne jest zatem zweryfikowanie, komu zostały przekazane dane osobowe, które były niekompletne lub nieprawidłowe, a następnie przekazanie informacji o tym, aby dane te zostały poprawione lub odpowiednio uzupełnione.

17.1.3. PRAWO DO USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM”)

ART. 17 RODO

„1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a, i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Ust. 1 i 2 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

- b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz i i art. 9 ust. 3;
- d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- e) do ustalenia, dochodzenia lub obrony roszczeń”.

Na prawo do bycia zapomnianym składają się dwa uprawnienia:

- ▶ żądanie usunięcia danych osobowych przez administratora danych osobowych;
- ▶ żądanie, aby administrator danych osobowych poinformował innych administratorów danych osobowych, którym upublicznił dane osobowe tej osoby, o tym, że osoba ta żąda usunięcia wszelkich łączy do tych danych, kopii danych oraz ich replikacji.

USUNIĘCIE DANYCH

Należy pamiętać, że prawo do usunięcia danych nie dotyczy każdej sytuacji, w której dane osobowe są przetwarzane. Prawo do żądania usunięcia danych osobowych przysługuje w następujących przypadkach:

- ▶ dane osobowe nie są już niezbędne do realizacji celów, w których zostały zebrane;
- ▶ dane osobowe są przetwarzane niezgodnie z prawem (np. zostały zebrane pomimo braku podstawy prawnej do ich zebrania i dalszego przetwarzania);
- ▶ cofnięcie zgody na przetwarzanie danych (gdy przetwarzanie odbywa się na podstawie zgody);
- ▶ osoba wniosła sprzeciw wobec przetwarzania jej danych osobowych (patrz szerzej: Prawo do sprzeciwu wobec przetwarzania danych osobowych);
- ▶ dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego wynikającego z przepisów prawa ciążącego na administratorze danych osobowych;
- ▶ dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

PRZYKŁADY

Kibic wycofał zgodę na przetwarzanie danych osobowych w celach marketingowych. Upłynął okres przechowywania dokumentacji księgowej wynikający z przepisów prawa. Organizacja sportowa przetwarza dane osobowe zawodnika w szerszym zakresie, niż jest to niezbędne. Kibic zrezygnował z konta w sklepie internetowym.

Należy pamiętać, że w przepisach RODO zostały wskazane również sytuacje, w których osoby nie będą mogły skutecznie zrealizować prawa do usunięcia danych osobowych. Organizacja sportowa może przetwarzać dane osobowe pomimo zgłoszenia żądania usunięcia danych osobowych, jeżeli jest to niezbędne:

- ▶ w celu korzystania z prawa do wolności wypowiedzi i informacji;
- ▶ do wywiązania się z prawnego obowiązku wymagającego przetwarzania na podstawie przepisów prawa;
- ▶ do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych osobowych;
- ▶ z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- ▶ do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych albo do celów statystycznych;
- ▶ do ustalenia, dochodzenia lub obrony roszczeń.

PRZYKŁADY

Przetwarzanie danych osobowych jest konieczne w celach związanych z rozliczeniem dotacji przez polski związek sportowy.

Klub sportowy przygotowuje statystyki związane z osiągnięciami sportowymi zawodników danej dyscypliny sportowej.

Polski związek sportowy prowadzi wykaz udzielonych licencji zawodniczych.

UWAGA!

Organizacja sportowa jako administrator danych osobowych ma samodzielny obowiązek usunięcia danych osobowych osoby, jeżeli nie są one już niezbędne do realizacji celu, w którym zostały zabrane (patrz: **Okres przechowywania danych osobowych**). Jeżeli pomimo istniejącego obowiązku usunięcia danych, administrator danych osobowych nadal przetwarza te dane, osoba, której one dotyczą, może żądać ich usunięcia.

ZREALIZOWANIE PRAWA DO USUNIĘCIA DANYCH

Jeżeli wniosek o usunięcie danych jest zasadny, organizacja sportowa powinna usunąć dane osobowe. Powinno to nastąpić w taki sposób, aby nie było możliwe ich odtworzenie. Należy trwale usunąć lub trwale zniszczyć nośniki danych, tak aby odtworzenie zapisanych na nich informacji (danych osobowych) nie było możliwe. Powyższe powinno prowadzić do braku możliwości dalszego dokonywania jakichkolwiek operacji na tych danych⁹⁶.

Wskazuje się, że skuteczne wykonanie prawa do bycia zapomnianym wymaga, aby administrator danych osobowych usunął dane również z kopii zapasowych. Co za tym idzie, należy ustalić, czy możliwe jest usunięcie poszczególnych informacji z kopii zapasowych administratora danych osobowych, a następnie je trwale usunąć.

POINFORMOWANIE INNYCH ADMINISTRATORÓW ORAZ ODBIORCÓW DANYCH O USUNIĘCIU DANYCH

Organizacja sportowa musi podjąć rozsądne działania mające na celu poinformowanie o zgłoszonym żądaniu innych administratorów danych osobowych, którym dane zostały przez nią udostępnione. Należy w tym zakresie wziąć pod uwagę dostępną technologię i koszt realizacji takiego działania. Nie trzeba tego wykonywać, jeżeli poinformowanie okaże się niemożliwe lub znacznie utrudnione⁹⁷, jednak administrator danych osobowych powinien podjąć inicjatywę w tym zakresie.

Ponadto, administrator danych osobowych jest zobowiązany do poinformowania o usunięciu danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe (patrz: Odbiorca danych), np. podmioty przetwarzające, podmioty, którym dane zostały udostępnione, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

17.1.4. PRAWO DO OGRANICZENIA PRZETWARZANIA

ART. 18 RODO

„1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

⁹⁶ P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE...*, *op.cit.*, s. 404.

⁹⁷ P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Komentarz do art. 17.

- b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1”.

Ograniczenie przetwarzania danych osobowych polega na zawężeniu operacji przetwarzania danych wyłącznie do ich przechowywania.

Prawo żądania ograniczenia przetwarzania danych osobowych nie przysługuje zawsze, ale tylko w określonych, wskazanych w art. 18 RODO przypadkach.

PRZYKŁADY

- ▶ czasowe przeniesienie wybranych danych osobowych do innego systemu informacyjnego;
- ▶ uniemożliwienie użytkownikom dostępu do wybranych danych osobowych (zablokowanie edycji, możliwości przeglądania, zmiany danych itd.);
- ▶ czasowe usunięcie opublikowanych danych ze strony internetowej;
- ▶ przechowywanie danych w oddzielnej teczce.

Nawet w przypadku, gdy zostanie zrealizowane prawo do ograniczenia przetwarzania danych osobowych na żądanie danej osoby, organizacja sportowa może przetwarzać dane jej dotyczące w szerszym zakresie niż tylko w zakresie przechowywania danych osobowych, jeżeli:

- ▶ osoba, której dane dotyczą, wyraziła na to zgodę;
- ▶ jest to konieczne w celu ustalenia, dochodzenia lub obrony roszczeń;
- ▶ jest to konieczne w celu ochrony praw innej osoby fizycznej lub prawnej;
- ▶ jest to konieczne z uwagi na ważne względy interesu publicznego.

POINFORMOWANIE ODBIORCÓW DANYCH O OGRANICZENIU PRZETWARZANIA DANYCH

Administrator danych osobowych jest zobowiązany do poinformowania o ograniczeniu przetwarzania danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe (czyli podmioty przetwarzające, podmioty, którym dane zostały udostępnione, organy i inne podmioty, którym ujawniono dane), chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

17.1.5. PRAWO DO PRZENOSZENIA DANYCH

ART. 20 RODO

„1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a lub na podstawie umowy w myśl art. 6 ust. 1 lit. b; oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych”.

Prawo do przenoszenia danych osobowych polega na możliwości przeniesienia (przesłania, przekazania) przez daną osobę jej danych osobowych przetwarzanych przez jednego administratora danych osobowych, na rzecz drugiego administratora danych osobowych. Może to jej ułatwić m.in. korzystanie z usług innego podmiotu niż dotychczasowy administrator danych osobowych.

Prawo do przenoszenia danych będzie miało zastosowanie jedynie w przypadku, gdy łącznie zostaną spełnione następujące przesłanki:

- ▶ przetwarzanie danych odbywa się na podstawie zgody (zarówno zgody na przetwarzanie danych zwykłych, jak również szczególnych kategorii danych) lub na podstawie umowy **oraz**
- ▶ przetwarzanie odbywa się w sposób zautomatyzowany (np. w systemie informatycznym).

PRZYKŁADY

Zawodnik żąda przekazania jego danych osobowych z dotychczasowego do nowego klubu sportowego, który będzie reprezentował.

Sędzia żąda przekazania jego danych osobowych pomiędzy związkami sportowymi, których rozgrywki będzie sędziował.

UWAGA!

Prawo do przenoszenia danych nie obejmuje przetwarzania danych w formie papierowej (kwestionariusze, akta, formularze), a jedynie za pośrednictwem systemów informatycznych.

W ramach prawa do przenoszenia danych osobie, której dane dotyczą, przysługują następujące uprawnienia:

- ▶ prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących;
- ▶ prawo do żądania przesłania przez administratora danych osobowych dotyczących jej danych innemu administratorowi danych osobowych.

PRAWO DO OTRZYMANIA DANYCH OSOBOWYCH W POWSZECHNIE UŻYWANYM FORMACIE

Zgodnie z motywem 68 RODO administratorów danych osobowych należy zachęcać do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych. Przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno jednak nakładać na administratorów danych osobowych obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania.

Format przenoszonych danych powinien być powszechnie używanym formatem w danej branży lub w zakresie określonych danych. Jeżeli określone formaty nie są w powszechnym użyciu w danej branży lub kontekście, administratorzy danych osobowych powinni przekazać dane osobowe przy użyciu powszechnie wykorzystywanych

formatów (np. XHTML, JSON, CSV) wraz z przydatnymi metadanymi na najlepszym poziomie szczegółowości⁹⁸.

BEZPOŚREDNIE PRZESŁANIE DANYCH POMIĘDZY ADMINISTRATORAMI DANYCH OSOBOWYCH

O ile jest to technicznie możliwe, osoba, której dane dotyczą, ma prawo żądać, by dane osobowe zostały przesłane przez jednego administratora danych osobowych bezpośrednio innemu administratorowi danych osobowych (np. jeden klub sportowy przesyła dane osobowe zawodnika drugiemu klubowi sportowemu).

Bezpośrednie przesłanie danych pomiędzy administratorami danych osobowych będzie możliwe w przypadku nawiązania komunikacji pomiędzy ich systemami w sposób bezpieczny (należy zapewnić odpowiednie zabezpieczenia przesyłu danych), a podmiot, któremu przesłano informacje, będzie miał techniczną możliwość otrzymania/otwarcia tych danych.

17.1.6. PRAWO DO SPRZECIWU WOBEC PRZETWARZANIA DANYCH OSOBOWYCH

ART. 21 RODO

„1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e lub f, w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

3. Jeżeli osoba, której dane dotyczą, wnieśli sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

⁹⁸ WP-242 – Wytyczne Grupy Roboczej Art. 29 dotyczące prawa do przenoszenia danych, s. 19.

4. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyrażnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

5. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

6. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym”.

Prawo do sprzeciwu wobec przetwarzania danych osobowych przysługuje osobie, której dane dotyczą, w przypadku przetwarzania danych osobowych:

- ▶ w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych osobowych;
- ▶ do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora danych osobowych lub osobę trzecią;
- ▶ do celów badań naukowych lub historycznych lub do celów statystycznych – chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
- ▶ do celów marketingu bezpośredniego.

Administrator danych osobowych nie powinien przetwarzać danych po wniesieniu sprzeciwu, chyba że wykáže istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia albo obrony roszczeń. W tym zakresie należy przeprowadzić test równowagi, analogicznie jak w przypadku oparcia przetwarzania danych osobowych o prawnie uzasadniony interes administratora (patrz: Jak przeprowadzić test równowagi?).

UWAGA!

W przypadku, gdy sprzeciw dotyczy przetwarzania danych osobowych w celu marketingu bezpośredniego, nie wolno już przetwarzać danych do takich celów. W tym

zakresie jest to prawo bezwarunkowe⁹⁹ i nie zależy od tego, czy administrator danych osobowych posiada prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec praw i wolności osoby, której dane dotyczą.

17.1.7. PRAWO DO NIEPODLEGANIA ZAUTOMATYZOWANEMU PODEJMOWANIU DECYZJI, W TYM PROFILOWANIU

ART. 22 RODO

„1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:

- a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
- c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3. W przypadkach, o których mowa w ust. 2 lit. a i c, administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a lub g i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą”.

Dzięki temu prawu osoba, której dane dotyczą, nie podlega decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływa¹⁰⁰.

⁹⁹ M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2017, nr 5, s. 37–42.

¹⁰⁰ Zob. szerzej: P. Siemieniak, *Prawo do niepodlegania decyzjom podjętym w warunkach zautomatyzowanego przetwarzania danych, w tym profilowania*, [w:] B. Fischer, M. Sakowska-Baryła (red.),

Pod pojęciem profilowania rozumie się dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Proces ten musi się odbywać w sposób zautomatyzowany, tzn. bez udziału człowieka w procesie budowania profilu, a profil budowany jest za pomocą odpowiednich środków technicznych.

PRZYKŁADY

Zawodnicy zostają powołani do kardy narodowej wyłącznie na podstawie decyzji systemu informatycznego, który analizuje ich wyniki sportowe.

Skauting zawodników do klubu sportowego odbywa się wyłącznie w oparciu o decyzję podjętą przez system sztucznej inteligencji na podstawie danych przez niego zgromadzonych i przeanalizowanych.

Rekrutacja pracowników do klubu sportowego odbywa się wyłącznie w oparciu o elektroniczny system rekrutacji.

W przypadku zautomatyzowanego podejmowania decyzji administrator danych osobowych powinien wdrożyć odpowiednie środki zapewniające ochronę praw i wolności osoby, której dane dotyczą. W szczególności osoba ta powinna mieć zapewnione prawo co najmniej do:

- ▶ uzyskania interwencji ludzkiej ze strony administratora danych osobowych (tzn. aby jej sprawa została rozpatrzona przez osobę lub podmiot działający w imieniu administratora danych osobowych lub przez samego administratora danych osobowych);
- ▶ wyrażenia własnego stanowiska;
- ▶ zakwestionowania decyzji podjętej w sposób zautomatyzowany.

KIEDY PRAWO TO NIE PRZYSŁUGUJE

Prawo do niepodlegania zautomatyzowanym decyzjom nie ma zastosowania w następujących przypadkach:

- ▶ decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem danych osobowych;

- ▶ podjęcie takiej decyzji jest dozwolone w przepisach prawa, jeżeli przepisy te przewidują właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;
- ▶ decyzja opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

UWAGA!

Co do zasady zautomatyzowane podejmowanie decyzji nie może opierać się na wykorzystaniu szczególnych kategorii danych, np. danych o stanie zdrowia. Pewne wyjątki w tym zakresie zostały uregulowane w treści art. 22 ust. 4 RODO. Nie jest zatem możliwe przetwarzanie w tym zakresie danych o stanie zdrowia zawodników, informacji o niepełnosprawności kandydatów do zatrudnienia itd.

17.1.8. PRAWO DO WYCOFANIA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

ART. 7 UST. 3 RODO

„3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie”.

Jeżeli przetwarzanie danych osobowych odbywa się na podstawie zgody osoby, której dane dotyczą, ma ona prawo w dowolnym momencie tę zgodę wycofać. Wycofanie zgody wiąże się z obowiązkiem zaprzestania przetwarzania danych w celu, w którym dane osobowe były przetwarzane na podstawie zgody.

Należy pamiętać, że wycofanie zgody musi być równie łatwe jak jej wyrażenie. A zatem administrator danych osobowych powinien zapewnić możliwość wycofania zgody w ten sam lub równie łatwy sposób, w jaki została ona udzielona. Co ważne, administrator danych osobowych nie powinien ograniczać sposobu, w jaki taka zgoda może być wycofana. Może wskazać rekomendowany sposób (np. udostępnić formularz, wzorcowe oświadczenie), ale nie powinien uzależniać skuteczności realizacji tego prawa od zachowania przez osobę, która chce taką zgodę wycofać, określonych wymogów formalnych.

Ponadto wycofanie zgody nie powinno wiązać się dla tej osoby z żadnymi negatywnymi konsekwencjami (np. cofnięciem udzielonych rabatów w sklepie internetowym, podwyższeniem ceny biletu na mecz itd.).

UWAGA!

Działania organizacji sportowej podjęte w okresie, gdy zgoda była udzielona, nie stają się bezprawne poprzez wycofanie zgody. Były one zgodne z prawem. Wycofanie zgody odnosi skutek na przyszłość, nie niweczy zaś zgodności z prawem przetwarzania danych przez administratora danych osobowych, które podejmował w czasie, gdy zgoda była wyrażona.

17.1.9. PRAWO DO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO

ART. 77 RODO

„1. Bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących narusza niniejsze rozporządzenie.
2. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78”.

W przypadku, gdy osoba, której dane są przetwarzane, uważa, że przetwarzanie to odbywa się niezgodnie z przepisami RODO, może złożyć skargę do organu nadzorczego. W Polsce organem uprawnionym do rozpatrywania skarg jest Prezes Urzędu Ochrony Danych Osobowych. Skarga może zostać złożona w formie tradycyjnej, w tym do protokołu w siedzibie Prezesa UODO¹⁰¹, lub w formie elektronicznej¹⁰².

Organ ten ma obowiązek rozpatrzyć skargę. W tym celu najczęściej wzywa administratora danych osobowych do złożenia wyjaśnień i odpowiedzi na skargę. administrator danych powinien złożyć stosowne i szczegółowe wyjaśnienia, przedstawić w razie potrzeby dowody na potwierdzenie swoich twierdzeń oraz współpracować w tym zakresie z organem.

¹⁰¹ UODO, *Składanie skargi w formie tradycyjnej, w tym do protokołu w siedzibie Prezesa Urzędu*, <https://uodo.gov.pl/pl/489/2247> [dostęp: 10.12.2024].

¹⁰² UODO, *Składanie skargi drogą elektroniczną*, https://uodo.gov.pl/489/id_art/2246 [dostęp: 10.12.2024].

TERMIN, W KTÓRYM NALEŻY ROZPATRZEĆ ŻĄDANIE DANEJ OSOBY

Przepisy RODO przewidują, że organizacja sportowa jako administrator danych osobowych powinna rozpatrzyć zgłoszone żądanie w terminie miesiąca od otrzymania żądania (kiedy żądanie wpłynęło, zostało doręczone, przekazane). Termin ten może zostać przedłużony o kolejne dwa miesiące (a zatem administrator danych osobowych ma łącznie trzy miesiące na odpowiedź), jeżeli żądanie ma skomplikowany charakter lub jednorazowa liczba żądań jest znaczna (np. dana osoba złożyła w jednym czasie kilka żądań). W takim przypadku w terminie miesiąca od dnia otrzymania żądań należy jednak poinformować tę osobę o:

- ▶ przedłużeniu terminu oraz
- ▶ podać przyczyny opóźnienia.

Jeżeli administrator danych osobowych nie podejmuje działań w związku z żądaniem osoby (np. uważa, że zgłoszone żądanie w zakresie realizacji prawa w tym przypadku nie przysługuje), powinien niezwłocznie, nie później niż w terminie miesiąca, ją o tym poinformować i podać:

- ▶ powody niepodjęcia działań;
- ▶ informację o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

CZY MOŻNA ŻĄDAĆ OPŁATY ZA REALIZACJĘ PRAWA?

Administrator danych osobowych nie powinien pobierać opłat za udzielenie informacji dotyczących przetwarzania danych osobowych. Jednak w przypadku, gdy żądania osoby są ewidentnie nieuzasadnione lub nadmierne (np. wielokrotnie w krótkich odstępach czasu zwraca się ona o przekazanie informacji), administrator danych osobowych może:

- ▶ pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielania informacji, prowadzenia komunikacji lub podjęcia żądanych działań (wysokość opłaty powinna odzwierciedlać faktycznie poniesione przez administratora danych osobowych w związku z tym koszty, np. koszty pracy związane z analizą żądania, przygotowaniem i wysyłką korespondencji¹⁰³; nie może jednak prowadzić do ograniczenia przysługujących osobie praw, ale ma zapobiegać nadużywaniu przez nią przysługujących jej praw¹⁰⁴) **albo**
- ▶ odmówić podjęcia działań w związku z tym żądaniem.

¹⁰³ E. Bielak-Jomaa, D. Lubasz (red.), *RODO...*, *op.cit.*

¹⁰⁴ Stanowisko Prezesa Urzędu Ochrony Danych Osobowych, *Kiedy administrator może pobrać opłatę za udzielenie informacji osobie, której dane dotyczą?*, <https://uodo.gov.pl/pl/225/1169> [dostęp: 10.09.2019].

WPROWADZENIE PROCEDUR DOTYCZĄCYCH REALIZACJI PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Organizacja sportowa powinna wprowadzić określone procedury dotyczące realizacji praw osób, których dane przetwarza, oraz sposobu obsługi wpływających w tym zakresie wniosków i żądań. To ułatwi administratorowi danych osobowych wywiązywanie się z nałożonych na niego przez przepisy RODO obowiązków, a jednocześnie realizację tych praw osobom, których dane dotyczą.

Administrator danych osobowych powinien wprowadzić procedury w szczególności w zakresie następujących kwestii:

- ▶ miejsca przyjmowania żądań (określony, dedykowany do tego adres e-mail, numer telefonu, adres do doręczeń);
- ▶ osób odpowiedzialnych za rozpatrywanie wpływających żądań podmiotów danych;
- ▶ sposobu i terminu rozpatrywania żądań, mając na uwadze przepisy prawa w tym zakresie;
- ▶ ewentualnych dodatkowych opłat za realizację żądań (należy pamiętać, że co do zasady realizacja praw osób, których dane dotyczą, jest wolna od opłat, jednak w pewnych sytuacjach możliwe jest pobranie opłat w określonej wysokości) oraz sposobów ich ustalania;
- ▶ formy i wzoru treści odpowiedzi na zgłoszone żądanie;
- ▶ formy i wzoru treści informacji kierowanych do odbiorców danych osobowych związanych ze zgłoszonymi żądaniami (w przypadku żądania prawa sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych);
- ▶ formy, sposobu oraz treści obowiązków informacyjnych kierowanych do poszczególnych kategorii osób, których dane są przetwarzane;
- ▶ wzoru rejestru wniosków dotyczących realizacji praw przysługujących osobom w związku z przetwarzaniem ich danych osobowych oraz osób odpowiedzialnych za jego prowadzenie w myśl zasady rozliczalności (patrz: **Zasada rozliczalności**).

Ustalenie powyższych kwestii może okazać się pomocne dla organizacji sportowych w ich codziennej działalności związanej z odpowiadaniem na żądania osób, których dane dotyczą.

18. BEZPIECZEŃSTWO DANYCH OSOBOWYCH ORAZ NARUSZENIA OCHRONY DANYCH OSOBOWYCH

18.1. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Bezpieczeństwo danych osobowych w sporcie jest niezwykle istotnym zagadnieniem w kontekście ochrony prywatności i praw jednostki. Współczesny świat sportu, zarówno zawodowego, jak i amatorskiego, staje się coraz bardziej z informatyzowany. Wraz z tym rośnie liczba danych przetwarzanych przez kluby, związki oraz inne podmioty zaangażowane w organizację i promocję sportu. Właściwa ochrona tych danych to klucz do zapewnienia bezpieczeństwa zawodników, kibiców oraz pracowników sektora sportowego.

Dane osobowe w sporcie mogą obejmować szeroki zakres informacji, takich jak:

- ▶ podstawowe dane osobowe – imię, nazwisko, data urodzenia, adres zamieszkania czy numer telefonu;
- ▶ dane medyczne – wyniki badań lekarskich, informacje o kontuzjach, historię chorób, a także wyniki testów dopingowych;
- ▶ dane finansowe – wysokość zarobków, dane o transferach i premie kontraktowe zawodników;
- ▶ dane audiowizualne – zdjęcia, nagrania wideo z treningów czy zawodów.

Przetwarzanie danych osobowych w sporcie wiąże się z wieloma wyzwaniami, takimi jak:

- ▶ zagrożenie cyberatakami – systemy informatyczne klubów sportowych i związków są coraz częściej celem ataków hakerów, co może prowadzić do wycieku danych osobowych zawodników, trenerów, sędziów, pracowników związków i klubów oraz wszystkich tych osób, które w organizacjach sportowych uczestniczą w procesach przetwarzania danych i zaangażowane są w rozwój sportu;
- ▶ nieuprawniony dostęp do danych – zarządzanie danymi, które może prowadzić do ich niewłaściwego wykorzystania, takiego jak brak odpowiednich uprawnień dla użytkowników systemów, w których przetwarzane są dane osobowe, brak nadzoru nad dokumentacją zawodniczą prowadzoną przez kluby i związki, niewłaściwie

zabezpieczone bazy kibiców czy dostęp do dokumentacji lekarskiej zawodników w zakresie ich stanu zdrowia oraz udzielanych świadczeń medycznych dla osób nieuprawnionych;

- niewystarczająca edukacja – brak świadomości wśród zawodników i personelu sportowego na temat zasad ochrony danych osobowych, który może prowadzić do niezamierzonych naruszeń.

18.2. NARUSZENIA OCHRONY DANYCH OSOBOWYCH I ZWIĄZANE Z TYM OBOWIĄZKI ADMINISTRATORÓW

Naruszenia ochrony danych osobowych mogą powodować poważne konsekwencje dla osób, których dane dotyczą, jak i dla podmiotów oraz organizacji sportowych zobowiązanych do ich zabezpieczania. Właściwe reagowanie na takie incydenty jest kluczowe dla ochrony podstawowych praw i wolności oraz spełniania wymogów prawnych (patrz: *Naruszenia ochrony danych osobowych, część szczegółowa*).

Wszędzie tam, gdzie przetwarzane są dane osobowe, może dojść do naruszenia ochrony danych osobowych. Jest nim zakłócenie bezpieczeństwa przetwarzanych danych osobowych, które może wpłynąć na ich poufność, integralność lub dostępność¹⁰⁵.

Wiedza na temat naruszeń ochrony danych osobowych jest szczególnie ważna dla podmiotów sportowych jako dla administratorów (patrz: *Administrator*), gdyż na nich spoczywa największa odpowiedzialność za ochronę danych osobowych, np. w klubie lub związku, ale znaczącą rolę w zapewnieniu bezpieczeństwa przetwarzania odgrywają także wyznaczeni inspektorzy ochrony danych w podmiotach sportowych i podmioty przetwarzające w imieniu administratorów i działające na podstawie umów z administratorami (patrz: *Podmiot przetwarzający*).

¹⁰⁵ UODO, *Poradnik. Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*, wersja 2.0, s. 8, <https://uodo.gov.pl/pl/138/3561> [dostęp: 10.08.2025].

19. ANALIZA RYZYKA

19.1. OBOWIĄZEK ANALIZY RYZYKA

ART. 32 RODO¹⁰⁶

„Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku”.

Zarządzanie ryzykiem zgodnie z RODO stanowi podstawę zgodności z przepisami prawa. Bez przeprowadzenia rzetelnej analizy ryzyka nie będziemy w stanie ustalić i udowodnić, że zastosowane przez administratora zabezpieczenia są adekwatne do istniejących zagrożeń.

Przy temacie analizy ryzyka zawsze pojawia się pytanie, z jaką częstotliwością należy przeprowadzać analizę ryzyka przetwarzania danych osobowych np. w większych czy mniejszych podmiotach sportowych. Taka analiza powinna być procesem ciągłym służącym do zrozumienia zmieniającego się ryzyka. Kryteria wskazane w przepisie art. 32 RODO determinują m.in. częstotliwość jej przeprowadzania, która powinna być skorelowana z obowiązkiem wskazanym w art. 32 ust. 1 lit. d RODO, tj. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Bezdiskusyjny pozostaje fakt, że podmioty sportowe działają i organizują wydarzenia sportowe w warunkach niepewności budowanej przez czynniki wewnętrzne i zewnętrzne, a ryzyko jest nieodłącznym elementem aktywności w obszarze sportu. Z kolei zarządzanie ryzykiem jest nieodłącznym elementem zarządzania projektami¹⁰⁷. W projekcie sportowym możemy napotkać ryzyka zarówno wewnętrzne, jak i zewnętrzne. Pierwsze zazwyczaj można kontrolować, natomiast drugie są

¹⁰⁶ P. Fajgielski, *Ogólne rozporządzenie...*, op.cit., Komentarz do art. 32.

¹⁰⁷ J. Łuczak, *Zarządzanie ryzykiem imprez biegowych i triathlonowych*, Poznań 2017.

w wielu przypadkach poza zasięgiem działania podmiotu sportowego, co oczywiście nie zwalnia administratora z konieczności odpowiedniego zaradzenia takiemu ryzyku.

W analizie ryzyka istotne jest to, że musi ona stanowić punkt wyjścia do doboru odpowiednich środków technicznych i organizacyjnych ochrony danych osobowych. Przedstawiciele wielu organizacji sportowych twierdzą, że u nich jest dobrze i nie ma potrzeby, aby dobierać inne środki niż te, które zostały już wprowadzone, dopóki nie ma naruszenia tam i wszystko działa prawidłowo, nikt nie może stwierdzić, że coś robione jest niewłaściwie i że pojawia się ryzyko.

Prezes UODO zawsze może zweryfikować, czy zastosowane środki techniczne i organizacyjne zapewniają odpowiednie bezpieczeństwo przetwarzanych danych osobowych. Ewentualne stwierdzenie naruszenia ochrony danych osobowych stanowi impuls dla organu nadzorczego, który będzie weryfikował i kontrolował, czy administrator dochował wszelkiej staranności i czy w związku z tym dobrał odpowiednie środki ochrony danych, czy zidentyfikował ryzyka i zagrożenia, jakie w podmiocie sportowym mogą mieć miejsce, albo też czy w ogóle doszło kiedykolwiek do identyfikowania jakichś ryzyk, i czy przeprowadzona była kiedykolwiek analiza ryzyka.

UWAGA!

Należy pamiętać, że procesy przetwarzania danych osobowych w działalności sportowej nie są statycznym zestawem i że na podstawie danych podejmowane są dynamiczne działania. Zatem raz wprowadzone środki bezpieczeństwa nie sprawdzą się na stałe, więc cały czas należy identyfikować swoje zasoby we wszystkich obszarach działalności organizacji, zarówno tych bezpośrednio powiązanych z działaniami sportowymi, jak i organizacyjnymi, tj. kadrowymi, administracyjnymi, marketingowymi, współpracy ze sponsorami i partnerami, oraz systemami i narzędziami informatycznymi wspomagającymi pracę klubu czy związku. Taka identyfikacja zagrożeń i podatności jest niezbędna by przeprowadzać analizy ryzyka.

19.2. PRZEPROWADZENIE ANALIZY RYZYKA – PRAKTYCZNE DZIAŁANIA

Ważne jest, żeby zarządzanie ryzykiem stało się procesem ciągłym, aby co jakiś czas przeprowadzać analizę i dokumentować ją, chociażby po to, żeby w razie materializacji ryzyka być w stanie udowodnić, że wykazano należyłą staranność w doborze odpowiednich do ryzyka środków. Przyjętą (nieoficjalnie) zasadą jest przeprowadzanie

analizy minimum raz na rok. Przeprowadzenie analizy ryzyka jest też obowiązkowe w przypadku wystąpienia naruszenia ochrony danych osobowych w podmiocie sportowym, jak również w każdej nowej okoliczności mogącej oddziaływać w sposób istotny na prawdopodobieństwo lub wagę ryzyka. Administrator musi zapewnić, aby pomimo zmieniających się okoliczności środki bezpieczeństwa były zawsze odpowiednie do ryzyka. Odpowiedzialność i decyzję za zlecenie oceny ryzyka na potrzeby zapewnienia odpowiedniego do ryzyka bezpieczeństwa danych osobowych w podmiocie sportowym spoczywa zawsze na administrаторze i w praktyce może być realizowana przez kierownictwo klubu, związku, obiektu sportowego lub organizatora wydarzenia sportowego. Wszystkie oceny ryzyka muszą być jednak przeprowadzane przez osoby do tego przygotowane, posiadające właściwą wiedzę i doświadczenie. Oczywiście ważne jest też, aby personel podmiotu wspierał taką osobę przy przeprowadzaniu analizy poprzez dostarczenie jej odpowiedniej wiedzy o zasobach organizacji, pomoc przy ich identyfikacji, dotarciu do źródeł, dokumentów czy wskazaniu zagrożeń i określaniu podatności jako luk, które powodują, że zagrożenie jest mniej lub bardziej realne. Personel podmiotu sportowego zazwyczaj posiada wiedzę praktyczną w swoim zakresie i to zawsze jest nieoceniony zasób wiedzy dla osoby przeprowadzającej taką analizę, bez względu na to, czy sama należy lub nie do tego zespołu.

Sposób udokumentowania przeprowadzanej pod przepisy RODO analizy ryzyka dla ochrony danych może być swobodny. W małych klubach czy podmiotach sportowych może to być krótki formularz, notatka z przeprowadzonego procesu, wypełniona tabela w pliku Excel. W dużych podmiotach sportowych należy dokonać wyboru metody oceny ryzyka i z takiej formy skorzystać jako bardziej profesjonalnej. Można wykorzystać metody jakościowe czy ilościowe, które umożliwiają obiektywne szacowanie ryzyka. W normie ISO/IEC dostępnych jest aż 31 metod przeprowadzania analizy ryzyka¹⁰⁸, jednak dla potrzeb podmiotów sportowych w kontekście RODO tylko kilka z nich może okazać się przydatnych.

19.3. METODY ANALIZY RYZYKA

Wyboru metody szacowania ryzyka dokonuje sam administrator, przy czym w sytuacji, gdy nie posiada eksperckiej wiedzy, warto skonsultować to z osobami zawodowo i praktycznie przygotowanymi do takich procesów. Wybór metody uzależniony jest często od możliwości i wielkości podmiotu sportowego, a także zasobów, którymi dysponuje. Wybrana metoda z jednej strony powinna być skorelowana w szczególności z liczbą zasobów narażonych na ryzyko wynikające

¹⁰⁸ Zarządzanie ryzykiem – zasady i wytyczne (2.3), PN-ISO 31000:2012.

z oddziaływania zagrożeń i podatności, liczbą osób oraz zakresem ich danych osobowych, a z drugiej strony powinna być narzędziem ułatwiającym zarządzanie ryzykiem oraz realnie przyczyniającym się do poprawy bezpieczeństwa przetwarzania danych osobowych. Dlatego najważniejsze jest, aby wyboru takiej metody dokonać w oparciu o kryterium skuteczności. Najczęściej stosuje się metody ilościowe, jakościowe lub ilościowo-jakościowe¹⁰⁹.

19.3.1. METODA ILOŚCIOWA ANALIZY RYZYKA

Metoda ilościowa wymaga zaangażowania osób, które potrafią wykorzystać w analizie wykresy, tablice, wyliczenia. Wymaga ona uruchomienia przeliczeń i użycia odpowiednich parametrów, by zrozumieć ryzyka na prezentowanych liczbach.

PRZYKŁAD ARKUSZA ANALIZY Z WYKORZYSTANIEM SKALI PRAWDOPODOBIENSTWA I SKUTKU

Numer ryzyka	Zagrożenie	Prawdopodobieństwo	Skutek	Wartość ryzyka
1.	Zagrożenie utraty danych. W pomieszczeniu klubu, do którego wchodzi wiele osób, znajduje się laptop z nieszyfrowanym dyskiem twardym. W razie jego kradzieży może dojść do utraty danych sędziów, trenerów, zawodników oraz danych kadrowych, które przechowywane są na tym komputerze.	Średnie	Duży	Duże ryzyko
2.	Zagrożenie ujawnienia danych. Brak autoryzacji w pomieszczeniach klubu na drukarce lub urządzeniu wielofunkcyjnym powoduje możliwość wysłania danych poza klub przez osobę nieuprawnioną.	Duże	Średni	Duże ryzyko
3.	Zagrożenie przetwarzania danych bez podstawy prawnej. Trener spisał na kartce dane osobowe od rodziców/opiekunów prawnych zawodnika małoletniego, który uczestniczy w treningu testowym pierwszy raz i nie odebrał od nich stosownych zgód na przetwarzanie tych danych.	Małe	Mały	Małe ryzyko

Źródło: opracowanie własne.

¹⁰⁹ D. Wróblewski (red.), *Zarządzanie ryzykiem – przegląd wybranych metodyk*, Józefów 2015, s. 178.

19.3.2. METODA JAKOŚCIOWA ANALIZY RYZYKA

Wśród metod jakościowych najprostszym narzędziem wykorzystywanym do przeprowadzenia analizy ryzyka jest metoda SWIFT przyjmująca formę listy kontrolnej bazującej na zestawie pytań zadawanych osobom, które biorą udział w procesie. Jest ona od razu weryfikowana, a jej wyniki łatwo wdrożyć. Metoda ta pozwala na szybkie:

- ▶ zidentyfikowanie zagrożeń dla organizacji i sytuacji niebezpiecznych;
- ▶ określenie skutków takich zagrożeń;
- ▶ wyznaczenie najlepszych metod redukcji tych zagrożeń i wdrożenie planu naprawczego.

Należy jednak pamiętać, że obowiązkiem administratora przy określeniu ryzyka na potrzeby doboru odpowiednich środków bezpieczeństwa do tego ryzyka naruszenia praw lub wolności osób fizycznych jest jego łączna ocena prawdopodobieństwa i wagi zagrożenia oraz uwzględnienie pozostałych kryteriów wskazanych w art. 32 RODO, takich jak: stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania. Natomiast metoda jakościowa może nie wykazywać, że przy doborze środków bezpieczeństwa odpowiednich do ryzyka uwzględniono kryteria wskazane w przepisie art. 32 RODO. Jeśli administrator nie jest w stanie wykazać tego w inny sposób, to zastosowanie metody jakościowej może nie być odpowiednie dla czynności przetwarzania, z którymi np. wiąże się wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

PRZYKŁAD OCENY RYZYKA METODĄ SWIFT

Numer ryzyka	Pytanie	Odpowiedź	Działania korygujące
1.	Co jeśli na skutek awarii komputerów, serwera w klubie dojdzie do utraty danych zawartych w formularzach rejestracji zawodników, a klub nie będzie dysponował wydrukowaną wersją papierową?	Wszystkie niewydrukowane formularze elektroniczne zostaną utracone.	Jeśli system nie ma odpowiednich zabezpieczeń, należy systematycznie drukować formularze lub zapisane przechowywać na innych dyskach określonych jako bezpieczne miejsca.
2.	Co jeśli przez błąd w adresie odbiorcy korespondencja elektroniczna prowadzona z trenerem w zakresie jego wynagrodzenia i benefitów, jakie posiada w klubie, zostanie wysłana do innej nieuprawnionej osoby?	Inne osoby nieuprawnione będą miały wgląd w umowę i pozostałą dokumentację z korespondencji z trenerem i będą mogły zapoznać się z ich treścią, w tym ze wszystkimi danymi tam zawartymi.	Należy wprowadzić konieczność szyfrowania lub opatrywania hasłem przed każdą wysyłką dokumentów zawierających dane osobowe oraz sprawdzać poprawność wpisanego adresu odbiorcy.

Numer ryzyka	Pytanie	Odpowiedź	Działania korygujące
3.	Co jeśli ktoś z personelu klubu umieści wizerunek małoletniego zawodnika bez stosownej podstawy prawnej w formie portretowej w klubowych mediach społecznościowych?	Upubliczni w ten sposób wizerunek dziecka, będzie on dostępny dla każdego, kto ma dostęp do takiego konta społecznościowego.	Należy wprowadzić procedurę, która ureguje, kto w klubie odpowiada za dostęp do mediów społecznościowych i został stosownie do tego upoważniony oraz posiada odpowiednią wiedzę, na jakich podstawach prawnych można publikować wizerunki osób związanych z klubem, a w szczególności niepełnoletnich. Taka osoba powinna zostać przeszkolona, jeśli jest pracownikiem/współpracownikiem i nie miała wcześniej kontaktu z realizacją tego typu zadań.

Źródło: opracowanie własne.

19.3.3. METODA ILOŚCIOWO-JAKOŚCIOWA ANALIZY RYZYKA

Analiza ryzyka może być przeprowadzana na różnych poziomach szczegółowości w zależności od ryzyka, celu analizy, dostępnych informacji, danych i zasobów. Może być jakościowa, ilościowa oraz mieszana będąca kombinacją powyższych w zależności od okoliczności¹¹⁰. Metoda mieszana polega na łączeniu metod jakościowej i ilościowej, by stworzyć jak najbardziej rzeczywisty obraz identyfikowanych ryzyk. Wówczas z metody jakościowej otrzymamy odpowiedzi i opinie osób, które brały udział w szacowaniu ryzyk ze swoich obszarów i procesów, a poprzez zastosowanie elementów metody ilościowej będziemy skalować odpowiedzi i opinie w sposób mierzalny.

¹¹⁰ Zarządzanie ryzykiem – zasady i wytyczne (5,4,3), PN-ISO 31000:2012.

PRZYKŁADOWY ARKUSZ ANALIZY RYZYKA METODĄ ILOŚCIOWO-JAKOŚCIOWĄ

Numer ryzyka	Zagrożenie	Wynik DPIA	Ocena zabezpieczeń	Uzasadnienie oceny zabezpieczeń	Prawdopodobieństwo	Skutek	Wartość ryzyka
1.	Zagrożenie utraty danych. W pomieszczeniu klubu, do którego wchodzi wiele osób, znajduje się laptop z nieszyfrowanym dyskiem twardym. W razie jego kradzieży może dojść do utraty danych sędziów, trenerów, zawodników oraz danych kadrowych, które przechowywane są na tym komputerze.	Ryzyko +1	Ryzyko -1	Zgodnie z procedurą pomieszczenie z laptopem nigdy nie pozostaje bez kontroli.	Średnie	Duży	Duże ryzyko
2.	Zagrożenie ujawnienia danych. Brak autoryzacji w pomieszczeniach klubu na drukarce lub urządzeniu wielofunkcyjnym powoduje możliwość wysłania danych poza klub przez osobę nieuprawnioną.	Ryzyko +1	Ryzyko -1	Każdy kto drukuje od razu odbiera z urządzenia swoje wydruki, nie zostawiając ich bez opieki. Takie zasady obowiązują na podstawie wdrożonej procedury.	Małe	Duży	Średnie ryzyko
3.	Zagrożenie przetwarzania danych bez podstawy prawnej. Trener spisał na kartce dane osobowe od rodziców/opiekunów prawnych zawodnika, który uczestniczy w treningu testowym pierwszy raz i nie odebrał stosownych zgód na przetwarzanie tych danych.	Ryzyko +1	Ryzyko +1	Rodzice, przekazując trenerowi dane, są świadomi, że będą one przetwarzane dla celów realizacji treningu i że żadna inna niepowołana osoba nie otrzyma tych danych, gdyż trener występuje jako przedstawiciel klubu, został upoważniony i działa zgodnie z procedurami klubowymi w zakresie ochrony danych osobowych. A przy najbliższym już potestowym treningu zostaną dopełnione wszystkie formalności na formularzach klubowych rejestracji zawodnika.	Małe	Mały	Małe ryzyko

DPIA (ang. *data protection impact assessment*) – proces oceny skutków dla ochrony danych

Źródło: opracowanie własne.

19.4. PLAN POSTĘPOWANIA Z RYZYKIEM I JEGO MONITOROWANIE

W dalszym kroku, jeśli administrator dokona już identyfikacji i określenia ryzyk, należy przejść do momentu, w którym kierownictwo organizacji musi odpowiedzieć sobie na pytanie, czy samo określenie, że w organizacji sportowej występują ryzyka wystarczy. Niestety, nie możemy w tym procesie poprzestać na tym etapie, teraz należałoby przystąpić do zarządzania ryzykiem. Podobnie jak proces analizy, tak i dalsze postępowanie z ryzykiem musi być możliwe do udowodnienia na potrzeby zapewnienia zgodności z RODO.

Przed administratorem zadanie określenia, w jaki sposób należy postąpić ze zidentyfikowanymi ryzykami. Na potrzeby zgodności z RODO należałoby rozpocząć od redukcji ryzyka i przejść przez etapy:

- ▶ redukcji ryzyka – czyli jego zmniejszenia do poziomu akceptowalności;
- ▶ unikania ryzyka – czyli niegenerowania sytuacji powodujących to ryzyko w praktyce działalności podmiotu sportowego;
- ▶ przeniesienia ryzyka – czyli przeniesienia ryzyka na inny podmiot, aby np. zastosować i wdrożyć zabezpieczenia zasobów, w których ryzyko się pojawiło;
- ▶ systematycznej oceny poziomu ryzyka – czyli należy stosować stały/okresowy monitoring poziomu ryzyka w stosunku do konkretnego zagrożenia;
- ▶ zwrócenia się do organu nadzorczego z wnioskiem o konsultację¹¹¹.

Z wnioskiem o uprzednie konsultacje należy wystąpić w sytuacji, gdy na liście badanych operacji przetwarzania znajdują się operacje, dla których ryzyko naruszenia praw i wolności oszacowane zostało jako wysokie i gdy administrator danych nie może znaleźć środków wystarczających do zmniejszenia (zminimalizowania) tego ryzyka do dopuszczalnego poziomu.

Proces zarządzania ryzykiem powinien być usystematyzowany i udokumentowany. Aby stworzyć plan postępowania z ryzykiem, należy zebrać i przeanalizować takie dokumenty, jak:

- ▶ polityka zarządzania ryzykiem w organizacji;
- ▶ rejestr ról, obowiązków i odpowiedzialności pracowników, współpracowników podmiotu sportowego;
- ▶ struktura podziału pracy;
- ▶ szablon planu zarządzania.

Jeśli wcześniej przeprowadzane były już w organizacji analizy ryzyka, to dalszy etap zależy od tego, czy podmiot ma już wcześniej przygotowany plan postępowania

¹¹¹ UODO, *Kto i w jakich sytuacjach zobowiązany jest do złożenia wniosku o uprzednie konsultacje?*, <https://uodo.gov.pl/pl/127/216> [dostęp: 10.08.2025].

z ryzykiem (wówczas wymagać on będzie tylko aktualizacji), czy może potrzebuje zupełnie nowego.

W szacowaniu ryzyka może również dojść do sytuacji, w której pojawi się ryzyko, co do którego nie podjęliśmy procesu zarządzania i nie zastosowaliśmy żadnej metody postępowania z tym ryzykiem ze względu na różne aspekty, takie jak ponoszenie kosztów, konieczność dokonywania zmian, brak czasu itd. Zazwyczaj dotyczy to ryzyk, które znalazły się poniżej granicy akceptowalności administratora. Mówimy wtedy o ryzyku szczątkowym, czyli ryzyku, które pozostaje po wprowadzeniu zabezpieczeń¹¹². Ryzyko szczątkowe jest na tyle niskie, że zarządzanie nim okazuje się zbędne. Należy pamiętać, że nigdy w organizacji nie uda się całkowicie wyeliminować ryzyka, bo zawsze może pojawić się następne zagrożenie, które wcześniej nie zostanie przewidziane, szczególnie w tak dynamicznym obszarze działalności jak sport.

19.5. REGULARNE TESTOWANIE, MIERZENIE I OCENIANIE SKUTECZNOŚCI ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH MAJĄCYCH ZAPEWNIĆ BEZPIECZEŃSTWO PRZETWARZANIA

Obowiązkiem administratora jest wdrożenie i utrzymywanie takich środków technicznych i organizacyjnych, aby zapewniały one bezpieczeństwo przetwarzania danych osobowych, przy czym nakład sił i środków musi być proporcjonalny do poziomu ryzyka jakie wiąże się z przetwarzaniem. Tutaj należy pamiętać, aby środki te poddawać regularnemu testowaniu, mierzeniu i ocenie skuteczności w odniesieniu do obowiązku wynikającego z art. 32 ust. 1 lit. d) RODO).

19.6. HARMONOGRAM PRAC ZARZĄDZANIA RYZYKIEM

Kiedy powstanie plan postępowania z ryzykiem, i wiemy już, jakie mamy ryzyka oraz jak będziemy z nimi postępować i je monitorować, należy przygotować harmonogram działań, a także ustalić sposoby komunikacji i przepływu dokumentów pomiędzy osobami wyznaczonymi w podmiocie sportowym do tego zadania.

¹¹² D. Wróblewski, T. Sowa, *Zarządzanie ryzykiem. Zagadnienia ogólne. Materiały dydaktyczne ze szkolenia dla auditorów działających w strukturze Polskiego Centrum Akredytacji*, Józefów 2009.

Wydaje się, że na tym etapie już wszystko zostało określone i przygotowane, jednak przed podmiotami wciąż jeszcze wiele zadań i pracy, dlatego ważne jest, aby rozplanować realizację tych zadań w czasie oraz przypisać je do konkretnych osób.

UWAGA!

Ważne jest, aby zakomunikować pracownikom i współpracownikom, że zostały zidentyfikowane ryzyka w działalności podmiotu sportowego i że powstał plan postępowania na wypadek ich wystąpienia.

19.7. PODSUMOWANIE

Każda ocena ryzyka niezależnie od wykorzystanej metody powinna pozwolić zidentyfikować zagrożenia, na które mogą być narażone wszystkie osoby, których dane osobowe przetwarza administrator, oraz środowisko sportowe i okołosportowe w miejscu wydarzenia lub w określonej jego części. Zidentyfikować należy konkretne grupy ludzi, którzy mogą być narażeni na ryzyko, ustalając, gdzie i w jakim momencie może ono wystąpić.

Ryzyko jest zazwyczaj identyfikowane z poniesieniem straty. Zwalczanie ryzyka może skupiać się na identyfikowaniu przyczyn oraz zapobieganiu skutkom zdarzeń albo też identyfikowaniu skutków i usuwaniu przyczyn. Zarządzanie ryzykiem jest zatem przydatnym narzędziem służącym do minimalizacji niepowodzenia w przypadku działalności każdego podmiotu sportowego, w szczególności by wykazać pełną zgodność z RODO w procesach ochrony prywatności i bezpieczeństwa danych osobowych dla potrzeb szeroko prowadzonej działalności sportowej.

20. OCENA SKUTKÓW DLA OCHRONY DANYCH

ART. 35 RODO. OCENA SKUTKÓW DLA OCHRONY DANYCH

„Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę”.

Ogólne rozporządzenie o ochronie danych (RODO) nakłada na administratorów danych m.in. obowiązek przeprowadzenia w przypadku dużego prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych procesu oceny skutków dla ochrony danych (DPIA). Ten wymóg wywołuje wiele pytań, wątpliwości, głównie dotyczących praktycznych kwestii związanych z procesem oceny, kiedy przeprowadzenie oceny skutków jest obowiązkowe, a w których sytuacjach nie jest konieczne, ponieważ RODO nie obliguje do przeprowadzenia oceny skutków ochrony danych w każdym procesie przetwarzania. Ocena ta jest obligatoryjna tylko wówczas, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1, 3 i 4 RODO), a w szczególności jest to konieczne w przypadku:

- ▶ systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- ▶ przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO; lub
- ▶ systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Ocena skutków dla ochrony danych to proces, który powinno się dostosować do zasad ochrony danych obowiązujących w organizacji i który pozwoli na ich bezpieczne przetwarzanie, m.in. przez podjęcie kluczowych decyzji już w fazie projektowania (patrz: *Zasada privacy by design*), domyślną ochronę danych (patrz: *Zasada privacy by default*) oraz wczesną minimalizację potencjalnych ryzyk prywatności. Warto zauważyć, że ocenę skutków dla ochrony danych osobowych należy przeprowadzać przed rozpoczęciem przetwarzania, co oznacza, że DPIA powinna być wykonana na etapie planowania nowych projektów i czynności związanych z przetwarzaniem danych bądź na etapie planowania modyfikacji w istniejących już procesach. Przeprowadzone DPIA pozwoli więc w podmiotach sportowych na wykazanie zgodności ich działań z RODO oraz opracowanie planu działania, aby ograniczać ryzyka dla ochrony danych osobowych. Będzie on wspierać podmioty sportowe w sytuacjach, w których rozpoczną pracę nad nowymi projektami rozwijającymi poszczególne dyscypliny sportu, by dzięki temu mogły identyfikować oraz minimalizować ryzyka związane z ochroną prywatności przed wdrożeniem nowych rozwiązań, oraz pozwoli na identyfikację możliwych problemów na wstępnym etapie i ułatwi ich wczesne rozwiązanie.

Aby ułatwić przeprowadzanie DPIA, organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych. Podstawą ogłoszenia Komunikatu Prezesa Urzędu Ochrony Danych Osobowych jest art. 54 ust. 1 pkt 1 w związku z art. 172 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Wykaz stanowi załącznik do Komunikatu Prezesa Urzędu Ochrony Danych. Wykaz ten w żaden sposób nie narusza ogólnego obowiązku administratora do dokonania właściwej oceny ryzyka i zarządzania ryzykiem. Przeprowadzenie oceny skutków dla ochrony danych nie zwalnia również administratora z innych obowiązków określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. oraz z obowiązków określonych w innych właściwych przepisach. Wykaz ten nie narusza nadrzędnego obowiązku administratora do przeanalizowania wszelkich operacji przetwarzania danych w oparciu o pełną ocenę skutków dla ochrony danych na podstawie art. 35 ust. 1 RODO. To bardzo istotny dokument, ponieważ podmioty sportowe, które przetwarzają dane w sposób wskazany w wykazie, będą zobligowane do wykonania oceny skutków przetwarzania danych dla ich ochrony. Jej brak może zostać uznany za naruszenie RODO i obarczony sankcją. Wykaz przygotowany przez PUODO ma charakter uzupełniający i administratorzy przetwarzający dane w sposób, który znajduje się w wykazie, mogą być pewni, że wykonanie oceny skutków przetwarzania danych dla ich ochrony będzie w tym przypadku obowiązkowe.

Szczególnie istotne w wykazie są pozycje, które mogą odnosić się do bardzo wielu podmiotów przetwarzających dane w podobny sposób. Administratorzy powinni

zweryfikować, czy sposób, w jaki przetwarzają dane, znajduje się w wykazie. Ci, którzy przetwarzają dane w inny sposób, powinni zweryfikować, czy ich sposób przetwarzania nie powoduje wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

Niewykonanie oceny skutków, w sytuacji, gdy powinna ona być wykonana, lub niewłaściwe wykonanie takiej oceny może zostać uznane za naruszenie RODO, a co za tym idzie, być obarczone dotkliwą karą finansową.

PRZYKŁAD

Przetwarzanie danych w podmiotach sportowych posiadających systemy monitorowania czasu pracy pracowników oraz wykorzystanych przez nich narzędzi (poczty elektronicznej, internetu) zostało objęte obowiązkiem wykonania oceny skutków.

UWAGA!

Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę, jednak w niektórych okolicznościach rozsądniej byłoby nie ograniczać oceny skutków dla ochrony danych do pojedynczego projektu. Przykład: podmioty sportowe planują wdrożyć wspólny projekt, np. aplikację lub platformę do korzystania przez różne struktury w organizacji (trenerów, sędziów, obserwatorów) w środowisku ich przetwarzania na dużą skalę.

W procesie oceny skutków przetwarzania dla ochrony danych należałoby także zwrócić uwagę i ustalić rolę inspektora ochrony danych wyznaczonego w podmiotach sportowych. Istotne jest, że to administrator zgodnie z RODO zobowiązany jest do wdrożenia odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych, zatem to administrator musi dokonać oceny, czy wprowadzone do tej pory środki ochrony wystarczają do zapewnienia bezpieczeństwa przetwarzania danych osobowych. Natomiast gdy określony rodzaj przetwarzania, szczególnie ten z wykorzystaniem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, wówczas administrator przed rozpoczęciem przetwarzania powinien zawsze dokonać oceny skutków planowanych operacji przetwarzania co do ochrony danych osobowych. Przepisy jednoznacznie wskazują, że przeprowadzenie takiej oceny jest obowiązkiem administratora. Nie oznacza to oczywiście, że inspektor w takiej sytuacji pozostaje bierny i nie wspiera administratora. Jego zadaniem jest

monitorowanie prawidłowości przeprowadzenia oceny i kontrola jej zgodności z prawem (art. 39 ust. 1 lit. c RODO).

UWAGA!

Nie należy delegować przeprowadzenia oceny skutków inspektorowi, gdyż wówczas doszłoby do konfliktu interesów, co doprowadziłoby do naruszenia przepisu art. 38 ust. 6¹¹³ RODO.

Jak powinna zatem wyglądać współpraca pomiędzy administratorem a inspektorem ochrony danych na gruncie oceny skutków dla ochrony danych? Przepisy RODO są w tej kwestii dość lakoniczne, w związku z tym warto sięgnąć do wytycznych Grupy Roboczej art. 29¹¹⁴. Grupa Robocza wyjaśnia, jaka jest rola inspektora ochrony danych w procesie dokonywania oceny skutków. Na tej podstawie można ustalić precyzyjny podział obowiązków pomiędzy administratorem a inspektorem, ale to administrator powinien zasięgnąć porady inspektora ochrony danych w kwestii, czy należy przeprowadzić ocenę skutków co do ochrony danych. Jeżeli ocena mimo rekomendacji inspektora nie zostanie przeprowadzona, ponieważ administrator nie zgodzi się z zaleceniami IOD, wówczas powinien w dokumentacji oceny skutków dla ochrony danych zawrzeć pisemne uzasadnienie nieuwzględnienia tych zaleceń. W związku z tym dokumentację należy uzupełnić o:

- ▶ stanowisko przedstawione przez inspektora ochrony danych;
- ▶ stanowisko administratora zawierające wskazania oraz wyjaśnienie powodów, dla których nie zastosował się do zaleceń wydanych przez inspektora ochrony danych.

Pamiętać należy, że to administrator powinien uzasadnić i udokumentować powody, dla których nie wykonano oceny. Opinia inspektora nie jest dla administratora wiążąca, jednak za nieprzeprowadzenie oceny, w przypadku gdy jest ona wymagana, odpowiedzialność poniesie sam administrator.

Ocena skutków w odniesieniu do ochrony danych to proces umożliwiający opisanie przetwarzania oraz ocenę jego konieczności i proporcjonalności. DPIA ma wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych i określenie środków pozwalających zaradzić tym czynnikom ryzyka. Ocena skutków w odniesieniu do ochrony danych stanowi zatem

¹¹³ P. Fajgielski, *Ogólne rozporządzenie...*, *op.cit.*, Komentarz do art. 38 ust. 6.

¹¹⁴ Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679.

podstawowe narzędzie służące do wykazania, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO (patrz: Zasada rozliczalności).

PRZYKŁAD

Klub zamierza wprowadzić nowy system dla zawodników w postaci monitorujących kamizelek lub opasek. System ma zapewnić rozszerzony, szczegółowy wgląd w stan zdrowia, samopoczucie i ogólne wyniki zawodnika, monitorować sen i zbierać dane biometryczne, takie jak obciążenie układu krążenia i mięśni. To rozwiązanie do monitorowania obejmuje informacje medyczne i treningowe, zapewnia trenerom, szkoleniowcom i personelowi sportowemu rozbudowany zestaw narzędzi do przygotowywania sportowców i zespołów. System pomaga unikać kontuzji i zwiększać wyniki na treningach, co przekłada się na lepsze rezultaty. Istotne kryteria do przeprowadzenia DPIA w takim przypadku to systematyczne monitorowanie zawodnika, innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych, dopasowanie lub łączenie różnych zbiorów danych. Na administratorze spoczywa więc obowiązek przeprowadzenia DPIA przed wprowadzeniem takiego narzędzia.

CZĘŚĆ II
SZCZEGÓŁOWA

1. PRZETWARZANIE DANYCH OSOBOWYCH W POSTACI WIZERUNKU

1.1. DEFINICJA WIZERUNKU

Obowiązujące przepisy prawa nie zawierają definicji wizerunku osoby fizycznej. Zgodnie z orzecznictwem sądów za wizerunek należy uznać różne cechy fizyczne człowieka tworzące jego wygląd, w tym zarówno twarz, jak i np. charakterystyczna sylwetka. Według niektórych poglądów prezentowanych przez polskie sądy w ramy wizerunku można włączyć również elementy dodatkowe, takie jak ubiór, fryzura, okulary, czy charakterystyczny zawód, np. sportowiec. Wizerunek pozwala zidentyfikować daną osobę.

UWAGA!

Elementem decydującym o tym, czy możemy mówić o wizerunku danej osoby nie jest wyłącznie jej twarz, lecz fakt, że osoba ta jest rozpoznawalna.

1.2. REGULACJE PRAWNE DOTYCZĄCE WIZERUNKU

Ochronie prawnej podlega prawo do wizerunku rozumiane jako kompetencja o charakterze wyłącznym do decydowania o rozpowszechnianiu utrwalonego wizerunku tej osoby przez osobę trzecią. Za dobro chronione uznaje się autonomię każdej osoby co do swobodnego rozstrzygania, czy w ogóle, a jeśli tak, to w jakich okolicznościach wizerunek tej osoby może być rozpowszechniany¹¹⁵.

¹¹⁵ Wyrok Sądu Apelacyjnego w Krakowie z dnia 19 grudnia 2002 r., sygn. akt I ACa 957/01.

Wizerunek danej osoby to zarówno dobro osobiste, jak i dana osobowa. Wizerunek podlega ochronie na podstawie przepisów Kodeksu cywilnego¹¹⁶ oraz ustawy o prawie autorskim i prawach pokrewnych¹¹⁷. Wskazane regulacje uzupełniają się. Dodatkowo, wizerunek podlega również ochronie na podstawie przepisów dotyczących ochrony danych osobowych, tj. RODO, oraz ustawy o ochronie danych osobowych.

UWAGA!

Cechą wspólną regulacji Kodeksu cywilnego i ustawy o prawie autorskim i prawach pokrewnych oraz regulacji RODO jest to, że w żadnej z nich nie musi istnieć możliwość dokładnego ustalenia tożsamości danej osoby (np. jej imienia i nazwiska). Wystarczające jest wskazanie takich unikalnych cech tej osoby, które odróżniają ją od innych. Chodzi więc o wyodrębnioną osobę fizyczną, a niekoniecznie osobę fizyczną znaną administratorowi¹¹⁸.

1.3. USTAWA O PRAWIE AUTORSKIM I PRAWACH POKREWNYCH

ART. 81 USTAWY O PRAWIE AUTORSKIM I PRAWACH POKREWNYCH. ZEZWOLENIE NA ROZPOWSZECHNIANIE WIZERUNKU

„1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

2. Zezwolenia nie wymaga rozpowszechnianie wizerunku:

- 1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
- 2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza”.

¹¹⁶ Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2023 r. poz. 1610 z późn. zm.).

¹¹⁷ Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2025 r. poz. 24 z późn. zm.).

¹¹⁸ M. Gumularz, P. Kozik (red.), *Ochrona danych osobowych w marketingu i sprzedaży*, wyd. 1, Warszawa 2019.

Zgodnie z art. 81 ustawy o prawie autorskich i prawach pokrewnych rozpowszechnienie wizerunku co do zasady wymaga zezwolenia przedstawionej osoby.

UWAGA!

Rozpowszechnianie wizerunku oznacza różne formy jego publicznego udostępniania, które powodują, że dostęp do wizerunku ma nieograniczony krąg odbiorców. Rozpowszechnianie wizerunku to publikowanie wizerunku w mediach społecznościowych (również w ramach tzw. relacji, których czas publikacji, w odróżnieniu od standardowych postów, jest dość krótki), na stronie internetowej, w serwisie internetowym, telewizji, na plakatach, broszurach czy w innych publikacjach drukowanych. Z punktu widzenia definicji rozpowszechniania wizerunku nie ma znaczenia cel, w jakim następuje takie rozpowszechnienie, tj. bez względu na to, czy publikacja służy osiągnięciu korzyści finansowych czy ma charakter niekomercyjny, np. służy promocji kultury fizycznej lub określonej dyscypliny sportowej, publikowanie wizerunku w taki sposób, że może zapoznać się z nim publiczność, stanowi jego rozpowszechnianie. Rozpowszechnianiem wizerunku będzie również udostępnienie go w mediach społecznościowych w tzw. grupie zamkniętej, jeżeli grupa ta będzie liczna (np. 300 osób).

Zezwolenie na rozpowszechnianie wizerunku może stanowić samodzielne oświadczenie, może być również wprowadzone do treści umowy lub regulaminu. Przykładem wprowadzenia zezwolenia do treści umowy będzie kontrakt zawodniczy określający m.in. zasady wykorzystania wizerunku sportowca do celów marketingowych klubu, np. jego uczestnictwo w akcjach promujących klub lub promocji określonych zawodów czy rozgrywek. Z tytułu wyrażenia przez sportowca wspomnianej zgody najczęściej jest mu wypłacane wynagrodzenie, np. jako element całkowitego wynagrodzenia wynikającego z umowy.

Za dopuszczalne należy uznać umieszczenie w treści regulaminu imprezy sportowej klauzuli zawierającej zezwolenie na rozpowszechnianie wizerunku kibica podczas transmisji tego wydarzenia. Takie zezwolenie będzie skutecznie wyrażone pod warunkiem wcześniejszego udostępnienia kibicowi treści wspomnianego regulaminu, np. w momencie zakupu biletu. Podobna sytuacja może dotyczyć zawodnika biorącego udział w lokalnym turnieju piłki nożnej. Rozpowszechnianie wizerunku wspomnianego zawodnika może nastąpić w związku z relacjonowaniem czy dokumentowaniem turnieju przez jego organizatora. Zawodnik przed dokonaniem rejestracji na turniej powinien być poinformowany o treści regulaminu i zaakceptować jego warunki.

UWAGA!

Należy pamiętać o tym, że czym innym jest wykorzystanie wizerunku w relacji czy transmisji z imprezy sportowej, a czym innym wykorzystanie wizerunku w spocie promującym dane wydarzenie. Relacja imprezy sportowej może być postrzegana jako naturalna konsekwencja uczestnictwa w wydarzeniu. Relacja z wydarzenia pokazuje jego przebieg i stanowi dokumentację tego, co faktycznie miało miejsce. Spot promocyjny wykracza poza zakres dokumentalny. W spocie promocyjnym uczestnicy mogą być przedstawiani w sposób, który wpływa na ich odbiór publiczny. Tego rodzaju materiał może być wielokrotnie emitowany w różnych mediach (np. w telewizji), co zwiększa zasięg i skalę ekspozycji wizerunku danej osoby. Ponadto wizerunek może być ukazwany w określonych kontekstach, w połączeniu np. z logotypami sponsorów (zarówno firmami prywatnymi, jak i podmiotami publicznymi), może być również poddawany obróbce. Zezwolenie na wykorzystanie wizerunku w relacji z wydarzenia nie obejmuje automatycznie zezwolenia na udział w spocie promocyjnym, ponieważ charakter i cel obu form są zupełnie inne. Umieszczanie zezwolenia na rozpowszechnianie wizerunku w spocie promującym dane wydarzenie sportowe w regulaminie imprezy należy uznać za rozwiązanie nieprawidłowe. Tego typu zapisy zawarte w regulaminie ograniczają możliwość danej osoby do decydowania o wykorzystaniu jej wizerunku i wkraczają daleko w jej sferę prywatności. W takim przypadku należy uzyskać odrębne oświadczenie o wyrażeniu zezwolenia na rozpowszechnianie wizerunku w celach promocyjnych w postaci spotu.

Zezwolenie na rozpowszechnianie wizerunku wyrażone na podstawie art. 81 ustawy o prawie autorskim i prawach pokrewnych może stanowić część regulaminu, pod warunkiem że spełnia wymogi dobrowolności, świadomości i możliwości wycofania. Jego warunki nie mogą również w sposób nieproporcjonalny ograniczać prawa danej osoby do decydowania o swoim wizerunku. Zapisy regulaminu, które w sposób szeroki, niczym nieograniczony narzucają kibicowi czy zawodnikowi wykorzystanie jego wizerunku bez wynagrodzenia, w celach komercyjnych czy reklamowych, przez bliżej niesprecyzowany czas, mogą być uznane za niedozwoloną klauzulę umowną (np. publikacja wizerunku kibica na plakatach reklamujących kolejną edycję imprezy sportowej, publikacja wizerunku zawodnika amatora w filmie promującym daną imprezę sportową). Za nieprawidłową praktykę należy również uznać stosowanie bardzo ogólnych zapisów w regulaminie, na bazie których trudno jest określić, w jaki sposób i w jakim celu wizerunek będzie wykorzystywany. Zapis regulaminu powinien jednoznacznie wskazywać na treść zezwolenia zgodnie z poniższymi wytycznymi.

Zezwolenie powinno dotyczyć konkretnych uzgodnień co do rozpowszechniania wizerunku, co oznacza, że powinno wskazywać:

- ▶ szczegółowy sposób rozpowszechniania wizerunku i miejsce, w którym to będzie następować (np. media społecznościowe, plakaty, ulotki, raporty, konkretne strony internetowe);
- ▶ cel rozpowszechniania (np. promocja projektu sportowego, reklama klubu sportowego, umożliwienie śledzenia w czasie rzeczywistym rozgrywek sportowych, zaprezentowanie członków drużyny, upowszechnianie danej dyscypliny sportowej, informowanie o przebiegu rozgrywek);
- ▶ warunki, na jakich wizerunek będzie rozpowszechniany (np. w postaci zdjęcia, nagrania, opatrzony podpisem, komentarzem, skadrowany, edytowany, w formie postu, relacji, transmisji, w materiale oznaczonym logotypem sponsora lub donora);
- ▶ podmiot, na rzecz którego jest wyrażane zezwolenie (np. dany klub sportowy, organizator turnieju);
- ▶ określony czas, przez który podmiot sportowy jest uprawniony do rozpowszechniania wizerunku.

Zezwolenie nie jest wymagane jedynie w następujących przypadkach:

- ▶ osoba otrzymała umówioną zapłatę za pozowanie, np. sportowiec będący modelem w kampanii reklamowej;
- ▶ osoba jest powszechnie znana, a wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych – np. wizerunek znanego sportowca utrwalony podczas relacji z zawodów, w których bierze udział;

UWAGA!

Powyższe nie dotyczy publikacji wizerunku w celach komercyjnych, jak również publikacji wizerunku jakiegokolwiek sportowca. W przypadku skorzystania z tego wyłączenia muszą być spełnione dwie przesłanki: sportowiec jest osobą znaną, publikacja wizerunku następuje w związku z realizacją jego roli zawodowej.

- ▶ wizerunek osoby stanowi jedynie szczegół takiej całości, jak zgromadzenie, krajobraz, publiczna impreza, np. zdjęcie publiczności na trybunach wykonane w planie ogólnym, tj. bez kadrowania konkretnych osób.

Jeżeli wizerunek jest jedynie elementem zdjęcia, stanowi jego małą część i w jego usunięcie nie zmieniliby przedmiotu i charakteru tego, co jest na zdjęciu pokazane, zgodnie z obowiązującymi przepisami nie ma potrzeby uzyskiwania zezwolenia na jego rozpowszechnianie. Jeżeli zatem zdjęcie z imprezy sportowej, zawodów sportowych,

pikniku sportowego będzie miało na celu przedstawienie tego wydarzenia, jego uczestnicy nie będą elementem dominującym (wizerunek danej osoby nie będzie przykuwał uwagi ze względu na szczególne walory czy cechy, nie będzie wykorzystane kadrowanie konkretnej osoby), zdjęcie będzie wykonane bez zbliżeń na daną osobę czy małą grupę osób, to można oprzeć się na powyższym wyłączeniu.

Jednocześnie pomimo braku konieczności uzyskania zezwolenia na rozpowszechnianie wizerunku zgodnie z art. 81 ustawy o prawie autorskim i prawach pokrewnych, jeżeli uwidoczniona na zdjęciu osoba będzie możliwa do zidentyfikowania, będzie przedstawiona w sposób wyraźny (pomimo faktu pokazania jej w dużej grupie osób lub pomimo faktu, że jest to osoba pełniąca funkcję publiczną), **wizerunek będzie stanowił daną osobową i niezbędne będzie stosowanie w tym zakresie regulacji dotyczących przetwarzania danych osobowych.**

UWAGA!

Zezwolenie na rozpowszechnienie wizerunku, o którym mowa w art. 81 ustawy o prawie autorskim i prawach pokrewnych, nie jest tożsame ze zgodą na przetwarzanie danych osobowych. Rozpowszechnianie wizerunku może stanowić przetwarzanie danych osobowych, co wiąże się z koniecznością ustalenia podstawy prawnej tego przetwarzania. Zgoda na przetwarzanie danych osobowych w postaci wizerunku zazwyczaj ma charakter szerszy niż zezwolenie na rozpowszechnienie wizerunku. Zgoda na przetwarzanie danych osobowych może dotyczyć różnych działań związanych z danymi osobowymi w postaci wizerunku (np. przechowywania), natomiast zezwolenie na rozpowszechnianie wizerunku dotyczy wyłącznie jego publicznego ujawnienia.

1.4. WIZERUNEK JAKO DANA OSOBOWA

UWAGA!

Przetwarzanie danych osobowych w postaci wizerunku to zarówno jego rozpowszechnianie, jak i utrwalanie (nagrywanie relacji wideo, robienie zdjęć), przechowywanie (na komputerze, telefonie), usuwanie (wykasowanie), modyfikowanie (obróbka), ujawnianie (przesyłanie plików ze zdjęciami e-mailem). Wszystkie wymienione czynności dokonywane na wizerunku stanowią operacje przetwarzania danych osobowych.

Przetwarzanie danych osobowych w postaci wizerunku może następować na następujących podstawach prawnych (patrz: Podstawy prawne przetwarzania danych osobowych):

- ▶ zgoda (art. 6 ust. 1 lit. a RODO);
- ▶ prawnie uzasadniony interes administratora danych (art. 6 ust. 1 lit. f RODO);
- ▶ realizacja umowy (art. 6 ust. 1 lit. b RODO);
- ▶ realizacja obowiązku prawnego administratora (art. 6 ust. 1 lit. c RODO).

1.4.1. ZGODA (ART. 6 UST. 1 LIT. A RODO)

Co do zasady zgoda na przetwarzanie danych osobowych będzie stanowiła podstawę prawną przetwarzania danych osobowych w postaci wizerunku w przypadku, w którym dochodzi do rozpowszechniania wizerunku danej osoby i rozpowszechnianie to wymaga uzyskania zezwolenia zgodnie z art. 81 ustawy o prawie autorskim i prawach pokrewnych, np. umieszczanie zdjęć niepełnoletnich zawodników na profilu w mediach społecznościowych klubu w celach promocyjnych klubu czy publikacja zdjęć pracowników klubu sportowego na stronie internetowej tego klubu. Jeżeli celem organizacji sportowej jest publiczne udostępnienie wizerunku w kampaniach reklamowych, marketing swojej działalności, przetwarzanie danych osobowych w postaci wizerunku powinno następować na podstawie zgody.

1.4.2. PRAWNIE UZASADNIONY INTERES ADMINISTRATORA DANYCH (ART. 6 UST. 1 LIT. F RODO)

WYJĄTKI OD UZYSKIWANIA ZEZWOLENIA NA ROZPOWSZECHNIANIE WIZERUNKU

Prawnienie uzasadniony interes administratora może być właściwą podstawą przetwarzania wizerunku w sytuacjach, gdy organizacja sportowa może skorzystać z wyłączeń od obowiązku uzyskiwania zgody na rozpowszechnienie wizerunku, o których mowa w art. 81 ustawy o prawie autorskim i prawach pokrewnych, np. zdjęcie publiczności na trybunach wykonane w planie ogólnym, zdjęcia znanego sportowca wykonane podczas jego udziału we współzawodnictwie sportowym.

ZGODA A UZASADNIONY INTERES ADMINISTRATORA

Uzasadniony interes administratora może stanowić również podstawę prawną przetwarzania wizerunku w sytuacjach, gdzie zgodnie z art. 81 ustawy o prawie autorskim i prawach pokrewnych wymagane jest zezwolenie na rozpowszechnianie wizerunku. Decyzja o tym, czy skorzystać z podstawy zgody, czy uzasadnionego interesu, zależy m.in. od przeprowadzenia **testu równowagi**. Test ten pozwala ocenić, czy prawa i wolności osoby, której wizerunek jest przetwarzany, nie przeważają nad

interesami administratora. Jeżeli okaże się, że interesy osoby są nadrzędne, wówczas organizacja powinna uzyskać zgodę na przetwarzanie wizerunku.

PRZYKŁAD

Uzasadniony interes administratora mógłby być podstawą przetwarzania danych osobowych w postaci wizerunku podczas transmisji czy relacji z imprezy sportowej (np. w postaci nagrań lub zdjęć), gdzie dochodzi do uwidocznienia wizerunków konkretnych osób, takich jak kibice, zawodnicy czy obsługa imprezy. W takim przypadku zezwolenie na rozpowszechnianie wizerunku mogłoby zostać uwzględnione w regulaminie imprezy, a podstawą prawną przetwarzania danych osobowych byłby art. 6 ust. 1 lit. f RODO.

PRZETWARZANIE WIZERUNKU BEZ ROZPOWSZECHNIANIA

Uzasadniony interes administratora może również stanowić podstawę przetwarzania wizerunku, gdy nie chodzi o jego publiczne rozpowszechnianie.

PRZYKŁADY

Wykorzystanie wizerunku w celach wewnętrznych, np. do rozliczeń, sprawozdań lub celów szkoleniowych.

Nagrania z monitoringu wizyjnego w celu zapewnienia bezpieczeństwa podczas imprezy sportowej.

1.4.3. REALIZACJA UMOWY (ART. 6 UST. 1 LIT B RODO)

Umowa będzie stanowiła podstawę prawną przetwarzania danych osobowych w sytuacji, w której dane osobowe w postaci wizerunku będą niezbędne do wykonania umowy lub do podjęcia działań przed jej zawarciem.

PRZYKŁADY

Przedmiotem umowy jest przeprowadzenie instruktażu prawidłowego wykonywania ćwiczeń, który jest nagrywany, a następnie publikowany w określonym miejscu, np. na kanale YouTube związku sportowego.

Przedmiotem umowy jest udział w kampanii promującej określoną dyscyplinę sportową. Przedmiotem umowy jest publikacja kalendarza ze zdjęciami reprezentantów klubu.

Przedmiotem umowy jest wykorzystanie wizerunku sportowca przez klub sportowy (np. w ramach kontraktu zawodniczego) lub sponsora (np. w ramach indywidualnej umowy sponsoringowej).

1.4.4. REALIZACJA OBOWIĄZKU PRAWNEGO ADMINISTRATORA (ART. 6 UST. 1 LIT C RODO)

Przesłanka ta będzie miała zastosowanie w sytuacjach, w których przetwarzanie wizerunku stanowi obowiązek wynikający z przepisów prawa. W przypadku podmiotów sportowych znaczenie będą miały przepisy ustawy o bezpieczeństwie imprez masowych, w szczególności art. 11 ust. 4, który wskazuje na obowiązek utrwalania (za pomocą urządzeń rejestrujących obraz i dźwięk) przebiegu imprezy masowej odbywającej się na stadionach, obiektach i terenie wskazanych w wykazie wojewody¹¹⁹, oraz art. 13 wprowadzający obowiązek identyfikacji osób uczestniczących w meczu piłki nożnej¹²⁰.

1.5. CZŁONKOWIE KADRY NARODOWEJ I REPREZENTACJI OLIMPIJSKIEJ

ART. 14 USTAWY O SPORCIE. PRAWO DO WIZERUNKU ZAWODNIKA¹²¹

1. Członek kadry narodowej udostępnia, na zasadach wyłączności, swój wizerunek w stroju reprezentacji kraju polskiemu związkowi sportowemu, który jest uprawniony do wykorzystania tego wizerunku do swoich celów gospodarczych w zakresie wyznaczonym przez przepisy tego związku lub międzynarodowej organizacji sportowej działającej w danym sporcie.

2. Członek reprezentacji olimpijskiej udostępnia, na zasadach wyłączności, z chwilą powołania do reprezentacji olimpijskiej, swój wizerunek w stroju reprezentacji olimpijskiej Polskiemu Komitetowi Olimpijskiemu, który jest uprawniony do wykorzystani

¹¹⁹ Art. 11 ust. 4 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz.U. z 2023 r. poz. 616). Wojewoda w uzgodnieniu z komendantem wojewódzkim (Komendantem Stołecznym) Policji i z komendantem wojewódzkim Państwowej Straży Pożarnej, oraz po zasięgnięciu opinii właściwego polskiego związku sportowego, sporządza wykaz stadionów, obiektów lub terenów, na których utrwalanie przebiegu imprezy masowej za pomocą urządzeń rejestrujących obraz i dźwięk jest obowiązkowe. Umieszczenie w wykazie określonego stadionu, obiektu lub terenu następuje w drodze decyzji administracyjnej.

¹²⁰ Art. 13 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz.U. z 2023 r. poz. 616).

¹²¹ Ustawa z dnia 25 sierpnia 2010 o sporcie (Dz.U. z 2024 r. poz. 1488 z późn. zm).

tego wizerunku do swoich celów gospodarczych w zakresie wyznaczonym przez swoje przepisy lub przepisy Międzynarodowego Komitetu Olimpijskiego.

3. Zawodnik przed zakwalifikowaniem do kadry narodowej lub reprezentacji olimpijskiej wyraża zgodę na rozpowszechnianie swojego wizerunku w stroju reprezentacji kraju w rozumieniu art. 81 ust. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 r. poz. 2509 oraz z 2024 r. poz. 1222 i 1254).”

Sąd Najwyższy stwierdził, że polski związek sportowy **nie ma potrzeby uzyskiwania zgody poszczególnych sportowców na udostępnienie ich wizerunków**. Zdaniem Sądu Najwyższego z zakwalifikowaniem sportowca do kadry narodowej i wyrażeniem przez niego zgody na występowanie w reprezentacji kraju ustawodawca powiązał powstanie na rzecz polskiego związku sportowego prawa do wykorzystania wizerunku kadrowicza w stroju reprezentacji kraju. Jak wskazał Sąd Najwyższy, woła przynależności zawodnika do reprezentacji kraju jest równoznaczna z jego zgodą na wykorzystanie wizerunku w zakresie wskazanym w ustawie¹²².

Podstawą prawną przetwarzania danych osobowych w postaci wizerunku w tym przypadku będzie uzasadniony interes administratora danych osobowych (art. 6 ust. 1 lit f RODO). Z uwagi na treść art. 14 ustawy o sporcie zgoda na przetwarzanie danych osobowych w tym wypadku nie miałaby charakteru dobrowolnego, zatem nie mogłaby stanowić skutecznej przesłanki przetwarzania danych osobowych.

1.6. WIZERUNEK W MATERIALE PRASOWYM

ART. 2 PRAWA PRASOWEGO. OGRANICZENIE STOSOWANIA PRZEPISÓW DO DZIAŁALNOŚCI ZWIĄZANEJ Z MATERIAŁAMI PRASOWYMI, DZIAŁALNOŚCI LITERACKIEJ, ARTYSTYCZNEJ ORAZ WYPOWIEDZI AKADEMICKICH¹²³

„1. Do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914), a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5–9, art. 11, art. 13–16, art. 18–22, art. 27, art. 28 ust. 2–10 oraz art. 30 rozporządzenia 2016/679.

¹²² Wyrok Sądu Najwyższego z dnia 16 grudnia 2009 r., sygn. akt I CSK 160/09.

¹²³ Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914).

Zgodnie z art. 2 ust. 1 ustawy o ochronie danych osobowych do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe nie stosuje się części przepisów RODO, w tym m.in. dotyczących zasad przetwarzania danych (art. 5 RODO), przesłanek legalności przetwarzania danych osobowych (art. 6 RODO), obowiązków informacyjnych (art. 13 i 14 RODO). Oznacza to, że w sytuacji, w której np. zdjęcie ma charakter materiału prasowego (tj. opublikowanego lub przekazanego do opublikowania w prasie tekstu albo obrazu o charakterze informacyjnym, publicystycznym, dokumentalnym lub innym, niezależnie od środków przekazu, rodzaju, formy, przeznaczenia czy autorstwa¹²⁴), nie istnieje obowiązek ustalania podstawy prawnej przetwarzania danych osobowych w postaci wizerunku (w tym odbierania zgody na przetwarzanie danych osobowych) oraz spełniania obowiązku informacyjnego wobec osoby, której wizerunek jest wykorzystywany.

1.7. WIZERUNEK OSÓB NIEPEŁNOLETNICH

Poza omówionymi powyżej zagadnieniami w przypadku wykorzystania wizerunku dzieci należy dodatkowo pamiętać o tym, że:

- ▶ opublikowanie zdjęcia czy filmu (czyli rozpowszechnianie), na którym uwidoczony jest wizerunek dziecka (np. niepełnoletniego zawodnika), wymaga zgody jego przedstawiciela prawnego (rodzica bądź opiekuna prawnego). Z punktu widzenia zasad wykonywania władzy rodzicielskiej wystarczy, że zgoda zostanie wyrażona przez jednego z rodziców. Jednocześnie w przypadku jakichkolwiek sporów czy różnicy zdań pomiędzy rodzicami w tym zakresie, rekomenduje się przyjąć, że zgoda nie została wyrażona. Rekomenduje się zapytanie również dziecka, czy wyraża zgodę na publikację swojego wizerunku, w szczególności w sytuacji, w której proces rozwoju i dojrzałość dziecka wskazują na jego świadomość co do konsekwencji wyrażenia takiej zgody;
- ▶ dzieci podlegają szczególnej ochronie, dlatego do rozpowszechniania ich wizerunku należy podchodzić odpowiedzialnie i ostrożnie. Publikacja wizerunku w internecie może wiązać się z wieloma konsekwencjami, w tym zagrożeniami dla bezpieczeństwa dziecka, dlatego każda organizacja sportowa powinna szczegółowo przeanalizować decyzję o publikacji wizerunku dziecka, w szczególności biorąc pod uwagę cel takiej publikacji oraz konieczność jej dokonania. Warto, aby kwestie dotyczące rozpowszechniania wizerunku zostały uregulowane w polityce ochrony dzieci przed krzywdzeniem, którą wszystkie organizacje sportowe

¹²⁴ Art. 7 ust. 2 pkt 4 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914).

pracujące z dziećmi zobowiązane są przyjąć w ramach obowiązujących u nich standardów ochrony dzieci.

UWAGA!

Zgodnie z RODO dane osobowe dzieci podlegają szczególnej ochronie¹²⁵. Oznacza to, że przetwarzanie wizerunku niepełnoletniego zawodnika na podstawie uzasadnionego interesu administratora wymaga szczególnej ostrożności i dokładnego przeprowadzenia testu równowagi. Europejska Rada Ochrony Danych wskazuje, że art. 6 ust. 1 lit f RODO może być stosowany jako podstawa prawna przetwarzania danych osobowych w sytuacji, gdy realizowane uzasadnione interesy administratora są zgodne z interesami dziecka. W przypadku konfliktu między uzasadnionymi interesami administratora (w tym w zakresie przetwarzania danych osobowych w celach komercyjnych) a interesami lub podstawowymi prawami i wolnościami dziecka, interesy i podstawowe prawa i wolności dziecka powinny przeważać¹²⁶.

Nieprawidłową praktyką jest uzależnianie dopuszczania dziecka do zajęć sportowych organizowanych przez klub sportowy od wyrażenia zgody na wykorzystanie wizerunku dziecka w celach komercyjnych czy reklamowych klubu. Taka zgoda powinna być wyrażona w sposób dobrowolny. Oznacza to, że rodzic powinien mieć możliwość podjęcia tej decyzji bez żadnej presji czy ograniczeń i nie może być zmuszony do wyrażenia zgody jako warunku uczestnictwa dziecka w zajęciach. Tego typu działanie należy uznać za niezgodne zarówno z przepisami ustawy o prawie autorskim i prawach pokrewnych, jak również RODO¹²⁷. W obu przypadkach zgoda musi spełniać kryterium dobrowolności.

Więcej informacji: *Wizerunek dziecka w internecie. Publikować czy nie*¹²⁸.

¹²⁵ Motyw 38 RODO. Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich. Zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku.

¹²⁶ Wytyczne EROD nr 1/2024 dotyczące przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit f RODO, wersja 1.0 (konsultacje publiczne zamknięte 20 listopada 2024 r.).

¹²⁷ Art. 7 ust. 4 RODO. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy m.in. od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

¹²⁸ *Prawo do prywatności a wizerunki dzieci w internecie. Poradnik*, <https://uodo.gov.pl/pl/138/3215> [dostęp: 26.06.2025].

1.8. FORMA ZGODY

Zarówno zezwolenie na rozpowszechnianie wizerunku, jak i zgoda na przetwarzanie danych osobowych może być wyrażona w dowolnej formie. Ani przepisy ustawy o prawie autorskich i prawach pokrewnych, ani przepisy RODO nie narzucają obowiązku uzyskiwania zezwolenia/zgody w formie pisemnej. Zezwolenie/zgodę można pozyskać również w formie ustnej, jednak ze względów dowodowych oraz z uwagi na zasadę rozliczalności (patrz: *Zasada rozliczalności*) rekomenduje się, aby odbyło się to w jakiś udokumentowany sposób. Zgoda może być wyrażona w formie pisemnego oświadczenia, wiadomości SMS, e-mailowej, a nawet nagrania albo w formie elektronicznej, np. poprzez zaznaczenie odpowiedniego checkboxa na stronie internetowej.

UWAGA!

Zezwolenie na rozpowszechnianie wizerunku wyrażone zgodnie z art. 81 ustawy o prawie autorskim i prawach pokrewnych nie powinno stanowić tego samego oświadczenia co zgoda na przetwarzanie danych osobowych. Zgoda na przetwarzanie danych osobowych nie może również być wpisana w treść umowy czy regulaminu (w przeciwieństwie do zezwolenia na rozpowszechnianie wizerunku). Rekomenduje się oddzielenie oświadczenia o wyrażeniu zgody na przetwarzanie danych od zezwolenia na rozpowszechnianie wizerunku. Nie musi to jednak oznaczać konieczności tworzenia nowego dokumentu. Wystarczy, że zgoda zostanie wyodrębniona w sposób pozwalający wyraźnie odróżnić ją od innych treści.

1.9. CO NALEŻY ZROBIĆ I O CO ZADBAĆ, PRZETWARZAJĄC DANE OSOBOWE W POSTACI WIZERUNKU?

Przetwarzając dane osobowe w postaci wizerunku, należy:

- ▶ ustalić, czy wizerunek będzie rozpowszechniany czy wykorzystywany w inny sposób;
- ▶ jeżeli wizerunek będzie rozpowszechniany – ustalić, czy konieczne jest uzyskanie zezwolenia na rozpowszechnianie zgodnie z art. 81 ustawy o prawie autorskim i prawach pokrewnych;
- ▶ jeżeli okaże się to konieczne – odebrać oświadczenie o zezwoleniu na rozpowszechnianie wizerunku (powinno to nastąpić przed publikacją wizerunku);

- ▶ ustalić, jaka jest podstawa prawna przetwarzania danych osobowych w postaci wizerunku;
- ▶ jeżeli podstawą prawną przetwarzania danych osobowych jest zgoda – dodatkowo odebrać oświadczenie o jej wyrażeniu (powinno to nastąpić przed wykorzystaniem wizerunku);
- ▶ w przypadku osób niepełnoletnich – odebrać zezwolenie/zgodę wyrażone przez rodziców lub opiekunów prawnych;
- ▶ w przypadku osób niepełnoletnich – przeanalizować, czy publikacja wizerunku jest konieczna do realizacji określonego celu i czy nie można skorzystać z innych rozwiązań, jak np. publikacja zdjęcia, na którym nie będzie widać cech fizycznych dziecka pozwalających na jego identyfikację, zakrycie na zdjęciu twarzy dziecka za pomocą elementów graficznych, a jeżeli zdjęcia mają służyć pokazaniu rodzicom przebiegu treningu, warto rozważyć publikowanie ich w zamkniętej grupie rodziców (po uprzednim przeanalizowaniu ryzyk z tym związanych i zgodnie z przyjętą przez organizację sportową polityką ochrony danych osobowych);
- ▶ na etapie pozyskiwania danych w postaci wizerunku – spełnić obowiązek informacyjny zgodnie z art. 13 lub 14 RODO (patrz: **Obowiązek informacyjny**), dotyczy to również sytuacji, w której rozpowszechnianie wizerunku nie wymaga uzyskania zezwolenia zgodnie z art. 81 ustawy o prawie autorskim i prawach pokrewnych; klauzula informacyjna może zostać np. umieszczona w treści regulaminu imprezy sportowej lub w zawieranej ze sportowcem umowie;
- ▶ odpowiednio zabezpieczyć dane w postaci wizerunku (art. 24 oraz art. 32 i nast. RODO) zgodnie z przyjętą przez organizację sportową polityką ochrony danych osobowych, np. nie przechowywać ich w pamięci prywatnych telefonów instruktorów czy członków klubu;
- ▶ jeżeli wizerunek jest przetwarzany przez inne podmioty działające na zlecenie organizacji sportowej np. fotografa, grafika, agencję reklamową, administratora strony internetowej – pamiętać o zawarciu stosownych umów powierzenia przetwarzania danych osobowych (patrz: **Powierzenie przetwarzania danych osobowych**);
- ▶ jeżeli wizerunek jest przekazywany innym podmiotom w celu realizacji ich własnych celów, np. sponsorom, donatorom będącym osobnymi administratorami danych osobowych – ustalić podstawę prawną takiego udostępnienia (patrz: **Udostępnienie danych osobowych**);
- ▶ zapewnić osobom, których wizerunek jest przetwarzany, możliwość skorzystania z przysługujących im zgodnie z RODO praw; pamiętać, że zgoda na przetwarzanie danych osobowych może być w każdej chwili cofnięta, co może wiązać się z koniecznością usunięcia opublikowanych wcześniej zdjęć lub nagrań (patrz: **Prawa osób, których dane są przetwarzane**);

- ▶ szczegółowo zapoznać się z treścią polityk prywatności dostawców mediów społecznościowych (odbiorców danych osobowych), z których korzysta dana organizacja sportowa, w szczególności w kontekście ewentualnego transferu danych osobowych poza EOG (patrz: *Transfer danych poza Europejski Obszar Gospodarczy*), a także sposobów wykorzystywania publikowanych na profilu danych osobowych, np. korzystania przez dostawcę z funkcji rozpoznawania twarzy (usługa dostępna w przeszłości na Facebooku), wykorzystywania danych gromadzonych na profilu w celu szkolenia AI (propozycja META, z której ostatecznie się wycofano).

UWAGA!

Wszystkie powyższe działania powinny być podejmowane w zgodzie z przyjętymi przez podmiot sportowy wewnętrznymi regulacjami, w szczególności politykami dotyczącymi ochrony danych osobowych.

2. TRANSFER DANYCH POZA EUROPEJSKI OBSZAR GOSPODARCZY (EOG)

ART. 44–50 RODO. ROZDZIAŁ V. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

RODO nie zawiera definicji transferu danych osobowych („przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej”), co może przysporzyć trudności już na samym etapie identyfikacji tego, czy w danym przypadku w ogóle dochodzi do transferu danych. Kwestie dotyczące transferu danych zostały uregulowane w rozdziale V RODO. **Transfer danych to takie przetwarzanie danych, w którym uczestniczą podmioty sportowe lub inne podmioty, które prowadzą swoją działalność poza EOG, w tym, jeśli mają zdalny dostęp do naszych danych spoza terenu EOG** (kraje inne niż państwa członkowskie Unii Europejskiej, Islandia, Norwegia i Liechtenstein, np. Chiny, Japonia, Indie, Turcja, Rosja czy USA).

Transfer może mieć charakter cykliczny, jak również incydentalny. Podmiot wysyłający dane poza EOG lub zapewniający dostęp do danych znajdujących się na terenie EOG spoza EOG nazywany jest eksporterem danych, a podmiot, do którego dane są wysyłane, to importer danych.

W związku z wydaniem przez Trybunał Sprawiedliwości Unii Europejskiej wyroku w sprawie Schrems II¹²⁹ zostały ustalone nowe zasady transferu danych do państw trzecich. W konsekwencji Europejska Rada Ochrony Danych (EROD) wydała zalecenia dotyczące transferu danych¹³⁰.

¹²⁹ Wyrok Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z dnia 16 lipca 2020 r. w sprawie Data Protection Commissioner przeciwko Facebook Ireland Limited, Maximillian Schrems (C-311/18) (dalej: sprawa Schrems II).

¹³⁰ Zalecenia EROD nr 1/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, wersja 2.0 przyjęta 18 czerwca 2021 r.

Transfer danych osobowych poza EOG jest ściśle regulowany przez RODO, które określa warunki, na jakich takie transfery mogą się odbywać. Do transferu danych osobowych poza EOG może dochodzić m.in. w sytuacjach, w których organizacje sportowe przekazują dane osobowe zawodników czy trenerów do międzynarodowych organizacji sportowych lub w celu wzięcia udziału w międzynarodowych wydarzeniach sportowych (turniejach, zawodach, olimpiadzie) organizowanych w państwach spoza EOG. Udział w takich działaniach często wymaga przekazania danych osobowych do co najmniej kilku podmiotów działających poza obszarem EOG. Dane osobowe mogą być przekazywane zarówno do organizatorów wydarzeń, jak również np. hoteli, wypożyczalni samochodów, biur podróży czy lokalnych linii lotniczych.

Zgodnie z wytycznymi Europejskiej Rady Ochrony Danych¹³¹ warunki zakwalifikowania określonej operacji przetwarzania danych jako transferu zostały ujęte w trzech grupach. Mianowicie EROD określiła trzy kryteria łączne kwalifikowania operacji przetwarzania jako przekazywanie danych:

- ▶ administrator lub podmiot przetwarzający („podmiot przekazujący”) podlega RODO w odniesieniu do danego przetwarzania;
- ▶ podmiot przekazujący ujawnia poprzez przesłanie lub w inny sposób udostępnia innemu administratorowi, współadministratorowi lub podmiotowi przetwarzającemu („podmiot odbierający”) dane osobowe poddane temu przetwarzaniu;
- ▶ podmiot odbierający znajduje się w państwie trzecim, niezależnie od tego, czy podlega on RODO w odniesieniu do danego przetwarzania zgodnie z art. 3 RODO, lub jest organizacją międzynarodową.

Jeśli trzy powyższe kryteria określone przez EROD będą spełnione, to przekazywanie danych (transfer) ma miejsce i w takim przypadku rozdział V RODO ma zastosowanie. Oznacza to, że transfer danych będzie mógł nastąpić jedynie pod pewnymi warunkami, np. będzie obowiązywała decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony (art. 45 RODO) lub będą zapewnione odpowiednie zabezpieczenia (art. 46 RODO). Przepisy rozdziału V mają na celu zapewnienie nieprzerwanej ochrony danych osobowych po ich przekazaniu do państwa trzeciego lub organizacji międzynarodowej.

Z kolei, jeżeli te trzy kryteria nie będą spełnione, to przekazywanie danych nie będzie miało miejsca i rozdział V RODO nie będzie miał zastosowania. W tym kontekście należy jednak podkreślić, że administrator musi tak czy inaczej przestrzegać pozostałych przepisów RODO i pozostaje w pełni odpowiedzialny za swoje czynności przetwarzania, niezależnie od tego, gdzie są one realizowane¹³².

¹³¹ Wytyczne EROD nr 5/2021 w sprawie wzajemnych zależności między stosowaniem art. 3 a przepisami dotyczącymi międzynarodowego przekazywania danych zgodnie z rozdziałem V RODO.

¹³² *Ibidem*, s. 3.

UWAGA!

Transfer danych może odbywać się przy okazji korzystania przez organizację z różnych narzędzi informatycznych, np.:

- ▶ przy korzystaniu z chmury obliczeniowej (zdarza się, że serwery dostawcy usług chmury obliczeniowej, z której korzysta dany dostawca usługi lub bezpośrednio związek sportowy, znajdują się poza EOG lub w ramach świadczenia usług chmurowych możliwy jest zdalny dostęp do danych spoza EOG przez dostawcę usług, np. w ramach świadczenia usług serwisowych, usuwania błędów, usług wsparcia technicznego itp.);
- ▶ przy wykorzystaniu elektronicznych formularzy dostarczanych przez firmę Google (zgodnie z polityką prywatności Google może transferować lub transferuje dane do różnych państw, w tym do państwa spoza EOG) w ramach stosowanych narzędzi i rozwiązań, w tym tych, które wykorzystują sztuczną inteligencję;
- ▶ przy wykorzystaniu plików cookie lub wtyczek i skryptów śledzących od zewnętrznych dostawców na swoich stronach internetowych (np. Google Analytics, Meta Pixel, TikTok Ads Manager).

Korzystając z takich narzędzi, organizacja powinna zapoznać się szczegółowo z zasadami świadczenia usług, zawartymi w nich umowami powierzenia przetwarzania danych osobowych i odpowiednimi politykami prywatności podmiotów, u których je zamawia.

Zgodnie z RODO, mając na uwadze specyfikę działalności podmiotów sportowych, transfery danych osobowych do krajów spoza EOG mogą być przeprowadzane m.in. na następujących podstawach:

- ▶ **decyzja KE** stwierdzająca odpowiedni stopień ochrony (art. 45 RODO);
- ▶ istnieją odpowiednie zabezpieczenia i skuteczne środki ochrony praw osób, których dane osobowe, i skuteczne środki ochrony prawnej, w tym m.in. podpisane przez strony tzw. **standardowe klauzule ochrony danych osobowych przyjęte przez KE (tzw. standardowe klauzule umowne)** lub wiążące reguły korporacyjne;
- ▶ przetwarzanie w oparciu o jeden z **wyjątków wskazanych w art. 49 RODO**.

2.1. PRZEKAZANIE NA PODSTAWIE DECYZJI KE STWIERDZAJĄCEJ ODPOWIEDNI STOPIEŃ OCHRONY (ART. 45 RODO)

Jeśli Komisja Europejska w drodze decyzji stwierdzającej odpowiedni stopień ochrony wydanej na podstawie art. 45 RODO lub poprzednio obowiązującej dyrektywy 95/46 stwierdziła już, że dane państwo, region lub sektor, do którego dane są

przesyłane, oferuje odpowiedni stopień ochrony, to do momentu, aż decyzja taka przestanie obowiązywać, nie będzie trzeba podejmować żadnych dalszych działań poza monitorowaniem, czy taka decyzja stwierdzająca odpowiedni stopień ochrony pozostaje ważna.

Komisja Europejska wydała decyzje uznające odpowiedni stopień ochrony dla następujących państw: Andora, Argentyna, Guernsey, Izrael, Japonia, Jersey, Kanada (w odniesieniu do komercyjnych organizacji przetwarzających dane), Korea Południowa, Nowa Zelandia, Szwajcaria, Urugwaj, Wielka Brytania, Wyspy Man, Wyspy Owcze¹³³.

Ponadto Komisja Europejska wydała decyzję stwierdzającą adekwatność ochrony w stosunku do organizacji w USA, które zapewniają zgodność z tzw. Ramami ochrony danych UE–USA (*Data Privacy Framework*¹³⁴). Lista tych organizacji została opublikowana przez Departament Handlu USA. Oznacza to, że przekazywanie danych osobowych z EOG do organizacji w USA, które przystąpiły do programu Ramy ochrony danych UE–USA i znajdują się na tej liście, jest możliwe bez konieczności uzyskiwania dodatkowych zezwoleń czy zastosowania takich instrumentów prawnych jak standardowe klauzule umowne bądź wiążące reguły korporacyjne¹³⁵. Wówczas nie ma też konieczności przeprowadzania oceny ryzyka transferu (tzw. *transfer impact assessment* – TIA).

UWAGA!

W przypadku transferu danych do USA należy zweryfikować, czy organizacja, której dane osobowe są przekazywane, przystąpiła do programu Ramy ochrony danych UE–USA, uzyskując certyfikat i wpis na listę. W przypadku, w którym dana organizacja nie znajduje się na wyżej wymienionej liście, przekazywanie do niej danych osobowych jest możliwe po spełnieniu warunków określonych poniżej. Weryfikacji można dokonać przy użyciu wyszukiwarki dostępnej pod adresem: <https://www.dataprivacyframework.gov/list>.

¹³³ *Adequacy decisions*, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [dostęp: 26.06.2025].

¹³⁴ Decyzja wykonawcza Komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. na podstawie RODO, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA.

¹³⁵ UODO, *Decyzja KE o zapewnieniu odpowiedniego poziomu ochrony przez Ramy ochrony danych UE–USA*, <https://uodo.gov.pl/pl/138/2767> [dostęp: 26.06.2025].

2.2. STANDARDOWE KLAUZULE OCHRONY DANYCH OSOBOWYCH PRZYJĘTE PRZEZ KE

W razie braku decyzji, administrator może przekazać dane osobowe wyłącznie, gdy zapewni **odpowiednie zabezpieczenia** i pod warunkiem że obowiązują **egzekwowalne prawa** osób, których dane osobowe dotyczą i skuteczne **środki ochrony** w tym m.in. zostały podpisane przez strony tzw. **standardowe klauzule ochrony danych osobowych przyjęte przez KE** (standardowe klauzule umowne)¹³⁶ (art. 46 RODO) lub podmioty posiadają wiążące reguły korporacyjne zgodnie z art. 47 RODO (obowiązują najczęściej w zakresie przetwarzania danych osobowych przez spółki z danej grupy, które przyjęły je do stosowania).

Standardowe klauzule ochrony danych to umowy zawarte pomiędzy stronami na wzorcu zaakceptowanym przez Komisję Europejską. Treść standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich stanowi załącznik do decyzji KE i jest dostępna na stronie internetowej Komisji¹³⁷.

Należy pamiętać, że transfer danych osobowych może być dokonywany zarówno w modelu administrator danych do administratora danych, administrator danych do podmiotu przetwarzającego, podmiot przetwarzający do podmiotu przetwarzającego oraz podmiot przetwarzający do administratora (*patrz: Role w procesie przetwarzania danych osobowych*). W przypadku organizacji sportowych najczęściej spotykanym modelem będzie zapewne model administrator do administratora lub w przypadku korzystania z usług różnych dostawców (w tym przede wszystkim takich o zasięgu globalnym) może to być model administrator do podmiotu przetwarzającego.

Co istotne, oprócz zawarcia samych umów zalecane jest stosowanie dodatkowych środków uzupełniających¹³⁸, m.in.:

- ▶ należy dokonać oceny sytuacji prawnej podmiotu, któremu przekazywane są dane, w tym w szczególności w zakresie przepisów regulujących dostęp do danych osobowych przez organy publiczne. Czy państwo trzecie posiada kompleksowe publicznie dostępne przepisy o ochronie danych osobowych? Czy istnieje niezależny organ nadzorczy ds. ochrony danych? Czy dostępna jest ochrona prawna poszkodowanych obywateli UE w przypadku wspomnianego dostępu organów państwowych do

¹³⁶ Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32021D0914&from=EN> [dostęp: 26.06.2025].

¹³⁷ *Ibidem*.

¹³⁸ Zalecenia EROD nr 1/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, wersja 2.0 przyjęta 18 czerwca 2021 r.

danych obywateli UE? Czy państwo trzecie przystąpiło do międzynarodowych umów/porozumień o ochronie danych? Ocenę trzeba udokumentować (patrz: **Zasada rozliczalności**). Ponadto należy zapewnić, że wybrany mechanizm transferu danych zgodnie z art. 46 RODO nie jest podważany przez istniejące przepisy lub praktykę prawną w danym państwie trzecim, a dostawca może rzeczywiście osiągnąć uzgodniony w umowie poziom ochrony danych (istnieją państwa, w których takie uzgodnienia umowne nie są wiążące). Należy więc poza samą oceną sytuacji prawnej wziąć pod uwagę faktyczną praktykę w państwie trzecim. Najlepiej zapytać o doświadczenia w tym zakresie dostawcę, dowiedzieć się, czy należy on do grupy podmiotów objętych szczególnymi wymaganiami, np. ze względu na sektor, branżę lub rodzaj danych, które zamierzamy transferować znajduje się pod szczególnym nadzorem organów państwa trzeciego;

- ▶ należy określić i przyjąć dodatkowe środki techniczne wzmacniające ochronę, które utrudniają dostęp do danych przez władze państwa trzeciego, np. szyfrowanie, pseudonimizacja. Należy to zrobić najlepiej przy wsparciu dostawcy i w zależności od rezultatu przeprowadzonej analizy zaleca się uzgodnić z tym dostawcą dodatkowe środki ochronne (dotyczy to również dodatkowych środków ochronnych przy przesyłaniu i dostępie do danych osobowych). Przy tej ocenie istotne jest również stosowne udokumentowanie tego działania (np. w ramach TIA);
- ▶ należy określić dodatkowe proceduralne środki zabezpieczające np. w formie dodatkowych klauzul umownych, jeżeli okazałoby się, że z analizy prawodawstwa i praktyk panujących w państwie przyjmującym wynika, iż podstawa transferu danych (w tym wypadku klauzule umowne) nie zapewnia poziomu ochrony zasadniczo równoważnego temu, który obowiązuje na terenie UE;
- ▶ należy monitorować zmiany w przepisach państw trzecich i ponownie dokonywać oceny przekazywania danych (np. w zakresie ilości otrzymanych przez dostawcę wniosków o udzielenie informacji dotyczących transferowanych danych).

Przed dokonaniem transferu danych poza EOG, których administratorem jest związek sportowy, konieczne będzie wykonanie oceny ryzyka transferu w celu ustalenia, czy poziom ryzyka jest akceptowalny. W przypadku wykazania niedostatecznego poziomu bezpieczeństwa należy wprowadzić dodatkowe środki techniczne i organizacyjne, które zapewnią odpowiednią ochronę danych. Dane osobowe będą mogły być przetwarzane poza EOG wyłącznie wtedy, gdy poziom bezpieczeństwa będzie merytorycznie równoważny z tym, który jest zagwarantowany na terenie EOG. Ma to również zastosowanie, jeśli dane będą przechowywane na terenie EOG, ale dostęp do nich będzie możliwy z państwa trzeciego. Celem TIA jest ocena, czy podmiot, któremu przekazujemy dane, może zapewnić odpowiedni poziom ochrony danych osobowych w związku z przetwarzaniem danych poza EOG. Jeśli w ramach TIA wykażemy, że ryzyko zostało wystarczająco ograniczone lub wyeliminowane, to transfer danych poza EOG będzie zgodny z wymaganiami RODO.

2.3. PRZETWARZANIA W OPARCIU O JEDEN Z WYJĄTKÓW WSKAZANYCH W ART. 49 RODO

W sytuacji, gdy nie ma podpisanych standardowych klauzul umownych, transfer może odbywać się w przypadku sporadycznych i niepowtarzających się operacji przetwarzania w oparciu o jeden z **wyjątków wskazanych w art. 49 RODO**¹³⁹, w szczególności:

- ▶ **wyraźna zgoda osoby**, której dane dotyczą – osoba ta powinna zostać poinformowana o ewentualnym ryzyku, jakie wiąże z przekazaniem jej danych do państwa, które nie posiada odpowiednich zabezpieczeń;
- ▶ **niezbędność do wykonania umowy lub do wprowadzenia w życie środków przedumownych** – dotyczy wyłącznie umów zawartych pomiędzy administratorem a osobą, której dane są transferowane (np. zawodnikiem), przesłanka może być stosowana sporadycznie¹⁴⁰;
- ▶ **niezbędność do zawarcia lub wykonania umowy zawartej w interesie osoby**, której dane są transferowane (np. zawodnika), przy czym przekazanie następuje pomiędzy administratorem a inną osobą fizyczną lub prawną – w tym wypadku np. hotel, linie lotnicze, przesłanka może być stosowana sporadycznie i powinna być ograniczone do konkretnych sytuacji;
- ▶ **niezbędność do ochrony żywotnych interesów osoby, której dane dotyczą**, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażania zgody, np. w sytuacjach awaryjnych, związanych z ochroną zdrowia zawodnika podczas wydarzeń sportowych.

UWAGA!

Jeśli organizacja dokonuje transferu danych poza EOG, który nie spełnia wymogów określonych w RODO (i wyroku Schrems II oraz wytycznych EROD), to naraża się na ryzyko podjęcia kroków przez organ nadzorczy, który może zakazać dalszego przetwarzania danych osobowych lub nałożyć administracyjną karę pieniężną.

¹³⁹ Zalecenia EROD nr 1/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, wersja 2.0 przyjęta 18 czerwca 2021 r., s. 2–3.

¹⁴⁰ Motyw 111 RODO.

2.4. TRANSFER DANYCH A OBOWIĄZEK INFORMACYJNY

ART. 13 RODO. INFORMACJE PODAWANE W PRZYPADKU ZBIERANIA DANYCH OD OSOBY, KTÓREJ DANE DOTYCZĄ

„1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

[...]

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia”.

ART. 14 RODO. INFORMACJE PODAWANE W PRZYPADKU POZYSKIWANIA DANYCH OSOBOWYCH W SPOSÓB INNY NIŻ OD OSOBY, KTÓREJ DANE DOTYCZĄ

„1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:

[...]

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

Dokonywanie transferu danych osobowych poza EOG wymaga przekazania osobie, której dane osobowe są transferowane, określonej informacji dotyczącej takiego transferu. **Taka informacja stanowi część klauzuli informacyjnej (patrz: Obowiązek informacyjny) i powinna zawierać:**

- informację o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony (czyli czy została wydana decyzja, o której mowa w rozdz. 2.1) lub

- ▶ w przypadku przekazania, o którym mowa w rozdz. 2.2 (standardowe klauzule umowne lub wiążące reguły korporacyjne) i rozdz. 2.3 (wyjątki) powyżej – wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych dotyczących tych zabezpieczeń lub o miejscu udostępnienia tych danych¹⁴¹.

UWAGA!

Poinformowanie o transferze powinno nastąpić przed przekazaniem danych do państwa trzeciego.

2.5. TRANSFER DANYCH A INNE OBOWIĄZKI WYNIKAJĄCE Z RODO

ART. 30 RODO. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

„1. Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

[...]

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń; [...]

2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

[...]

c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń”.

¹⁴¹ Art. 13 ust. 1 lit f RODO.

ART. 28 RODO. PODMIOT PRZETWARZAJĄCY

„3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiązą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny”.

Informacja o transferze danych musi znaleźć się w rejestrze czynności przetwarzania oraz w rejestrze kategorii czynności przetwarzania (w zależności od pełnionej roli). Kwestie transferów danych należy także uregulować w zawieranych umowach powierzenia przetwarzania danych osobowych, a także uwzględnić w przeprowadzanej analizie ryzyka. Pytanie dotyczące faktu, czy w ramach naruszenia ochrony danych dochodzi do transgranicznego przetwarzania danych, znajduje się również w formularzu zgłoszenia naruszenia ochrony danych.

3. PRZETWARZANIE DANYCH OSOBOWYCH A STANDARDY OCHRONY MAŁOLETNICH

Przetwarzanie danych osobowych w ramach ochrony małoletnich jest kluczowym elementem zapewnienia bezpieczeństwa dzieci w organizacjach sportowych. Zastosowanie odpowiednich procedur zgodnych z przepisami prawa minimalizuje ryzyko naruszeń i zapewnia zgodność z RODO. Najważniejsze aspekty dotyczące przetwarzania danych osobowych w ramach ochrony małoletnich dotyczą dwóch zagadnień:

- ▶ przetwarzania danych osobowych w ramach realizacji obowiązku weryfikacji niekaralności personelu;
- ▶ przetwarzania danych osobowych w ramach wdrożonych przez organizację standardów ochrony małoletnich.

3.1. PRZETWARZANIE DANYCH OSOBOWYCH W RAMACH REALIZACJI OBOWIĄZKU WERYFIKACJI NIEKARALNOŚCI PERSONELU

ART. 21 USTAWY O PRZECIWDZIAŁANIU ZAGROŻENIOM PRZESTĘPCZOŚCIĄ NA TLE SEKSUALNYM I OCHRONIE MAŁOLETNICH. OBOWIĄZEK UZYSKANIA INFORMACJI Z REJESTRU PRZED ZATRUDNIENIEM; OBOWIĄZEK PRZEDŁOŻENIA INFORMACJI Z KRAJOWEGO REJESTRU KARNEGO LUB REJESTRU KARNEGO INNEGO PAŃSTWA¹⁴²

„1. Przed nawiązaniem z osobą stosunku pracy lub przed dopuszczeniem osoby do innej działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu

¹⁴² Ustawa z dnia 13 maja 2026 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (Dz.U. z 2024 r. poz. 1802 z późn. zm).

lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi na pracodawcy lub innym organizatorze takiej działalności oraz na osobie, z którą ma być nawiązany stosunek pracy lub która ma być dopuszczona do takiej działalności, ciążą obowiązki określone w ust. 2–8.

2. Pracodawca lub inny organizator uzyskuje informacje, czy dane osoby, o której mowa w ust. 1, są zamieszczone w Rejestrze z dostępem ograniczonym lub w Rejestrze osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze.

3. Osoba, o której mowa w ust. 1, przedkłada pracodawcy lub innemu organizatorowi informację z Krajowego Rejestru Karnego w zakresie przestępstw określonych w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz.U. z 2023 r. poz. 1939), lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego.

4. Osoba, o której mowa w ust. 1, posiadająca obywatelstwo innego państwa niż Rzeczpospolita Polska, ponadto przedkłada pracodawcy lub innemu organizatorowi informację z rejestru karnego państwa obywatelstwa uzyskiwaną do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi.

5. Osoba, o której mowa w ust. 1, składa pracodawcy lub innemu organizatorowi oświadczenie o państwie lub państwach, w których zamieszkiwała w ciągu ostatnich 20 lat, innych niż Rzeczpospolita Polska i państwo obywatelstwa, oraz jednocześnie przedkłada pracodawcy lub innemu organizatorowi informację z rejestrów karnych tych państw uzyskiwaną do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi.

6. Jeżeli prawo państwa, o którym mowa w ust. 4 lub 5, nie przewiduje wydawania informacji do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi, przedkłada się informację z rejestru karnego tego państwa.

7. W przypadku gdy prawo państwa, z którego ma być przedłożona informacja, o której mowa w ust. 4–6, nie przewiduje jej sporządzenia lub w danym państwie nie prowadzi się rejestru karnego, osoba, o której mowa w ust. 1, składa pracodawcy lub innemu organizatorowi oświadczenie o tym fakcie wraz z oświadczeniem, że nie była prawomocnie skazana w tym państwie za czyny zabronione odpowiadające przestępstwom określonym w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii oraz nie wydano wobec niej innego orzeczenia, w którym stwierdzono, iż dopuściła się takich czynów zabronionych, oraz że nie ma obowiązku wynikającego z orzeczenia sądu, innego uprawnionego organu lub ustawy stosowania się do zakazu zajmowania wszelkich lub określonych stanowisk, wykonywania wszelkich lub określonych zawodów albo

działalności, związanych z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi.

8. Oświadczenia, o których mowa w ust. 5 i 7, składane są pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia. Składający oświadczenie jest obowiązany do zawarcia w nim klauzuli następującej treści: »Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia«. Klauzula ta zastępuje pouczenie organu o odpowiedzialności karnej za złożenie fałszywego oświadczenia.

9. Informacje, o których mowa w ust. 2, pracodawca lub inny organizator utrwała w formie wydruku i załącza do akt osobowych pracownika albo dokumentacji dotyczącej osoby dopuszczonej do działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi. Informacje oraz oświadczenia, o których mowa w ust. 3–7, pracodawca lub inny organizator załącza do akt osobowych pracownika albo dokumentacji dotyczącej osoby dopuszczonej do takiej działalności.

10. Wykonanie obowiązków, o których mowa w ust. 1–8, nie jest wymagane przed dopuszczeniem do działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi, członka rodziny małoletniego lub osoby znanej osobiście rodzicowi małoletniego albo przedstawicielowi ustawowemu małoletniego, gdy jest ona wykonywana w stosunku do małoletniego dziecka, którego rodzic albo przedstawiciel ustawowy są dopuszczającymi do działalności.

11. Przez członka rodziny, o którym mowa w ust. 10, należy rozumieć osobę spokrewnioną albo osobę niespokrewnioną, pozostającą w faktycznym związku oraz wspólnie zamieszkującą i gospodarującą”.

Obowiązek weryfikacji personelu został uregulowany w art. 21 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich¹⁴³. Dotyczy on osób zatrudnianych lub angażowanych do działalności związanej z opieką nad dziećmi, ich edukacją, wychowaniem czy innymi aktywnościami, w tym m.in. uprawianiem sportu. Obowiązek weryfikacji

¹⁴³ Ustawa z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (Dz.U. z 2024 r. poz. 1802 z późn. zm.).

dotyczy nie tylko osób zatrudnianych w ramach stosunku pracy, ale także na podstawie jakiegokolwiek innej formy współpracy, np. umowy cywilnoprawnej, wolontariatu, stażu itp.

Proces weryfikacji obejmuje m.in.:

- ▶ sprawdzenie osoby w Rejestrze sprawców przestępstw na tle seksualnym (RSPTS);
- ▶ uzyskanie informacji o niekaralności z Krajowego Rejestru Karnego (KRK); w przypadku obcokrajowców dodatkowo pozyskanie informacji z rejestru karnego państwa obywatelstwa uzyskiwanej do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi;
- ▶ pozyskanie informacji o państwach zamieszkania w ciągu ostatnich 20 lat (dotyczy zarówno obywateli RP, jak i obcokrajowców);
- ▶ uzyskanie informacji wymaganych ustawą, potwierdzających brak karalności i ograniczeń związanych z pracą z dziećmi, pochodzących z rejestrów zagranicznych państw, w których w ostatnich 20 latach weryfikowana osoba zamieszkiwała, albo w przypadku braku tych rejestrów w danym państwie – uzyskanie stosownych oświadczeń od tych osób (dotyczy zarówno obywateli RP, jak i obcokrajowców).

Jak zatem wynika z powyższego opisu, zakres procesu weryfikacji może być różny w zależności od konkretnego stanu faktycznego.

PRZYKŁAD

Jeżeli organizacja zatrudnia obywatela polskiego, który w ostatnich 20 latach nie przebywał długoterminowo za granicą, proces weryfikacji sprowadzi się do sprawdzenia takiej osoby w RSPTS oraz pozyskania informacji z KRK. Sprawa będzie bardziej skomplikowana w przypadku obcokrajowca, który powinien zostać zweryfikowany w RSPTS, powinien przekazać informację z KRK, jak również z rejestru państwa obywatelstwa uzyskiwaną do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi. W sytuacji, w której taki obcokrajowiec dodatkowo w ciągu ostatnich 20 lat przebywał długoterminowo w innych państwach – powinien przedstawić informacje pochodzące z rejestrów zagranicznych tych państw.

W ramach procesu weryfikacji dane osobowe osoby weryfikowanej mogą być przetwarzane w różnym zakresie. Zaznaczyć również należy, że część przetwarzanych danych będzie pozyskiwana bezpośrednio od osoby, która jest weryfikowana (m.in. zaświadczenia z KRK, oświadczenie o państwach zamieszkania czy numer PESEL niezbędny do zweryfikowania w RSPTS), natomiast część danych zostanie pozyskana z właściwego rejestru – RSPTS.

UWAGA!

Weryfikacja powinna zostać dokonana przed nawiązaniem stosunku pracy lub przed dopuszczeniem danej osoby do działalności z dzieć. Nie powinno się jednak dokonywać tej weryfikacji wobec wszystkich kandydatów do zatrudnienia, ale tylko wobec osób, które zostały wybrane w procesie rekrutacji do zatrudnienia. Brak jest podstaw prawnych do dokonywania weryfikacji w trakcie zatrudnienia. Brak podstaw do weryfikacji osób zatrudnionych przed 15 lutego 2024 r., tj. przed datą wejścia w życie wskazanego wyżej przepisu.

W praktyce działalności organizacji sportowych ustalenie, czy dana osoba jest zaangażowana w wykonywanie czynności wskazanych w art. 21 ustawy, nastrocza sporo wątpliwości. Oczywistym jest, że weryfikacji powinni podlegać trenerzy, animatorzy czy wolontariusze prowadzący zajęcia sportowe dla dzieci. Wątpliwości natomiast mogą budzić sytuacje, w których styczność z dzieckiem ma charakter jednorazowy, sporadyczny, następuje w obecności innych opiekunów, np. rodziców, lub jest tylko pośrednio związana z działalnością prowadzoną przez organizację sportową. Wydaje się, że obowiązek weryfikowania powinien dotyczyć nie tylko personelu merytorycznego, realizującego cel działania podmiotu sportowego (m.in. trenerów). Zdaniem Fundacji Dajemy Dzieciom Siłę taka interpretacja jest zbyt wąska i nie gwarantuje należytej ochrony dzieci przed krzywdzeniem¹⁴⁴. Jednocześnie dokonywanie weryfikacji wszystkich pracowników i współpracowników danego klubu czy związku sportowego jest zbyt daleko idącym i nadmiarowym procesem, który może powodować naruszenie praw i wolności osoby podlegającej weryfikacji, w tym stanowić naruszenie przepisów o ochronie danych osobowych. Wydaje się, że najbardziej właściwe jest oparcie działań na interpretacji celowościowej przepisu art. 21 wyżej wymienionej ustawy. Celem wprowadzenia obowiązku weryfikacji personelu jest zapewnienie ochrony dzieci przed krzywdzeniem i zminimalizowanie ryzyka występowania tego zjawiska. W sytuacjach niepewnych wydaje się, że weryfikacji powinny podlegać osoby, których zakres i sposób zaangażowania w działania wobec dzieci wskazują na wysokie ryzyko wystąpienia takiego krzywdzenia. Pomocne w tym zakresie mogą okazać się wytyczne Fundacji Dajemy Dzieciom Siłę zawarte opublikowanym na jej stronie przewodniku po narzędziu do analizy ryzyka w procesie weryfikacji personelu¹⁴⁵.

¹⁴⁴ U. Kubicka-Kraszyńska (oprac.), *Bezpieczna placówka, bezpieczna organizacja. Przewodnik po narzędziu do analizy ryzyka w procesie weryfikacji personelu*, <https://standardy.fdds.pl/upload/upload2/bezpieczna-placowka-bezpieczna-organizacja-przewodnik-po-narzedziu-do-analizy-ryzyka-w-procesie-weryfikacji-personelu-pdf-1718947597-1-21.pdf> [dostęp: 10.08.2025].

¹⁴⁵ *Ibidem*.

UWAGA!

Dokonywanie weryfikacji niezgodnie z dyspozycją wynikającą z art. 21 ustawy, w tym m.in. dokonywanie weryfikacji osób, które takiej weryfikacji nie powinny być poddawane lub dokonywanie weryfikacji przez nieuprawniony do tego podmiot albo w szerszym zakresie, niż jest to wymagane przepisami prawa, stanowi naruszenie przepisów o ochronie danych osobowych, w szczególności zasady zgodności z prawem (patrz: **Zasada zgodności z prawem, rzetelności, przejrzystości**). Jednocześnie, kto bez uprawnienia uzyskuje z RSPTS z dostępem ograniczonym informacje o osobie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch (art. 24 ustawy).

Podstawą prawną przetwarzania danych osobowych w procesie weryfikacji personelu jest art. 6 ust. 1 lit c oraz art. 10 RODO w związku z art. 21 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich. Dane te, choć nie mają charakteru szczególnych kategorii danych, są dodatkowo chronione, ponieważ dotyczą wyroków skazujących i czynów zabronionych. Zgodnie z przepisami mogą być przetwarzane wyłącznie pod nadzorem władz publicznych lub jeśli zezwala na to prawo Unii lub państwa członkowskiego (patrz: **Definicja danych osobowych**).

Wprowadzenie obowiązku weryfikowania personelu wiąże się z obowiązkiem dokonania dodatkowych czynności związanych z przetwarzaniem danych osobowych w ramach tego procesu. Każda organizacja powinna:

- ▶ zweryfikować i zaktualizować środki techniczne i organizacyjne stosowane w organizacji w celu ochrony dodatkowych danych, w tym zweryfikować zakres wydanego upoważnienia do przetwarzania danych osobowych lub wyznaczyć osobę uprawnioną do dokonywania weryfikacji i nadać jej stosowne upoważnienie (patrz: **Upoważnienie do przetwarzania danych osobowych**);
- ▶ zaktualizować rejestr czynności przetwarzania danych osobowych – cele przetwarzania (konieczność weryfikacji niekaralności i sprawdzenia w RSPTS), podstawę prawną przetwarzania, okres przechowywania danych, kategorie przetwarzanych danych;
- ▶ zaktualizować klauzule informacyjne związane z gromadzeniem danych w celu zatrudnienia/podjęcia współpracy – cele przetwarzania (konieczność weryfikacji niekaralności i sprawdzenia w RSPTS), podstawę prawną przetwarzania, okres przechowywania danych, źródła pochodzenia danych.

Warto, żeby organizacja sportowa opracowała wewnętrzne zasady dokonywania weryfikacji personelu. Mogą one stanowić część przyjętych przez organizację standardów ochrony małoletnich. Zasady te powinny m.in. określać:

- ▶ reguły kwalifikowania personelu podlegającego weryfikacji (np. stosowanie analizy ryzyka w przypadkach niejednoznacznych);
- ▶ okres trwałości odbieranych zaświadczeń z KRK – maksymalny czas, przez jaki zaświadczenie z KRK jest honorowane, licząc od dnia jego wystawienia (w szczególności w sytuacjach zawierania kolejnych umów lub kilku umów z jedną osobą);
- ▶ okresy przechowywania gromadzonych dokumentów (zaświadczeń i oświadczeń) w przypadku osób niebędących pracownikami podmiotu sportowego (patrz: *Jak ustalić okres retencji danych osobowych*).

Przepisy ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich nie określają, jak długo mają być przechowywane dokumenty i informacje zgromadzone przez organizację w ramach prowadzenia procesu weryfikacji personelu. W związku z tym należy stosować przepisy prawa pracy (przepisy dotyczące przechowywania dokumentacji pracowniczej) oraz ogólne zasady wynikające z RODO. Rekomendowane jest przyjęcie przez organizację wewnętrznej procedury przechowywania wyżej wymienionej dokumentacji, uwzględniającej specyfikę jej działalności.

W przypadku pracowników informacje (wydruki, oświadczenia) z rejestrów będą przechowywane w części A akt osobowych. Okres przechowywania dokumentacji pracowniczej wynosi 10 lat, licząc od końca roku kalendarzowego, w którym ustał stosunek pracy.

W przypadku osób niebędących pracownikami (m.in. wolontariuszy, współpracowników) stosuje się zasadę adekwatności. Okres przechowywania dokumentacji powinien być powiązany z czasem realizacji współpracy, np. do zakończenia działań wymagających weryfikacji. Należy ewentualnie dokonać analizy, czy istnieje konieczność przechowywania danych w innych celach, np. w celu obrony przed potencjalnymi roszczeniami.

UWAGA!

Nie należy poddawać weryfikacji każdego pracownika zatrudnionego w organizacji.

Należy pozyskiwać tylko te dane, które zostały wskazane w ustawie.

Nie należy dokonywać weryfikacji w trakcie zatrudnienia.

Należy ustalić, jaki jest okres przechowywania danych osobowych zarówno dla pracowników, jak i innych osób (współpracowników, wolontariuszy, stażystów).

Należy zaktualizować klauzulę informacyjną.

Należy zaktualizować rejestr czynności przetwarzania (patrz: *Rejestrowanie czynności i kategorii czynności przetwarzania*).

Należy zweryfikować i zaktualizować upoważnienia do przetwarzania danych osobowych.

3.2. PRZETWARZANIE DANYCH OSOBOWYCH W RAMACH WDROŻONYCH PRZEZ ORGANIZACJĘ STANDARDÓW OCHRONY MAŁOLETNI

Zgodnie z art. 22c ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich¹⁴⁶ obowiązek przyjęcia standardów ochrony małoletnich mają m.in. placówki sportowe, do których uczęszczają albo w których przebywają lub mogą przebywać małoletni, jak również organizatorzy działalności sportowej¹⁴⁷.

Standardy ochrony małoletnich obejmują m.in.:

- ▶ zasady zapewniające bezpieczne relacje między małoletnim a personelem placówki lub organizatora, a w szczególności zachowania niedozwolone wobec małoletnich;
- ▶ procedury interwencji w sytuacji podejrzenia krzywdzenia małoletniego, zasady i procedury podejmowania interwencji w sytuacji podejrzenia krzywdzenia lub posiadania informacji o krzywdzeniu małoletniego;
- ▶ procedury i osoby odpowiedzialne za składanie zawiadomień o podejrzeniu popełnienia przestępstwa na szkodę małoletniego, zawiadamianie sądu opiekuńczego oraz w przypadku instytucji, które posiadają takie uprawnienia, osoby odpowiedzialne za wszczynanie procedury „Niebieskiej Karty”;
- ▶ osoby odpowiedzialne za przyjmowanie zgłoszeń o zdarzeniach zagrażających małoletniemu i udzielenie mu wsparcia;
- ▶ sposób dokumentowania i zasady przechowywania ujawnionych lub zgłoszonych incydentów albo zdarzeń zagrażających dobru małoletniego.

Jak wynika z powyższego, nie ulega wątpliwości, że w związku z wdrożeniem, a następnie realizacją wyżej wymienionych procedur i obowiązków, organizacje sportowe będą przetwarzały dane osobowe. Tym samym podobnie jak w przypadku weryfikacji personelu powstaje potrzeba zaimplementowania regulacji dotyczących przetwarzania danych osobowych do procesów prowadzonych w ramach realizacji standardów ochrony małoletnich. Każda organizacja sportowa, która wprowadziła standardy ochrony małoletnich, powinna zadbać o prawidłowe przetwarzanie danych osobowych osób będących uczestnikami realizowanych przez nią działań. Tym samym niezbędne jest przeanalizowanie obowiązujących w organizacji wewnętrznych regulacji dotyczących przetwarzania danych osobowych (patrz: *Co administrator powinien dokumentować?*) i ich dostosowanie do nowych przepisów

¹⁴⁶ Ustawa z dnia 13 maja 2026 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (Dz.U. z 2024 r. poz. 1802 z późn. zm.).

¹⁴⁷ Więcej o tym, jak wdrożyć standardy małoletnich w klubie sportowym, można przeczytać w: M. Hojnor, K. Katana, A. Krawczak, U. Kubicka-Kraszyńska, K. Poniatowska, J. Rosiak, J. Ruchała, A. Sotomska (oprac.), *Standardy ochrony dzieci w klubach sportowych*, <https://standardy.fdds.pl/standardy-w-dzialaniu/kluby> [dostęp: 26.05.2025].

prawa. Wprowadzając nowy proces przetwarzania danych osobowych w związku z wprowadzeniem standardów ochrony małoletnich, należy mieć na uwadze stosowanie zasady dotyczącej ochrony danych w fazie projektowania i domyślnej ochrony danych (patrz: *Ochrona danych w fazie projektowania i domyślna ochrona danych*). Ponieważ ustawa nie reguluje kluczowych kwestii dotyczących danych osobowych, jej stosowanie w zakresie tej tematyki może nastroczać sporo wątpliwości, a tym samym wymaga szczególnej uwagi, zwłaszcza jeśli chodzi o¹⁴⁸:

- ▶ podstawę prawną przetwarzania danych osobowych;
- ▶ zakres przetwarzanych danych osobowych;
- ▶ okres przechowywania danych osobowych;
- ▶ obowiązek informacyjny;
- ▶ poufność i integralność danych osobowych.

3.2.1. PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

W ramach standardów ochrony małoletnich mogą być przetwarzane zarówno dane osobowe zwykłe, jak i szczególne kategorie danych osobowych (m.in. dane osobowe dotyczące stanu zdrowia czy seksualności). Organizacja sportowa może przetwarzać dane dzieci, jak i osób trzecich (m.in. sprawców, świadków, osób dokonujących zgłoszenia).

Przetwarzanie danych w ramach procesów realizowanych w związku z wdrożeniem standardów ochrony małoletnich wymaga precyzyjnego doboru podstaw prawnych (patrz: *Podstawy prawne przetwarzania danych osobowych*). W przypadku danych zwykłych wydaje się, że powinien mieć zastosowanie art. 6 ust. 1 lit. c RODO (obowiązek prawny). W niektórych sytuacjach możliwy do rozważania będzie również art. 6 ust. 1 lit. d RODO (ochrona żywotnych interesów osoby, której dane dotyczą). W przypadku szczególnych kategorii danych osobowych zastosowanie powinien znaleźć art. 9 RODO. Przesłanką przetwarzania danych osobowych w tym wypadku nie będzie zgoda, chodzi zatem o regulację, która miałaby oparcie w przepisie prawa (m.in. art. 9 ust. 1 lit. g RODO, ewentualnie w niektórych sytuacjach również art. 9 ust. 1 lit. c RODO). I tutaj pojawia się problem, jak bowiem zauważył PUODO, w ustawie brak jest podstawy prawnej dla przetwarzania danych osobowych w ramach standardów ochrony małoletnich. PUODO wskazuje, że ustawa odsyła do wytycznych niemających charakteru norm prawnych, które nie

¹⁴⁸ Opracowano na podstawie informacji opublikowanej na stronie UODO: *Jak stosować „ustawę Kamilka” w zgodzie ze standardami ochrony danych osobowych*, <https://uodo.gov.pl/pl/138/3278> [dostęp: 26.06.2025].

mogą kształtować przetwarzania danych osobowych¹⁴⁹. Tym samym PUODO zwraca uwagę na konieczność dostosowania przepisów ustawy o ochronie małoletnich do zasad ochrony danych osobowych wynikających z RODO, szczególnie w kontekście przetwarzania danych szczególnych kategorii i danych dotyczących wyroków skazujących.

3.2.2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

Ponieważ ustawa nie wskazuje na zakres przetwarzanych danych osobowych, każda organizacja, kierując się zasadą minimalizacji danych osobowych, powinna samodzielnie ocenić, które dane są adekwatne i niezbędne do realizowanego przez nią celu. Należy ograniczyć zakres pozyskiwanych danych do minimum niezbędnego do realizacji obowiązków nałożonych przepisami prawa (*patrz: Zasada minimalizacji danych*).

3.2.3. OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

Ze względu na brak w ustawie przepisów określających okresy przechowywania danych osobowych, w tym dokumentacji związanej z prowadzonymi interwencjami oraz innymi informacjami pozyskanymi przez administratora, konieczne jest samodzielne ustalenie przez niego zasad retencji. Obejmuje to określenie, jak długo będą przechowywane poszczególne dane oraz dokumentacja związana z realizowanymi procesami, zgodnie z zasadą ograniczonego przechowywania (*patrz: Zasada ograniczenia przechowywania*).

3.2.4. OBOWIĄZEK INFORMACYJNY

Każdy administrator powinien pamiętać o obowiązku informacyjnym względem wszystkich osób, których dane zostaną pozyskane (dzieci, rodziców, świadków, osób dokonujących zgłoszenia). Klauzule informacyjne należy zweryfikować w szczególności pod względem podstawy prawnej przetwarzania danych osobowych, informacji o odbiorcach lub kategoriach odbiorców danych, retencji danych, źródła pochodzenia danych. Spełniając obowiązek informacyjny wobec dzieci, należy

¹⁴⁹ UODO, *Ustawa Kamilka wymaga korekt. Wystąpienie PUODO do Ministra Sprawiedliwości*. <https://uodo.gov.pl/pl/138/3377> [dostęp: 26.06.2025].

zadbać o to, żeby treść tego obowiązku była dla nich zrozumiała i czytelna (patrz: *Obowiązek informacyjny*). Dobrym pomysłem jest załączenie klauzul informacyjnych do dokumentacji wdrażającej standardy ochrony małoletnich, w tym m.in. do przyjętej przez organizację polityki ochrony małoletnich, która bardzo często udostępniana jest wszystkim potencjalnym zainteresowanym (w tym publikowana na stronach internetowych danej organizacji).

Problematiczne może okazać się spełnienie obowiązku informacyjnego wobec sprawcy lub potencjalnego sprawcy krzywdzenia dziecka. Aktualna treść ustawy nie przewiduje wyłączeń w zakresie spełnienia obowiązku informacyjnego (patrz: *Wyłączenia spełniania obowiązku informacyjnego*), co oznacza, że obowiązek informacyjny wobec wskazanych wyżej osób powinien być również spełniony.

3.2.5. POUFNOŚĆ I INTEGRALNOŚĆ DANYCH OSOBOWYCH

W procesach interwencyjnych w ramach standardów ochrony małoletnich poufność i integralność danych są kluczowe dla ochrony praw i bezpieczeństwa małoletnich. Ponieważ w ustawie brak wskazania środków zapewniających bezpieczeństwo przetwarzanych danych, jak również brak uregulowania zasad dostępu do danych osobowych i związanych z tym zabezpieczeń mających zapewnić poufność danych, realizacja poufności i integralności danych osobowych wymaga m.in.:

- ▶ **przeprowadzenia analizy ryzyka zgodnie z wymogami RODO** – w ramach tego procesu należy ocenić, jakie potencjalne zagrożenia mogą dotyczyć danych, jakie jest prawdopodobieństwo ich wystąpienia oraz jakie negatywne skutki mogą wynikać zarówno dla osób, których dane dotyczą (w szczególności dzieci), jak również organizacji sportowej (patrz: *Analiza ryzyka*). Na podstawie takich ustaleń można zaplanować i wdrożyć odpowiednie środki bezpieczeństwa, zarówno techniczne, jak i organizacyjne. Niezbędne jest wdrożenie środków minimalizujących ryzyko, np.: szyfrowanie danych, pseudonimizacja, korzystanie z silnych haseł, ograniczenie dostępu poszczególnych osób, stosowanie bezpiecznych kanałów komunikacji, zapewnienie dzieciom możliwości odbywania rozmów z zachowaniem poufności, ograniczenie działań do dokumentów, które są niezbędne, oraz monitorowanie systemów (patrz: *Bezpieczeństwo danych osobowych*);
- ▶ **wskazania osób**, które będą działały na podstawie upoważnienia administratora, będą posiadały dostęp do danych osobowych oraz realizowały zadania wynikające z nowych przepisów dotyczących standardów ochrony małoletnich – powinno się określić zakres uprawnień takich osób oraz zobowiązać je do zachowania poufności w odniesieniu do przetwarzanych danych. Aktualność uprawnień powinna być weryfikowana na bieżąco;

- ▶ **prowadzenia szkoleń** – osoby zaangażowane w przetwarzanie danych w procesach w ramach standardów ochrony małoletnich (w tym w szczególności procesach interwencyjnych) powinny być regularnie szkolone w zakresie ochrony danych osobowych, ze szczególnym uwzględnieniem poufności i integralności. Upoważnione do przetwarzania danych osoby muszą być świadome ustalonych procedur oraz w pełni je rozumieć. W tym celu należy wdrożyć stosowne procedury, a następnie przeprowadzić odpowiednie szkolenia dotyczące procesów przetwarzania danych osobowych. Szczególny nacisk powinien zostać położony na zwiększenie świadomości w zakresie przetwarzania danych należących do szczególnych kategorii danych osobowych;
- ▶ **dopełnienia innych obowiązków** – procesy związane ze standardami ochrony małoletnich, szczególnie interwencyjne, mogą być powtarzalne i dotyczą informacji wrażliwych, a tym samym szczególnych kategorii danych osobowych. Przetwarzanie danych w tych procesach wiąże się z podwyższonym ryzykiem dla praw i wolności małoletnich oraz osób zgłaszających zdarzenia. Tym samym niezbędne jest rejestrowanie czynności przetwarzania danych osobowych dokonywanych w ramach tych procesów.

4. PRZETWARZANIE DANYCH OSOBOWYCH W CELACH MARKETINGU

ART. 4 PKT 11 RODO

„ [...] »zgoda« osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych”.

ART. 7 RODO. WARUNKI WYRAŻENIA ZGODY

„1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy m.in. od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy”.

4.1. KLUCZOWE POJĘCIA W ZAKRESIE MARKETINGU

Prowadzenie działań marketingowych może być bardzo istotnym elementem bieżących aktywności każdej organizacji sportowej. Dzięki nim związek czy klub może zwiększać świadomość odbiorców na temat swojej działalności oraz kreować swój wizerunek wśród ogółu społeczności. W związku z bardzo szybkim rozwojem narzędzi cyfrowych oraz ogólnie wzrastającą świadomością na temat przysługujących praw związanych z ochroną prywatności konieczna jest znajomość wymagań prawnych w zakresie prowadzenia marketingu bezpośredniego oraz przesyłania informacji handlowej. Spełnienie przez organizację sportową niezbędnych w tym zakresie wymagań pozwoli uniknąć negatywnych konsekwencji prawnych i wizerunkowych.

Pojęcie marketingu bezpośredniego nie zostało wprost zdefiniowane w przepisach RODO ani w przepisach krajowych rangi ustawowej, regulujących kwestie dopuszczalności kierowania treści marketingowych do odbiorców tego typu komunikatów. W słowniku języka polskiego marketing zdefiniowany został jako działania mające na celu poznanie potrzeb konsumentów, ustalenie wielkości produkcji oraz metod dystrybucji, sprzedaży i reklamy towarów¹⁵⁰. W konsekwencji, aby prowadzić działania marketingowe zgodnie z obowiązującymi regulacjami, należy uwzględnić wymagania dotyczące zgody na przetwarzanie danych osobowych określone wprost w RODO oraz przepisy wynikające z ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (dalej: PKE).

Istotą marketingu bezpośredniego jest dostarczanie informacji o możliwości nabywania towarów lub usług oraz składanie obecnym lub potencjalnym klientom albo osobom/podmiotom współpracującym ze związkiem propozycji współpracy / nabywania usług / zawarcia umowy. Pojęcie marketingu bezpośredniego występuje wielokrotnie w motywach i przepisach dyrektywy 2002/58/WE¹⁵¹. Obejmuje ono wszelkie formy reklamy i promocji, w ramach których materiały o takiej zawartości kierowane są bezpośrednio do zidentyfikowanego podmiotu lub podmiotów przy użyciu usług łączności elektronicznej (telefon, SMS, e-mail etc.). Poza oferowaniem produktów i usług w celach komercyjnych pojęcie to obejmować może również promowanie celów pozagospodarczych, czyli np. działalności organizacji sportowej¹⁵².

¹⁵⁰ *Marketing*, [w:] *Słownik języka polskiego PWN*, <https://sjp.pwn.pl/slowniki/marketing.html> [dostęp: 10.07.2025].

¹⁵¹ Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).

¹⁵² S. Piątek, *Prawo komunikacji elektronicznej. Komentarz*, wyd. 1, Warszawa 2025.

4.2. CO WARTO WZIĄĆ POD UWAGĘ?

ART. 398 PRAWA KOMUNIKACJI ELEKTRONICZNEJ. OCHRONA PRZED MARKETINGIEM BEZPOŚREDNIM ORAZ PRZESYŁANIEM NIEZAMÓWIONYCH INFORMACJI HANDLOWYCH¹⁵³

„1. Zakazane jest używanie:

- 1) automatycznych systemów wywołujących,
- 2) telekomunikacyjnych urządzeń końcowych, w szczególności w ramach korzystania z usług komunikacji interpersonalnej

– do celów przesyłania informacji handlowej w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344 oraz z 2024 r. poz. 1222), w tym marketingu bezpośredniego, do abonenta lub użytkownika końcowego, chyba że uprzednio wyraził on na to zgodę.

2. Zgoda, o której mowa w ust. 1, może być wyrażona przez udostępnienie przez abonenta lub użytkownika końcowego identyfikującego go adresu elektronicznego w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, w celu przesyłania informacji handlowej na podany przez abonenta lub użytkownika końcowego adres elektroniczny.

3. Używanie środków, o których mowa w ust. 1, do przesyłania informacji handlowej, w tym marketingu bezpośredniego, nie może odbywać się na koszt użytkownika końcowego lub abonenta.

4. Działanie, o którym mowa w ust. 1, stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz. 1233)”.¹⁵⁴

ART. 400 PRAWA KOMUNIKACJI ELEKTRONICZNEJ. ODESŁANIE DO PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH¹⁵⁴

„Do uzyskania zgody abonenta lub użytkownika końcowego stosuje się odpowiednio przepisy o ochronie danych osobowych”.

Aby zatem spełnić wymagania regulacyjne i zastosować prawidłowo przepisy, należy w działaniach marketingowych prowadzonych przez organizację sportową uwzględnić przede wszystkim wymagania dotyczące:

¹⁵³ Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz.U. z 2024 r. poz. 1221 z późn. zm).

¹⁵⁴ *Ibidem*.

- ▶ w szczególności (poza innymi związanymi z przetwarzaniem danych osobowych) wyrażenia zgody na przetwarzanie danych osobowych określone w RODO;
- ▶ zgody do celów przesyłania informacji handlowej w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, w tym marketingu bezpośredniego do abonenta lub użytkownika końcowego, określone w ustawie Prawo komunikacji elektronicznej.

Organizacja sportowa musi uwzględnić tego typu zgody, bowiem prowadzenie działań marketingowych zawsze będzie wiązało się z przetwarzaniem danych osobowych w postaci np. numeru telefonu lub adresu e-mail. Poza tym zgodnie z artykułem 400 PKE do uzyskania zgody abonenta lub użytkownika końcowego stosuje się odpowiednio przepisy o ochronie danych osobowych (RODO). Konkludując, ustawodawca uznaje marketing jako hipotetycznie ryzykowny proces biznesowy, który wiąże się z dużą ingerencją w sferę prywatności, stąd prowadzenie tych działań (realizacja procesów) wymaga szczególnej troski o zapewnienie zgodności i przejrzystości.

UWAGA!

Ogólnie rzecz ujmując, przy zbieraniu zgód marketingowych organizacja sportowa jako administrator danych osobowych zawsze musi zagwarantować, że:

- ▶ uzyskała ważną zgodę na wysyłanie treści marketingowych;
- ▶ spełniła obowiązek informacyjny wobec osób fizycznych;
- ▶ odpowiednio udokumentowała zebranie zgody (kiedy została wyrażona, przez kogo, o jakiej treści).

4.3. POJĘCIE ZGODY

Wymagania dotyczące zgody zostały już szczegółowo opisane w rozdziale dotyczącym podstaw prawnych przetwarzania danych (patrz: *Podstawy prawne przetwarzania danych osobowych*). Przypominamy zatem dla porządku, że zgoda jest jedną z sześciu zgodnych z prawem podstaw przetwarzania danych osobowych wymienionych w art. 6 RODO. Zgodnie z art. 4(11) zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Co do zasady zgoda może być właściwą, zgodną z prawem podstawą wyłącznie wówczas, gdy osobie, której dane dotyczą, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia zaoferowanych warunków albo odrzucenia ich bez niekorzystnych konsekwencji. Zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody. Zgoda uzyskana w pełnej zgodności z RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy dotyczące ich dane osobowe będą przetwarzane. W braku zgodności zgody z RODO kontrola ze strony osoby, której dane dotyczą, staje się złudna, a zgoda będzie nieważną podstawą przetwarzania, co spowoduje niezgodność z prawem czynności przetwarzania¹⁵⁵.

Należy również pamiętać o warunkach wyrażenia zgody określonych w art. 7 RODO. Zgoda nie może być wymuszana.

PRZYKŁAD

Aplikacja mobilna do edycji zdjęć prosi użytkowników o włączenie lokalizacji GPS dla korzystania z jej usług. Aplikacja informuje również użytkowników, że wykorzysta zebrane dane do reklamy behawioralnej. Ani geolokalizacja, ani internetowa reklama behawioralna nie są konieczne do korzystania z usługi edycji zdjęć i niewątpliwie są to usługi wykraczające poza świadczenie podstawowe. Ponieważ użytkownicy nie mogą korzystać z aplikacji bez wyrażenia zgody na te cele, zgody nie można uznać za dobrowolną¹⁵⁶.

W ramach działań marketingowych, które organizacja sportowa zamierza prowadzić we własnym imieniu i na własną rzecz, będzie ona występowała w roli administratora danych osobowych. Sytuacja i rola organizacji sportowej może być inna, jeśli będzie zlecała te działania innym podmiotom lub sama będzie realizowała je dla innych podmiotów – wówczas należy ustalić rolę poszczególnych podmiotów w procesie przetwarzania danych osobowych i dostosować wymagania wynikające z RODO w tym zakresie do konkretnego stanu faktycznego (patrz: *Rola w procesie przetwarzania danych osobowych*).

UWAGA!

Dokumentuj zgodę i umożliwaj jej wycofanie.

¹⁵⁵ Wytyczne EROD nr 5/2020 dotyczące zgody na mocy rozporządzenia 2016/679, s. 5.

¹⁵⁶ *Ibidem*, s. 8.

4.4. FORMY MARKETINGU BEZPOŚREDNIEGO

W praktyce prowadzenia działań marketingowych wykorzystuje się działania polegające na:

- ▶ wykonywaniu połączeń telefonicznych;
- ▶ wysyłaniu wiadomości SMS, MMS;
- ▶ używaniu komunikatorów internetowych;
- ▶ wysyłaniu wiadomości e-mail (w tym newsletterów).

Najczęściej występującą formą marketingu bezpośredniego jest telemarketing za pomocą połączeń telefonicznych. Oznacza on w praktyce kontakt telefoniczny na wskazany numer telefonu. Nawiązanie takiego kontaktu w celu przedstawienia komunikatów marketingowych wymaga uzyskania uprzedniej zgody od odbiorcy takich połączeń. Zgodnie z art. 398 ust. 1 PKE organizacja sportowa musi uzyskać zgodę niezależnie od tego, czy będzie wykonywała połączenia przy użyciu telefonii stacjonarnej, komórkowej, rozmów wideo lub innych podobnych form nawiązywania kontaktu z osobą, do której będzie kierowany komunikat marketingowy. Istotny jest fakt, że taka zgoda musi być uzyskana uprzednio, to znaczy przed nawiązaniem połączenia w celach marketingowych.

Należy podkreślić, że wskazany przepis PKE nakłada obowiązek uzyskania zgody zarówno od osoby fizycznej, jak i prawnej. Wynika to z faktu, że mowa w tym przepisie o abonencie oraz użytkowniku końcowym (patrz definicje poniżej).

- ▶ **Abonent** – użytkownik, który jest stroną umowy o świadczenie usług komunikacji elektronicznej.
- ▶ **Użytkownik końcowy** – osoba korzystająca z publicznie dostępnych usług komunikacji elektronicznej lub żądająca świadczenia takich usług dla zaspokojenia własnych potrzeb.
- ▶ **Informacja handlowa** – każda informacja przeznaczona bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niesłużącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi.

Rekomenduje się umożliwienie osobie, do której ma być kierowany marketing, wyboru kanału przyszłej komunikacji marketingowej, czyli w praktyce uzyskiwanie osobnej zgody na każdy kanał komunikacji (tzw. granularność zgody). Zapewni to przejrzystość oraz konkretność zgody, a także uczyni zadość oczekiwaniom ze

strony podmiotów danych, umożliwiając im dokonanie wyboru kanału, którym będą odbierali adresowaną do nich komunikację marketingową. Przy czym podkreślić należy, że kontakt przy pomocy połączeń telefonicznych jest bardzo mocno wpływającą na prywatność abonenta lub użytkownika końcowego formą komunikacji, a zatem konieczne jest uzyskanie wyraźnej, osobnej zgody na ten kanał komunikacji marketingowej.

Inną formą prowadzenia marketingu jest wysyłanie wiadomości drogą elektroniczną za pośrednictwem poczty elektronicznej, SMS, MMS, czatów w komunikatorach. Takie działania niewątpliwie wiążą się z przetwarzaniem danych osobowych osób, których one dotyczą (np. numeru telefonu, adresu e-mail lub nazwy użytkownika korzystającego z komunikatora). Wysyłanie treści marketingowych z wykorzystaniem tych kanałów komunikacji także wymaga uzyskania uprzedniej zgody. Zastosowanie w tym przypadku będą miały również przepisy art. 398 PKE oczywiście w związku z przepisami RODO.

PRZYKŁAD ZGODY MARKETINGOWEJ

☐ Zgadzam się na przetwarzanie moich danych osobowych w zakresie adresu e-mail i/lub numeru telefonu przez [nazwa związku sportowego] w celu przesyłania mi informacji marketingowych dotyczących działalności, usług, wydarzeń związanych z [nazwa związku sportowego].

Zgoda dotyczy przesyłania informacji za pośrednictwem:

- wiadomości e-mail na adres (np. newslettery)
- wiadomości SMS/MMS na numer telefonu
- połączeń telefonicznych na numer telefonu

Mam świadomość, że powyższa zgoda jest dobrowolna i mogę wycofać ją w każdej chwili, co nie będzie miało wpływu na zgodność z prawem przetwarzania, które odbyło się przed jej wycofaniem.

Wycofanie zgody jest możliwe poprzez kliknięcie przycisku „rezygnuję” w wiadomości mailowej, wysłanie SMS o treści „NIE” na numer [numer związku] lub kontakt z [nazwa związku sportowego] pod adresem mailowym [adres mailowy związku].

Klauzula informacyjna opisująca zasady przetwarzania danych osobowych w związku z marketingiem bezpośrednim [link do klauzuli informacyjnej].

Przy treści należy dodać checkbox, który użytkownik musi samodzielnie zaznaczyć, jeśli zgoda będzie zbierana elektronicznie, a w przypadku zbierania zgody na formularzu papierowym, wymagany jest podpis osoby, której zgoda dotyczy (lub osoby uprawnionej).

4.5. OBOWIĄZKI INFORMACYJNE W MARKETINGU BEZPOŚREDNIM

ART. 5, 6, 12, 13, 14, 17, 22 RODO

Uzyskanie zgody nie zwalnia administratora z obowiązków przestrzegania zasad przetwarzania zawartych w RODO, w szczególności w art. 5 RODO, w odniesieniu do rzetelności, konieczności i proporcjonalności oraz jakości danych, ani w żaden sposób nie zmniejsza zakresu tych obowiązków. Nawet jeśli osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie jej danych osobowych, nie czyni to legalnym gromadzenia danych, które nie są konieczne w związku z określonym celem przetwarzania. Tak zatem w ramach czynności marketingu bezpośredniego każda osoba, której dane dotyczą, przed wyrażeniem zgody powinna zostać poinformowana o:

- ▶ tożsamości administratora danych;
- ▶ celu przetwarzania danych;
- ▶ zakresie przetwarzanych danych;
- ▶ prawie do wycofania zgody;
- ▶ informacji o wykorzystywaniu danych do zautomatyzowanego podejmowania decyzji zgodnie z art. 22 RODO;
- ▶ jeśli zgoda dotyczy przekazywania danych do państw trzecich – o możliwych zagrożeniach związanych z przekazywaniem danych do państw trzecich (w przypadku braku decyzji stwierdzającej stopień ochrony oraz odpowiednich zabezpieczeń zgodnie z art. 49 ust. 1 lit. a RODO).

Podobnie jak w innych procesach także i w tym przypadku organizacja sportowa musi zadbać o to, aby przetwarzanie danych osobowych było przejrzyste. Treść klauzuli informacyjnej dotyczącej przetwarzania danych osobowych w celu marketingu powinna być przede wszystkim czytelna. Transparentność zagwarantuje, że osoba, której dane dotyczą, będzie miała pełną kontrolę nad kierowanymi do niej komunikatami, będą one dla niej zrozumiałe, a także będzie miała możliwość łatwego skorzystania z przysługujących jej praw, w szczególności z prawa do wycofania zgody (patrz: *Obowiązek informacyjny*).

4.6. MOŻLIWOŚĆ WYCOFANIA ZGODY

Organizacja sportowa musi umożliwić wycofanie zgody na otrzymywanie komunikatów marketingowych w dowolnym momencie i w łatwy sposób. Dodatkowo wycofanie zgody powinno być skuteczne niezwłocznie, czyli organizacja sportowa

po otrzymaniu wniosku o wycofaniu zgody od osoby, której dane dotyczą, musi niezwłocznie zaprzestać dalszego wysyłania komunikatów marketingowych oraz przetwarzania danych osobowych w tym celu.

Przykładowym mechanizmem umożliwiającym cofnięcie zgody będzie dodanie linku np. w wiadomości mailowej, którego kliknięcie spowoduje wycofanie zgody (np. można dodać na końcu dopisek: „jeśli nie chcesz otrzymywać od nas wiadomości – wystarczy, że klikniesz poniżej w link rezygnacja lub wypisz się”), albo wprowadzenie możliwości dokonania zmian w ustawieniach konta aplikacji przez użytkownika, albo wysłanie SMS o odpowiedniej treści, który będzie dezaktywował zgodę na komunikację marketingową.

Związek nie może więc utrudniać cofnięcia zgody. Zgodnie z ogólnie przyjętą zasadą wycofanie zgody musi być równie łatwe jak jej wyrażenie. Jeżeli ktoś wyraża zgodę np. poprzez kliknięcie checkboxa, jej wycofanie nie powinno odbywać się poprzez kontakt użytkownika z infolinią.

UWAGA!

Wycofanie zgody nie powinno być utrudniane np. poprzez wprowadzenie obowiązku podania przyczyny decyzji lub odsyłanie do trudno dostępnego formularza.

Przetwarzanie danych osobowych już po cofnięciu zgody jest dopuszczalne tylko wówczas, gdy istnieje inna podstawa prawna legalizująca dalsze przetwarzanie danych osobowych. Może to być np. realizacja obowiązków prawnych zgodnie z art. 6 ust. 1 RODO.

5. NEWSLETTER

Organizacja sportowa może chcieć promować swoją działalność poprzez wysyłkę newsletterów z aktualnymi informacjami promującymi jej aktywność. W tym celu osoba zapisująca się do takiego newslettera może wyrazić odrębną zgodę na przetwarzanie jego danych osobowych w celu otrzymywania informacji marketingowych za pośrednictwem tego newslettera. Organizacja sportowa przy zbieraniu zgód na wysyłkę newslettera, analogicznie jak przy zbieraniu innych zgód marketingowych, jest zobowiązana zapewnić, aby taka zgoda była ważna. Musi więc być sformułowana jasnym, prostym, zrozumiałym językiem i wyrażona przez podmiot danych zawsze przed rozpoczęciem procesu przetwarzania danych osobowych (uprzednia zgoda). Oczywiście będzie ona ważna do czasu jej wycofania i – co szczególnie istotne – zgoda wymaga wyraźnego oświadczenia bądź wyraźnego działania podmiotu danych (wyraźne działanie potwierdzające). Milczenie, brak aktywności podmiotu, brak odznaczenia okienka z uprzednio zaznaczoną zgodą nie będzie oznaczało, że osoba, której dane dotyczą, wyraziła zgodę.

Najbardziej jaskrawym przejawem niewłaściwej praktyki w tym zakresie jest umieszczanie np. na stronie internetowej lub w formularzu papierowym domyślnie zaznaczonych checkboxów. Zgoda zebrana w ten sposób będzie nieważna.

UWAGA!

Zasada rozliczalności wymaga, by administrator danych osobowych mógł udowodnić wyrażenie zgody przez podmiot danych. Rekomenduje się więc stosowanie przy zapisie na newsletter modelu tzw. *double opt-in*, który składa się z dwóch kroków.

PRZYKŁAD ZGODY PRZY ZAPISIE NA NEWSLETTER W MODELU TZW. DOUBLE OPT-IN

Krok 1

☐ Zgadzam się na otrzymywanie na podany adres e-mail od [nazwa organizacji] informacji o charakterze marketingowym, materiałów promocyjnych, reklamowych, dotyczących usług [nazwa organizacji].

Mam świadomość, że powyższa zgoda jest dobrowolna i mogę wycofać ją w każdej chwili, co nie będzie miało wpływu na zgodność z prawem przetwarzania, które odbyło się przed jej wycofaniem.

Wycofanie zgody jest możliwe poprzez kliknięcie przycisku „rezygnuję” w wiadomości mailowej lub kontakt z [nazwa organizacji sportowej] pod adresem mailowym [adres mailowy organizacji].

Klauzula informacyjna / polityka prywatności opisująca zasady przetwarzania danych osobowych w związku z zapisaniem się do newslettera [link do klauzuli informacyjnej].

Krok 2

W kolejnym kroku użytkownik otrzymuje na wskazany przez niego adres e-mail wiadomość z podziękowaniem za zapisanie się do newslettera i prośbą o potwierdzenie zapisu, np.:

Dziękujemy za zapisanie się do newslettera [nazwa organizacji].

Potwierdź swoją subskrypcję klikając w link zamieszczony w poniższej wiadomości.

Klauzula informacyjna / polityka prywatności opisująca zasady przetwarzania danych osobowych w związku z zapisaniem się do newslettera [link do klauzuli informacyjnej / polityki prywatności].

Jeśli chcesz zrezygnować z subskrypcji, napisz do nas e-mail na adres [adres e-mail organizacji] lub kliknij w przycisk „rezygnuj z newslettera” w stopce wiadomości.

5.1. WYSYŁANIE NEWSLETTERA JAKO USŁUGA ŚWIADCZONA DROGĄ ELEKTRONICZNĄ

Wysyłka newslettera wiąże się najczęściej z przetwarzaniem danych osobowych subskrybentów, dlatego zawsze wymaga odpowiedniej podstawy prawnej zgodnie z art. 6 ust. 1 RODO.

Choć zgoda jest często wykorzystywana jako podstawa prawna do wysyłki newslettera, nie jest to jedyna możliwa opcja. Prawnie uzasadniony interes lub umowa mogą stanowić alternatywne podstawy przetwarzania danych osobowych pod warunkiem spełnienia określonych kryteriów. Organizacja sportowa może wysyłać newsletter jako usługę świadczoną drogą elektroniczną.

PRZYKŁAD

[Organizacja sportowa] przetwarza twoje dane osobowe w celu [promowania działalności statutowej]. Możesz zrezygnować z subskrypcji i zażądać usunięcia swojego adresu e-mail. Więcej informacji o tym, jak przetwarzamy twoje dane i jakie przysługują ci prawa, znajdziesz w polityce prywatności [link].

Adres e-mail:

☐ Akceptuję regulamin usługi [link do regulaminu]

Następnie ścieżka dla potwierdzenia zapisu w formie *double opt-in* jak opisano wyżej.

W podanym przykładzie dochodzi do zamówienia usługi, które następuje poprzez:

- ▶ podanie adresu e-mail w formularzu oraz
- ▶ wyrażenie zgody na postanowienia regulaminu i otrzymywanie na podany w formularzu adres e-mail informacji;
- ▶ kliknięcie w przycisk „wyślij” na końcu zapisu.

Potwierdzenie linku do zapisu (*double opt-in*) i rejestracji powoduje, że adres e-mail zostaje dodany do danej listy mailingowej subskrybentów i subskrybentek. W takim przypadku przetwarzanie danych będzie odbywało się na podstawie art. 6 ust. 1 lit. b RODO, czyli umowy o wysyłkę newslettera, która oparta jest na zasadach opisanych w regulaminie (należy stworzyć regulamin i go udostępnić), oraz na podstawie art. 6 ust. 1 lit. f RODO, czyli realizacji prawnie uzasadnionego interesu, którym może być analiza interakcji pomiędzy organizacją sportową oraz odbiorcami wiadomości.

5.2. PRAWNIE UZASADNIONY INTERES ORGANIZACJI SPORTOWEJ

Artykuł 6 ust. 1 lit. f RODO pozwala na przetwarzanie danych, gdy jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Motyw 47 RODO wyraźnie stwierdza, że przetwarzanie danych osobowych do celów marketingu bezpośredniego można uznać za wykonywane w prawnie uzasadnionym interesie. Newsletter często służy nie tylko celom marketingowym, ale także informacyjnym, co może być uznane za uzasadniony interes administratora przy przetwarzaniu danych osobowych w utrzymywaniu relacji z klientami. W przypadku istniejących klientów/członków wysyłka newslettera może być postrzegana

jako naturalna kontynuacja relacji dotyczącej współpracy. Niemniej jednak należy pamiętać o wymaganiach innych przepisów, takich jak ustawa o świadczeniu usług drogą elektroniczną i Prawo komunikacji elektronicznej.

Przetwarzanie danych osobowych odbiorców newslettera może być oparte na podstawie prawnie uzasadnionego interesu administratora, jeśli:

- ▶ odbiorca/subskrybent jest już klientem organizacji / organizacja ma z nim relację;
- ▶ odbiorca/subskrybent może w każdej chwili wnieść sprzeciw;
- ▶ organizacja sportowa jako administrator danych przeprowadziła test równowagi i wykazał on, że jest to dopuszczalne.

Przy konstruowaniu procesu zapisywania się na newsletter kluczowe jest zapewnienie transparentności, dobrowolności i konkretności zgody, a także umożliwienie jej łatwego wycofania. Należy pamiętać, że każdy przypadek powinien być rozpatrywany indywidualnie, a wybór podstawy prawnej powinien być dobrze uzasadniony i udokumentowany.

UWAGA!

Projektowanie procesów związanych ze zbieraniem zgód marketingowych wiąże się z potrzebą spełnienia wielu wymagań, zarówno z punktu widzenia RODO, jak i PKE, a także szerzej – dotyczących ochrony praw konsumentów, m.in. poprzez unikanie rozwiązań, które będą stosowały tzw. *dark patterns* (ciemne lub mroczne wzorce). Chodzi o stosowanie w internecie lub aplikacjach „sztuczek” wprowadzających użytkownika w błąd.

6. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

ART. 4. PKT. 12 RODO¹⁵⁷

Definicje

„Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”.

UWAGA!

Naruszenia ochrony danych osobowych w sporcie stanowią poważny problem, który może prowadzić do strat finansowych, reputacyjnych oraz prawnych. Organizacje sportowe mają obowiązek przestrzegania przepisów RODO, aby minimalizować ryzyko takich incydentów. Poprzez stosowanie bezpiecznych technologii, edukację personelu oraz wdrażanie procedur ochrony danych osobowych można skutecznie zapobiegać naruszeniom i budować zaufanie wśród zawodników, pracowników i współpracowników podmiotów sportowych oraz kibiców.

Naruszenie ochrony danych osobowych pojawia się zawsze, gdy dochodzi do zdarzenia, które:

- ▶ jest incydem bezpieczeństwa;
- ▶ dotyczy przetwarzanych danych osobowych;
- ▶ może doprowadzić do ich nieuprawnionego zniszczenia, utracenia, zmodyfikowania, ujawnienia lub dostępu do nich.

Naruszeniem ochrony danych osobowych nie jest zdarzenie niespełniające któregoś z tych warunków¹⁵⁸.

¹⁵⁷ P. Fajgielski, *Ogólne rozporządzenie...*, *op.cit.*, art. 4 pkt. 12.

¹⁵⁸ UODO, *Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*, wersja 2.0, s. 8, <https://uodo.gov.pl/pl/138/3561> [dostęp: 10.08.2025].

Naruszeniem ochrony danych osobowych w środowisku sportowym może być m.in. :

- ▶ ujawnienie danych medycznych zawodników, np. informacji o kontuzjach, leczeniu, wynikach testów antydopingowych bez zgody zainteresowanych;
- ▶ publikacja w mediach społecznościowych listy uczestników zawodów, zawierającej imiona i nazwiska oraz inne dodatkowe dane, takie jak adresy e-mail i daty urodzenia, co pozwala na ich identyfikację i kontakt;
- ▶ dostęp nieuprawnionych osób do wyników analizy wydolnościowej przechowywanych w systemach informatycznych klubów lub związków sportowych;
- ▶ kradzież danych osobowych i w konsekwencji upublicznienie informacji o kontraktach trenerów i ich danych finansowych;
- ▶ zagubienie (utrata) przez pracownika klubu nośnika cyfrowego, na którym zgromadzone zostały dane o kibicach, stanowiącego jedyną bazę informacji w klubie.

Naruszeniem ochrony danych osobowych w środowisku sportowym nie będzie m.in.:

- ▶ zagubienie dokumentacji niezawierającej danych osobowych, np. wzorów kontraktów zawodniczych, których nie można powiązać z konkretnym sportowcem;
- ▶ przekazywanie danych osobowych (np. między międzynarodowymi związkami sportowymi) przy zastosowaniu odpowiednich zabezpieczeń i zgodnie z przepisami o transferze danych poza EOG;
- ▶ opublikowanie wyników biegu z numerami startowymi i czasem zawodników;
- ▶ udostępnienie składu drużyny na stronie internetowej klubu, zawierającego imiona i nazwiska zawodników, ale bez dodatkowych danych;
- ▶ wysłanie do osoby uprawnionej załącznika bez szyfrowania mimo przyjętej w klubie procedury, zgodnie z którą załączniki zawierające dane osobowe powinny być szyfrowane (choćby pracownik klubu naruszył w tym przypadku procedurę i jest to incydent bezpieczeństwa, wskazane działanie nie stanowi naruszenia ochrony danych osobowych z art. 4 pkt 12 RODO).

6.1. OCENA RYZYKA NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH W ZWIĄZKU Z ZAISTNIAŁYM NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

Naruszenie ochrony danych osobowych w sporcie może mieć poważne konsekwencje prawne, reputacyjne i finansowe dla organizacji sportowych, dlatego każdy podmiot sportowy musi dokonać oceny ryzyka naruszenia praw lub wolności osób fizycznych w związku z zaistniałym naruszeniem ochrony danych osobowych.

W przypadku wystąpienia incydentu bezpieczeństwa organizacja powinna bezwzględnie ustalić, czy doszło do naruszenia ochrony danych osobowych, a jeśli tak, to podjąć odpowiednie kroki, w tym w razie potrzeby zgłosić naruszenie ochrony danych osobowych do właściwego organu nadzorczego (w Polsce – do Prezesa Urzędu Ochrony Danych Osobowych). Jeżeli naruszenie może wiązać się z wysokim ryzykiem negatywnego wpływu na prawa lub wolności osób fizycznych, należy bez zbędnej zwłoki poinformować o tym również te osoby.

UWAGA!

„Wysokie ryzyko negatywnego wpływu na prawa lub wolności osób fizycznych” to sytuacja, w której naruszenie ochrony danych osobowych może prowadzić do poważnych konsekwencji dla osób, których dane dotyczą. Administrator ma obowiązek ocenić to ryzyko, zawiadomić osoby dotknięte naruszeniem oraz zgłosić je do odpowiednich organów.

Każdy administrator już na etapie wdrażania polityk i procedur wewnętrznych powinien przygotować się na ewentualność, że dojdzie do naruszenia danych w jego podmiocie sportowym. Posiadanie solidnych procedur wykrywania naruszeń, prowadzenia wewnętrznego postępowania i raportowania ułatwi podejmowanie decyzji, czy należy powiadomić odpowiedni organ nadzorczy lub osoby dotknięte naruszeniem, czy też obie te strony. Niezbędne jest także prowadzenie rejestru wszelkich naruszeń ochrony danych osobowych niezależnie od tego, czy istnieje obowiązek powiadomienia o naruszeniu. W każdym takim przypadku należy dokonać oceny indywidualnie, biorąc pod uwagę wszystkie istotne czynniki.

UWAGA!

Naruszenie ochrony danych osobowych, względem którego administrator nie podjął odpowiedniej reakcji i które nie zostało odpowiednio i terminowo rozwiązane, może skutkować szkodami fizycznymi, materialnymi lub niematerialnymi dla osób fizycznych, takimi jak utrata kontroli nad danymi osobowymi lub ograniczenie jej praw, dyskryminacja, oszustwo lub kradzież tożsamości, strata finansowa, nieautoryzowane odwrócenie pseudonimizacji, utrata reputacji podmiotu sportowego, utrata poufności danych osobowych chronionych tajemnicą lub jakakolwiek inna znacząca niedogodność ekonomiczna lub społeczna dla osoby fizycznej, której dane dotyczą.

6.2. KIEDY MUSIMY ZAWIADOMIĆ OSOBY O NARUSZENIU OCHRONY ICH DANYCH OSOBOWYCH?

ART. 34 UST. 1 RODO. ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH¹⁵⁹

„Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu”.

Zawiadomić należy osobę po to, by umożliwić jej podjęcie wszystkich działań profilaktyczno-zapobiegawczych, aby uchronić ją od naruszenia jej praw lub wolności, szczególnie jeśli istnieje potrzeba złagodzenia bezpośredniego ryzyka szkody. Zatem jednym z najważniejszych powodów informowania osób jest pomoc w podjęciu kroków w celu jej ochrony przed skutkami naruszenia.

UWAGA!

Osobę taką należy zawiadomić bez zbędnej zwłoki w terminie możliwie najszybszym, dobierając taki środek komunikacji, który umożliwi jej wielokrotne zapoznanie się z treścią zawiadomienia. Administrator powinien dokonać wyboru sposobu wysyłki zawiadomienia. Może on zdecydować się na tradycyjną wysyłkę pocztą lub pocztą elektroniczną.

6.3. JAKIE INFORMACJE MUSIMY PRZEKAZAĆ W ZAWIADOMIENIU OSOBY O NARUSZENIU OCHRONY DANYCH OSOBOWYCH?

W zawiadomieniu należy:

- ▶ opisać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazać kategorie i przybliżoną liczbę osób,

¹⁵⁹ P. Fajgielski, *Ogólne rozporządzenie...*, *op.cit.*, art. 34 ust. 1.

których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie (czyli co się właściwie stało, jakich kategorii danych oraz ilu osób dotyczyło naruszenie);

- ▶ wskazać imię i nazwisko oraz dane kontaktowe wyznaczonego inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- ▶ opisać możliwe konsekwencje naruszenia ochrony danych osobowych;
- ▶ opisać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeśli to możliwe, administrator powinien udzielić konkretnych i jasnych porad osobom, jakie kroki mogą podjąć, aby się chronić, i w czym może takiej osobie pomóc.

PRZYKŁADY

W klubie dochodzi do naruszenia ochrony danych osobowych, które skutkuje przypadkowym publicznym ujawnieniem dokumentacji zawodników. Prawdopodobnie będzie to miało znaczący wpływ na zawodników dotkniętych tym naruszeniem ze względu na wrażliwość danych i ujawnienie np. danych medycznych o stanie zdrowia i kontuzjach innym osobom. Może to spowodować wysokie ryzyko dla praw lub wolności, więc zawodnicy muszą zostać poinformowani o naruszeniu.

Lekarz medycyny sportowej, będący administratorem przetwarzanych danych medycznych, wysyła dokumentację medyczną, w tym wyniki badań, osobie innej niż ta, której dane dotyczą. Natychmiast powinien poinformować o tym odbiorcę mylnie wysłanej wiadomości/listu, aby ten trwale usunął informacje nie dla niego przeznaczone, ciąży na nim również obowiązek, by o tym naruszeniu poinformować adresata, do którego kierowane były dane medyczne, a którego prywatność w ten sposób została naruszona. Jeżeli lekarz wykonuje pracę dla innego administratora, np. podmiotu medycznego, obowiązek informacyjny wobec takiej osoby spoczywa na tej placówce medycznej jako administratorze, a nie bezpośrednio na lekarzu.

Członek personelu klubu przypadkowo usuwa zapis danych kontaktowych rodziców/opiekunów prawnych małoletniego zawodnika. Dane te muszą więc zostać odtworzone z kopii zapasowej. Jest mało prawdopodobne, aby skutkowało to wysokim ryzykiem dla praw lub wolności tych osób, więc nie muszą być informowane o naruszeniu.

PRZYKŁAD ZAWIADOMIENIA

Wysyłamy tę wiadomość, ponieważ z przykrością musimy poinformować o naruszeniu ochrony danych osobowych zawartych w systemie informatycznym służącym do rejestracji zawodników. Przyczyną naruszenia był atak hackerski wykorzystujący lukę w zewnętrznym systemie obsługiwanym przez zewnętrznego dostawcę.

Przepraszamy za wszelkie niedogodności związane z incydem i zapewniamy, że traktujemy tę sprawę z najwyższą powagą. Kwestia bezpieczeństwa jest dla nas priorytetem, dlatego natychmiast podjęliśmy działania mające na celu zablokowanie nieautoryzowanego dostępu do systemu i wyeliminowanie źródła naruszenia.

Co się wydarzyło?

7 stycznia 2025 r. wspólnie z dostawcą wykryliśmy nieautoryzowany dostęp do bazy danych naszego systemu. W bazie znajdowały się dane dotyczące składanych wniosków o rejestrację zawodników w naszym związku, tj. imię, nazwisko, PESEL, adres zamieszkania, dane kontaktowe – e-mail i numer telefonu. Nie mamy jednak dowodów na pobranie tych danych przez osoby nieautoryzowane.

Podjęte kroki

Natychmiast podjęliśmy działania mające na celu ochronę państwa danych i ograniczenie skutków naruszenia:

- ▶ Zablokowanie dostępu: nasz dostawca zablokował atakującemu dostęp do systemu, aby zapobiec dalszemu wyciekowi danych.
- ▶ Zabezpieczenia: dostawca natychmiast usunął w systemie lukę, która umożliwiała atak. Wspólnie wdrożyliśmy też dodatkowe zabezpieczenia i narzędzia ochrony danych osobowych, aby zapobiec podobnym sytuacjom w przyszłości.
- ▶ Zgłoszenie incydentu do odpowiednich organów: powiadomiliśmy Prezesa Urzędu Ochrony Danych Osobowych oraz policję i CERT Polska (zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w internecie, działający przy państwowym instytucie NASK).
- ▶ Podjęliśmy działania mające na celu identyfikację przyczyn naruszenia oraz wzmocniliśmy środki ochronne.
- ▶ Podjęliśmy stałe monitorowanie zasobów sieci w celu wykrycia, czy doszło do ujawnienia danych lub innej aktywności ze strony hakerów.

Jakie mogą być możliwe zagrożenia i konsekwencje naruszenia ochrony danych osobowych, takich jak imię, nazwisko, PESEL, adres zamieszkania, e-mail lub numer telefonu?

- ▶ Kradzież tożsamości – osoby trzecie mogą wykorzystać dane do nieautoryzowanego zaciągania kredytów lub pożyczek w instytucjach finansowych na szkodę osoby, której dane dotyczą.

- ▶ Zawieranie umów cywilnoprawnych (np. najmu).
- ▶ Wyłudzenie świadczeń ubezpieczeniowych na szkodę właściciela danych.
- ▶ Nieuprawniony dostęp do świadczeń zdrowotnych – atakujący mogą próbować uzyskać dostęp do systemów medycznych i danych o stanie zdrowia osoby dotkniętej wyciekami.
- ▶ Wykorzystanie praw obywatelskich osoby poszkodowanej, np. oddanie głosu w ramach budżetu obywatelskiego lub innych procesów wymagających potwierdzenia tożsamości.
- ▶ Możliwość oszustw telekomunikacyjnych, np. rejestracja karty SIM na czyjeś dane, co może umożliwić dostęp do kont bankowych czy innych usług powiązanych z numerem telefonu.
- ▶ Ryzyko dalszych nadużyć i naruszeń prywatności, w tym wyłudzenia dokumentów tożsamości czy poświadczenia nieprawdy (np. otrzymywanie mandatów na cudze nazwisko).
- ▶ Wykorzystanie prywatnych informacji na forum publicznym w celu naruszenia dobrego imienia osoby lub podważenia jej wyników i osiągnięć sportowych.
- ▶ Otrzymywanie niezamówionych ofert handlowych, np. drogą mailową.
- ▶ Ryzyko prób wyłudzenia także innych danych osobowych przez osoby podszywające się pod zaufane instytucje lub osoby.
- ▶ Osoby nieuprawnione mogą próbować wykorzystać adres e-mail do zakładania kont w internecie.

Co zrobić, aby się chronić? Jakie środki zaradcze rekomendujemy w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych osobowych?

- ▶ Należy powiadomić odpowiednie organy i instytucje. W przypadku kradzieży lub wycieku numeru PESEL i innych danych warto niezwłocznie skontaktować się z bankiem, aby zablokować konta i zmienić hasła oraz zastrzec numery kart płatniczych. Można także zgłosić incydent na policję, dostarczając dokumentację zdarzenia.
- ▶ Możliwe jest zastrzeżenie numeru PESEL, np. w urzędzie gminy, banku, przez aplikację mObywatel lub portal gov.pl, co zmniejsza ryzyko wykorzystania tych danych przez osoby nieuprawnione.
- ▶ Należy zebrać i przechowywać wszelkie dowody naruszenia, takie jak korespondencja, informacje o podejrzanych działaniach czy transakcjach, co może pomóc w ewentualnym procesie odszkodowawczym lub zgłoszeniu przestępstwa.
- ▶ W przypadku obawy o utratę dostępu lub przejęcie kont internetowych lub społecznościowych, w tym na takich platformach, jak Facebook, Instagram czy Twitter, należy skorzystać z dedykowanych formularzy zgłoszeniowych i procedur ich odzyskiwania.
- ▶ Należy dokładnie sprawdzać nadawców wszelkich wiadomości kierowanych do państwa z wykorzystaniem adresu e-mail czy też numeru telefonu.

- ▶ Należy zachować szczególną ostrożność w przypadku otrzymywania z nieznanych źródeł podejrzanych wiadomości, zwłaszcza tych zawierających linki lub prośby o podanie dodatkowych danych. Nie należy klikać w linki i załączniki w wiadomościach pochodzących od nieznanych nadawców.
- ▶ Należy unikać podawania swoich danych osobowych w odpowiedzi na podejrzane wiadomości (np. e-mail).

Co dalej?

Jeśli mają państwo jakiekolwiek pytania lub wątpliwości związane z incydem, prosimy o kontakt z:

1. Biurem związku pod adresem:
2. Z naszym inspektorem ochrony danych [imię i nazwisko] pod adresem e-mail: ochronadanych@... lub listownie na adres:, z dopiskiem „IOD”¹⁶⁰.

Z poważaniem

.....

6.4. ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

RODO nakłada na wszystkie podmioty obowiązek zgłaszania naruszeń ochrony danych osobowych właściwemu organowi nadzorczemu. Organem właściwym do zgłaszania naruszeń jest Prezes Urzędu Ochrony Danych Osobowych. Należy to zrobić w ciągu 72 godzin od stwierdzenia naruszenia lub uzyskania informacji o naruszeniu. Jeśli administrator nie dysponuje jeszcze wszystkimi danymi może skorzystać ze zgłoszenia wstępnego i później sukcesywnie je uzupełniać.

Zgłoszenia do organu nadzorczego można dokonać elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie biznes.gov.pl będącego odwzorowaniem formularza dostępnego na oficjalnej stronie Urzędu Ochrony Danych Osobowych (uodo.gov.pl).

¹⁶⁰ Obowiązek podania imienia i nazwiska IOD oraz jego danych kontaktowych wynika wprost z art. 34 ust. 2 w zw. z art. 33 ust. 3 lit. b rozporządzenia 2016/679.

UWAGA!

Jeżeli organizacja sportowa nie dokona zgłoszenia do organu nadzorczego w ciągu 72 godzin od stwierdzenia naruszenia, musi podać w zgłoszeniu przyczynę tego opóźnienia.

Gdy doszło do naruszenia ochrony danych osobowych, podmiot sportowy musi ustalić prawdopodobieństwo ryzyka wystąpienia naruszenia praw lub wolności osób fizycznych. Jeśli jest prawdopodobne, że zdarzenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, należy powiadomić UODO, jeżeli jest to mało prawdopodobne, wówczas zgłoszenie nie jest konieczne. Jeśli jednak podmiot podejmie decyzję o niezgłaszaniu naruszenia, to musi być w stanie ją uzasadnić, co należy odpowiednio udokumentować w rejestrze naruszeń.

Aby prawidłowo ocenić ryzyko, administratorzy powinni oszacować wagę potencjalnych konsekwencji oraz prawdopodobieństwo ich wystąpienia, uwzględniając następujące okoliczności zdarzenia:

- ▶ rodzaj naruszenia ochrony danych osobowych;
- ▶ charakter, wrażliwość i zakres danych osobowych;
- ▶ łatwość identyfikacji osób, których dane dotyczą;
- ▶ dotkliwość konsekwencji dla osób, których dane dotyczą;
- ▶ cechy szczególne osób, których dane dotyczą;
- ▶ cechy szczególne administratora;
- ▶ liczbę osób, których dane dotyczą.

RODO dotyczy wyłącznie **praw lub wolności osób fizycznych**. Podczas oceny ryzyka związanego z naruszeniem ochrony danych osobowych nie ma więc znaczenia, jakie konsekwencje incydentu poniesie przetwarzająca te dane organizacja jako taka (np. osoba prawna). Administratorzy powinni przyjąć w tym procesie **perspektywę osób**, których dane dotyczą¹⁶¹.

Jeśli podmiot sportowy powierzył przetwarzanie danych osobowych podmiotowi przetwarzającemu, wymagania dotyczące zgłaszania naruszeń powinny zostać szczegółowo opisane w umowie pomiędzy stronami (administrator, podmiot przetwarzający) zgodnie z wymogami art. 28 RODO¹⁶² (patrz: **Powierzenie przetwarzania danych osobowych**).

Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi, wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator, kierując się wytycznymi Europejskiej Rady Ochrony Danych

¹⁶¹ UODO, *Obowiązki administratorów...*, op.cit., s. 64.

¹⁶² P. Fajgielski, *Ogólne rozporządzenie...*, op.cit., art. 28.

nr 8/2022, powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem, jest Prezes UODO, czy też może inny europejski organ nadzorczy. Celem wskazanych wytycznych jest wyjaśnienie zasad identyfikacji organu nadzorczego, który ma sprawować nadzór nad transgranicznym przetwarzaniem danych osobowych. Pomagają one wyeliminować wątpliwości co do tego, który organ nadzorczy powinien być wiodący, zwłaszcza przy podmiotach działających w więcej niż jednym państwie członkowskim UE/EOG, ujednolicają podejście do kwestii transgranicznego przetwarzania i poprawiają efektywność nadzoru, zapewniając jasność administracyjną zarówno dla organów, jak i dla przedsiębiorstw oraz innych podmiotów przetwarzających dane¹⁶³.

UWAGA!

Obowiązujący wzór zgłoszenia znajduje się na stronie www.uodo.gov.pl.

6.5. A CO, JEŚLI NIE DYSPONUJEMY JESZCZE WSZYSTKIMI WYMAGANYMI INFORMACJAMI?

RODO uznaje, że nie zawsze będzie możliwe pełne zbadanie naruszenia w ciągu 72 godzin od momentu stwierdzenia naruszenia, aby dokładnie zrozumieć, co się stało i co należy zrobić. Dlatego art. 33 RODO¹⁶⁴ pozwala na dostarczanie wymaganych informacji etapami, sukcesywnie do organu nadzorczego, o ile odbywa się to bez zbędnej dalszej zwłoki. Obowiązkiem administratora w takich sytuacjach jest także wyjaśnienie organowi, dlaczego nastąpiło to opóźnienie, i poinformować go, kiedy może spodziewać się przesłania dodatkowych informacji.

PRZYKŁAD

W siedzibie związku sportowego wykryte zostało włamanie na skrzynki pocztowe wszystkich pracowników i współpracowników. Uzyskane zostały informacje, że ktoś posiada już dostęp do wiadomości zawierających załączniki z danymi osobowymi, ale nie wiadomo jeszcze, w jaki sposób i w jakim zakresie atakujący uzyskał dostęp do tych danych oraz czy skopiował również dane z całej poczty e-mail.

¹⁶³ Wytyczne EROD nr 8/2022 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego, wersja 2.0, przyjęta 28 marca 2023 r.

¹⁶⁴ P. Fajgielski, *Ogólne rozporządzenie...*, *op.cit.*, art. 33 ust. 4.

Należy powiadomić Prezesa Urzędu Ochrony Danych Osobowych w ciągu 72 godzin od momentu stwierdzenia naruszenia, w formie zgłoszenia wstępnego wyjaśniając, że podmiot sportowy nie posiada jeszcze wszystkich istotnych szczegółów, ale że prowadzi postępowanie wyjaśniające w tej sprawie i spodziewa się jego wyników w ciągu kilku następnych dni. Gdy postępowanie ujawni szczegóły dotyczące naruszenia bezzwłocznie przekaze dalsze informacje i dowody organowi nadzorcemu.

6.6. DOKUMENTOWANIE NARUSZEŃ

ART. 33 UST. 5 RODO¹⁶⁵

„Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu na weryfikowanie przestrzegania niniejszego artykułu”.

UWAGA!

Obowiązkiem podmiotu sportowego jest odnotowanie wszystkich naruszeń, niezależnie od tego, czy muszą zostać zgłoszone do organu nadzorczego, czy też nie.

Wymagane jest udokumentowanie faktów dotyczących naruszenia, jego skutków i podjętych działań zaradczych. Jest to obowiązek administratora, u którego doszło do przedmiotowego naruszenia. Jego dopełnienie pozwala organowi nadzorcemu zweryfikować, czy organizacja wywiązuje się z obowiązków, jakie nakładają na administratora przepisy prawa.

Podobnie jak w przypadku każdego incydentu bezpieczeństwa, należy zbadać, czy naruszenie było wynikiem błędu ludzkiego, czy też problemu systemowego, i sprawdzić, jak można zapobiec jego powtórzeniu w przyszłości.

¹⁶⁵ *Ibidem*, art. 33 ust. 5.

UWAGA!

Błąd ludzki jest główną przyczyną zgłaszanych naruszeń ochrony danych osobowych. Aby zmniejszyć jego ryzyko, należy podjąć stosowne działania, takie jak:

- ▶ obowiązkowe szkolenie wprowadzające i szkolenia doszkalające z zakresu ochrony danych dla pracowników i współpracowników podmiotów sportowych;
- ▶ wsparcie, nadzór i kontrola nad obowiązkami pracowników i współpracowników, podmiotów sportowych, którzy na swoich stanowiskach pracy i w trakcie pełnienia określonych funkcji przetwarzają dane osobowe, w szczególności na dużą skalę;
- ▶ aktualizowanie zasad i procedur wewnętrznych dla pracowników i współpracowników, podmiotów sportowych, którzy powinni czuć się uprawnieni do zgłaszania incydentów administratorowi;
- ▶ stosowanie dobrych praktyk w zakresie zabezpieczania środowiska przetwarzania danych;
- ▶ badanie przyczyn naruszeń, które następowały w przeszłości;
- ▶ wdrażanie środków technicznych i organizacyjnych w podmiotach sportowych wspierających bezpieczeństwo danych.

W ramach procesu zarządzania naruszeniami należy prowadzić systematyczne oceny ryzyka, aby ocenić wpływ naruszeń i spełnić wymagania dotyczące raportowania i rejestrowania. Będzie to stanowić podstawę polityki dotyczącej naruszeń i pomoże wykazać odpowiedzialność administratora.

6.6.1. CO SIĘ STANIE, JEŻELI NIE POWIADOMIMY ORGANU NADZORCZEGO O WSZYSTKICH NARUSZENIACH PODLEGAJĄCYCH ZGŁOSZENIU?

Niepowiadomienie Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu, gdy jest to wymagane, może skutkować wysoką karą finansową (do 10 lub 20 mln euro, do 2% lub 4% całkowitego rocznego obrotu podmiotu z poprzedniego roku). Kara finansowa może być łączona z innymi uprawnieniami naprawczymi Prezesa Urzędu Ochrony Danych Osobowych. Ważne jest, aby podmiot sportowy upewnił się, że posiada opracowany proces zgłaszania naruszeń oraz że możliwe jest wykrycie naruszenia, jeżeli ono wystąpi, i obowiązkowo powiadamiać o naruszeniach na czas, dostarczając niezbędne szczegóły organowi nadzorcemu, chyba że jest mało prawdopodobne, by dane zdarzenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Jeśli podmiot zdecyduje, że nie musi zgłaszać naruszenia, powinien być w stanie uzasadnić tę decyzję i ją udokumentować.

6.6.2. DOBRE PRAKTYKI W ZAPOBIEGANIU NARUSZENIOM OCHRONY DANYCH OSOBOWYCH

Aby uniknąć naruszeń ochrony danych osobowych, organizacje sportowe powinny skorzystać z wdrożenia niektórych środków wspomagających administratora w podnoszeniu poziomu bezpieczeństwa danych w organizacji:

- ▶ szyfrowanie *end-to-end* z zarządzaniem kluczami – szyfrowanie danych polega na kodowaniu informacji w taki sposób, aby dostęp do nich miały tylko upoważnione osoby. Szyfrowanie przekształca dane w nieczytelny format. Pozostają one zakodowane, dopóki nie dotrą do miejsca przeznaczenia. Tylko osoby mające dostęp do kluczy deszyfrujących mogą ponownie odblokować dane w punkcie końcowym;
- ▶ kontrola dostępu – role mogą być oparte na funkcjach pełnionych w organizacji w związku z przynależnością do określonego zespołu lub projektu. Użytkownicy mają dostęp tylko do tych informacji, których potrzebują, aby wykonywać swoją pracę i zadania;
- ▶ w przypadku pracy w systemach i z wykorzystaniem poczty mailowej należy zadbać o bezpieczne tworzenie kopii zapasowych i odzyskiwanie danych. Aby bezpiecznie zarządzać danymi, kopia zapasowa musi być zawsze dostępna. W przypadku naruszenia lub utraty danych szybko i skutecznie można przywrócić wszystkie informacje;
- ▶ poufność zapewnia, że prywatne dane są dostępne tylko dla upoważnionych osób lub podmiotów. Zasada ta obejmuje stosowanie silnego szyfrowania, kontroli dostępu i uwierzytelniania. Zapobiega to nieautoryzowanemu dostępowi, ujawnieniu lub wyciekowi danych i poufnych informacji;
- ▶ regularne audyty bezpieczeństwa – weryfikacja obszarów przetwarzania danych i systemów informatycznych pod kątem podatności na zagrożenia;
- ▶ ciągłe monitorowanie bezpieczeństwa i wykrywanie włamań – wdrożenie rozwiązania do monitorowania bezpieczeństwa, i zwalczanie cyberzagrożeń. Im szybciej wykryje się zagrożenie, tym łatwiej zapobiec szkodom;
- ▶ szkolenia personelu – podnoszenie świadomości pracowników, współpracowników, osób, które są upoważnione do przetwarzania danych w projektach sportowych na temat bezpieczeństwa i ochrony danych osobowych;
- ▶ wdrożenie planów reagowania na incydenty – opracowanie procedur postępowania w przypadku naruszenia danych osobowych.

7. ODPOWIEDZIALNOŚĆ I SANKCJE

Brak zgodności z przepisami RODO może prowadzić nie tylko do odpowiedzialności administracyjnej egzekwowanej przez organ nadzoru, ale również do odpowiedzialności cywilnoprawnej, dochodzonej w postępowaniu sądowym, oraz odpowiedzialności karnej, którą wprowadziły przepisy ustawy o ochronie danych osobowych.

Prezes Urzędu Ochrony Danych Osobowych posiada szerokie uprawnienia i kompetencje kontrolne oraz nadzorcze w zakresie ochrony danych osobowych w Polsce, wynikające zarówno z RODO, jak i krajowej ustawy o ochronie danych osobowych.

7.1. ODPOWIEDZIALNOŚĆ ADMINISTRACYJNA

ART. 58 UST. 2 RODO. UPRAWNIENIA¹⁶⁶

„Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia naprawcze:

- a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania;
- b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania;
- c) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
- d) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;

¹⁶⁶ P. Fajgielski, *Ogólne rozporządzenie...*, *op.cit.*, art. 58 ust. 2.

- e) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
- g) nakazanie na mocy art. 16, 17 i 18 sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- h) cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
- i) zastosowanie, oprócz lub zamiast środków, o których mowa w niniejszym ustępie, administracyjnej kary pieniężnej na mocy art. 83, zależnie od okoliczności konkretnej sprawy;
- j) nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej”.

Osoba, której dane są przetwarzane, jeśli uzna, że administrator naruszył ochronę jej danych osobowych, może złożyć skargę do organu nadzorczego. Po zakończonym postępowaniu Prezes UODO wydaje decyzję administracyjną, w której w przypadku stwierdzenia naruszenia może nałożyć karę pieniężną w wysokości do 10 mln euro albo do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, a w przypadku poważniejszych naruszeń – w wysokości do 20 mln euro albo do 4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego.

Kary pieniężne nakładane za naruszenia RODO mają być skuteczne, proporcjonalne i odstraszające.

Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, Prezes UODO zwraca w każdym indywidualnym przypadku należytą uwagę na:

- ▶ charakter, wagę i czas trwania naruszenia przy jednoczesnym uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczbę poszkodowanych osób, których dane dotyczą, oraz rozmiar poniesionej przez nie szkody;
- ▶ umyślny lub nieumyślny charakter naruszenia;
- ▶ działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

- ▶ stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych przez nich wdrożonych;
- ▶ wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
- ▶ stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
- ▶ kategorie danych osobowych, których dotyczyło naruszenie.

UWAGA!

Organ bierze pod uwagę fakt, czy administrator zgłosił naruszenie.

PRZYKŁAD

Ukarany podmiot: Dolnośląski Związek Piłki Nożnej

Kwota: 12 950 euro (55 750,50 zł).

Podstawa naruszenia: art. 6 RODO

Zakres naruszenia: związek sportowy opublikował dane osobowe dotyczące sędziów, którym przyznano licencje sędziego drogą internetową: imiona i nazwiska, a także dokładne adresy i numery PESEL. Tymczasem *nie ma podstawy prawnej*, aby tak szeroki zakres danych dotyczących sędziów był dostępny w internecie. Ujawniając je, administrator stwarzał potencjalne ryzyko ich nieuprawnionego użycia, np. podszywania się pod nich w celu zaciągania pożyczek lub innych zobowiązań. Chociaż związek sam zauważył swój błąd, o czym świadczy powiadomienie Prezesa UODO o naruszeniu ochrony danych osobowych, fakt, że próby usunięcia go były nieskuteczne, determinował nałożenie kary.

Zakres oceny naruszenia: przy ustalaniu wysokości kary finansowej (55 750,50 zł) Prezes UODO wziął pod uwagę m.in. czas trwania naruszenia oraz fakt, że dotyczył on dużej grupy osób (585 sędziów). Prezes UODO stwierdził, że chociaż naruszenie zostało ostatecznie usunięte, miało ono poważny charakter.

Okoliczności łagodzące: nakładając karę, Prezes UODO wziął również pod uwagę okoliczności łagodzące, takie jak dobra współpraca pomiędzy administratorem a organem nadzorczym czy brak dowodów, że szkoda została wyrządzona osobom, których dane zostały ujawnione.

Podmiot, który został ukarany administracyjną karą pieniężną może zaskarżyć decyzję w ramach postępowania sędowo-administracyjnego, wnosząc w terminie 30 dni od dnia jej doręczenia skargę do Wojewódzkiego Sądu Administracyjnego.

ART. 108 USTAWY O OCHRONIE DANYCH OSOBOWYCH¹⁶⁷

„Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch”.

Brak współpracy z organem nadzorczym w ramach postępowania administracyjnego stanowi także podstawę do nałożenia wyższej kary pieniężnej przez Prezesa UODO. Okoliczność wskazana w art. 108 UODO może stać się podstawą odpowiedzialności karnej. Udaremnienie kontroli może też stać się podstawą ewentualnej sankcji administracyjnej ze strony organu nadzorczego. Tej samej karze podlega każdy, kto w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej nie dostarcza danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarcza dane, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej.

7.2. ODPOWIEDZIALNOŚĆ CYWILNA

Niezależnie od złożenia skargi do Prezesa UODO podmiot danych może także dochodzić obrony swoich praw na drodze procesu cywilnego. RODO przewiduje dwa rodzaje powództw:

- ▶ pierwsze dotyczy przywrócenia stanu zgodnego z prawem, czyli zaprzestania naruszeń (czy to w wyniku podjęcia czy też zaniechania określonych działań);
- ▶ drugie to powództwo o odszkodowanie.

ART. 82 RODO. PRAWO DO ODSZKODOWANIA I ODPOWIEDZIALNOŚĆ¹⁶⁸

„Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę”.

W procesie wytoczonym na tej podstawie mamy do czynienia z tzw. odwróconym ciężarem dowodowym. To nie powód musi udowodnić, że pozwany ponosi

¹⁶⁷ *Ibidem*, s. 886, art. 108.

¹⁶⁸ *Ibidem*, art. 82.

odpowiedzialność za szkodę. Przeciwnie – administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności, jeżeli to oni udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

7.3. ODPOWIEDZIALNOŚĆ KARNA

RODO nie reguluje kwestii związanych z odpowiedzialnością karną w razie jego naruszenia. Motyw 149 preambuły wskazuje jednak, że państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie jego postanowień, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Polska Ustawa o ochronie danych osobowych penalizuje dwa typy czynów zabronionych.

ART. 107 USTAWY O OCHRONIE DANYCH OSOBOWYCH. BEZPRAWNE PRZETWARZANIE DANYCH OSOBOWYCH¹⁶⁹

„1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech”.

¹⁶⁹ *Ibidem*, art. 107.

8. ORGANIZACJA „MAŁEJ” IMPREZY SPORTOWEJ – ZAPROJEKTOWANIE PROCESU ORGANIZACJI IMPREZY SPORTOWEJ POD KĄTEM PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Mając na uwadze obowiązującą zasadę ochrony danych w fazie projektowania, należy odpowiednio zaprojektować proces organizacji imprezy sportowej pod kątem przepisów o ochronie danych osobowych (patrz: *Ochrona danych w fazie projektowania i domyślna ochrona danych*). Szczególnie trzeba zwrócić uwagę na następujące kwestie:

- ▶ zebranie jakich danych od uczestników imprezy sportowej jest niezbędne;
- ▶ w jakim celu dane te będą wykorzystywane;
- ▶ w oparciu o jaką podstawę prawną możliwe jest przetwarzanie tych danych osobowych;
- ▶ jak długo dane te będą musiały być przechowywane;
- ▶ w jaki sposób dane osobowe będą przetwarzane (w formie zgłoszeń papierowych czy elektronicznych; czy na potrzeby imprezy sportowej zostanie stworzona odrębna strona internetowa);
- ▶ kto będzie miał dostęp do danych osobowych;
- ▶ czy dane osobowe uczestników będą przekazywane do innych podmiotów (jeżeli tak, jaka będzie ich rola w zakresie przetwarzania danych osobowych);
- ▶ jakie środki bezpieczeństwa zastosować, biorąc w szczególności pod uwagę zakres zbieranych danych, cele oraz sposoby przetwarzania;
- ▶ w jaki sposób zostanie umożliwione korzystanie z praw przez osoby, których dane dotyczą, w jaki sposób będzie spełniany obowiązek informacyjny.

8.1. ZAKRES ZBIERANYCH DANYCH

Organizacja sportowa, która zamierza zorganizować imprezę sportową, zapewne zbierać będzie dane osobowe uczestników. Każdorazowo należy zastanowić się, jakie dane są niezbędne i w jakim celu będą wykorzystywane.

Najprawdopodobniej konieczne będą dane identyfikacyjne, dotyczące np. wieku uczestników, jeżeli współzawodnictwo sportowe lub podział na grupy jest uzależnione od kryterium wiekowego, a w przypadku, gdy organizator imprezy będzie również zapewniać wyżywienie, konieczne może być zebranie informacji o alergiach pokarmowych czy przeciwskazaniach do przyjmowania określonych pokarmów.

Jeżeli organizacja sportowa zamierza wykorzystywać wizerunek uczestników imprezy, powinna zapewnić sobie taką możliwość. W tym zakresie istotne jest to, w jakich celach wizerunek będzie wykorzystywany (patrz: *Przetwarzanie danych osobowych w postaci wizerunku*). Każdorazowo jednak należy to ustalić przed zebraniem danych i odpowiednio ten proces zaplanować.

Jeżeli organizacja sportowa chce wykorzystywać dane uczestników imprezy sportowej w celach marketingowych czy też promocji kolejnych wydarzeń, które będzie organizować, powinna co do zasady uzyskać zgodę uczestnika (patrz: *Przetwarzanie danych w celach marketingu*).

PRZYKŁAD

W zależności od realizacji celu organizacja sportowa może wykorzystywać w szczególności następujące dane osobowe:

- ▶ imię i nazwisko;
- ▶ wiek uczestnika;
- ▶ przynależność do klubu sportowego / szkoły sportowej;
- ▶ zaświadczenie o braku przeciwwskazań do udziału w imprezie sportowej;
- ▶ informacje o preferencjach żywieniowych, alergiach pokarmowych;
- ▶ wizerunek.

UWAGA!

Nie należy zbierać danych „na zapas”. Zawsze trzeba zastanowić się, po co i jakie dane są w konkretnej sytuacji potrzebne, i tylko w tym zakresie je zbierać.

8.2. REGULAMIN UCZESTNICTWA W IMPREZIE

Częstą praktyką jest ustalanie zasad uczestnictwa w imprezie sportowej w formie regulaminu imprezy sportowej. W takim przypadku dokument ten powinien określać, jakie dane będą zbierane od uczestników, w jakiej formie oraz na jakich zasadach możliwy jest udział zawodnika w imprezie sportowej.

UWAGA!

W przypadku, gdy uczestnikami imprezy sportowej są małoletni (osoby poniżej 18. roku życia), wszystkie zgody, formularze powinny być wypełnione i podpisane przez ich przedstawicieli ustawowych, czyli rodziców lub opiekunów prawnych.

8.3. PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH UCZESTNIKÓW IMPREZY

Co do zasady podstawą prawną przetwarzania danych osobowych uczestników imprezy sportowej mogą być:

- ▶ wykonanie umowy (poprzez akceptację regulaminu imprezy sportowej) – art. 6 ust. 1 lit. b RODO;
- ▶ wypełnienie obowiązku prawnego ciążącego na organizacji sportowej jako administratorze – art. 6 ust. 1 lit. c RODO – w sytuacji, gdy np. uczestnictwo w imprezie jest związane z koniecznością zapłaty opłat/wpisowego, a co za tym idzie, koniecznością dokonania rozliczeń podatkowych przez organizację sportową wynikających z przepisów prawa;
- ▶ prawnie uzasadniony interes administratora danych osobowych – art. 6 ust. 1 lit. f RODO, jeżeli przetwarzanie danych jest niezbędne do dochodzenia roszczeń lub obrony przed roszczeniami związanymi z prowadzoną działalnością, monitorowaniem imprezy sportowej czy też podania i udokumentowania wyników rywalizacji sportowej oraz umożliwienia śledzenia rywalizacji sportowej na żywo;
- ▶ zgoda osoby, której dane dotyczą – art. 6 ust. 1 lit. a RODO, gdy dane są przetwarzane w celach marketingowych czy też wizerunek jest wykorzystywany w celach marketingowych;
- ▶ realizacja zadania w interesie publicznym – art. 6 ust. 1 lit. e RODO, gdy impreza sportowa organizowana jest przez polski związek sportowy;

- ▶ odnośnie do danych szczególnej kategorii (np. informacji o niepełnosprawności zawodnika, jeżeli jest niezbędna do udziału w imprezie sportowej, informacja o braku przeciwwskazań zdrowotnych do udziału) – art. 9 ust. 2 lit. d RODO w przypadku, gdy zawodnik jest np. członkiem stowarzyszenia, lub art. 9 ust. 2 lit. a RODO, a więc wyraźna zgoda uczestnika imprezy sportowej.

8.4. ZAPEWNIENIE REALIZACJI PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Należy pamiętać, by zapewnić możliwość realizacji praw uczestników imprezy sportowej wynikających z przepisów o ochronie danych osobowych. W szczególności należy pamiętać o zapewnieniu prawa dostępu do danych osobowych, ewentualnie uzyskania kopii danych osobowych, a także prawa do sprostowania danych, gdy okażą się one nieprawidłowe lub niepełne (patrz: Prawa osób, których dane są przetwarzane).

W przypadku, gdy przetwarzanie danych odbywa się na podstawie zgody uczestnika, konieczne jest zapewnienie możliwości wycofania zgody w dowolnym momencie. Istotne jest, aby było to równie łatwe jak jej wyrażenie (patrz: Zgoda osoby, której dane osobowe są przetwarzane).

8.5. OBOWIĄZEK INFORMACYJNY

Konieczne jest spełnienie wobec uczestników imprezy sportowej obowiązku informacyjnego (patrz: Obowiązek informacyjny). Powinno to nastąpić przy pozyskaniu danych osobowych, jeżeli dane zostały bezpośrednio podane przez uczestników imprezy sportowej. Możliwe jest to m.in. poprzez umieszczenie wymaganych informacji w regulaminie imprezy sportowej. Ewentualnie treści wymaganych informacji można przekazać podczas odbioru zgłoszenia udziału w imprezie lub inaczej w zależności od sposobu zbierania danych osobowych i możliwości kontaktu z uczestnikami.

8.6. UREGULOWANIE ZASAD DOSTĘPU DO DANYCH OSOBOWYCH

Osoby, które będą przetwarzać dane osobowe uczestników imprezy sportowej w imieniu organizatora, powinny mieć zapewniony stosowny dostęp. W tym zakresie należy pamiętać, że dostęp do danych powinni mieć tylko takie osoby, dla których jest to niezbędne do realizacji obowiązków służbowych, np. prowadzący zapisy

na imprezę, rejestrujący uczestników, wydający pakiety startowe, rozliczający wpłaty uczestników itd. Osoby te powinny zostać przeszkolone w zakresie ochrony danych osobowych, a także zobowiązane do zachowania w poufności danych osobowych, z którymi zetknęły się przy realizacji obowiązków służbowych.

UWAGA!

Nie każda osoba, która pomaga organizatorowi w przygotowaniu i podczas trwania imprezy sportowej, musi mieć nadane upoważnienie do przetwarzania danych osobowych. Przykładowo wolontariusz, który czuwa nad prawidłowym przebiegiem imprezy sportowej czy też pomaga zawodnikom w kwestiach organizacyjnych, może nie mieć potrzeby dostępu do danych osobowych uczestników imprezy sportowej.

W przypadku, gdy organizator imprezy będzie korzystał z usług podmiotów zewnętrznych przy przetwarzaniu danych osobowych (podmioty te będą przetwarzały dane w jego imieniu i na jego rzecz), powinien zwrócić uwagę na to, aby wybrać do współpracy tylko takie podmioty, które spełniają gwarancje bezpieczeństwa przetwarzania danych osobowych. konieczne jest również zawarcie z tymi podmiotami umowy powierzenia przetwarzania danych osobowych zgodnie z wymogami RODO (patrz: Podmiot przetwarzający).

PRZYKŁADY

- ▶ podmiot udostępniający narzędzie internetowe do obsługi zapisów na imprezę sportową;
- ▶ podmiot zewnętrzny rozliczający wpłaty uczestników;
- ▶ podmiot monitorujący parametry uczestników w trakcie zawodów;
- ▶ podmiot prowadzący monitoring wizyjny imprezy sportowej.

UWAGA!

Przekazywanie danych osobowych do podmiotów zewnętrznych, które posiadają swoje cele przetwarzania i samodzielnie ustalają sposoby przetwarzania, np. podmiotów świadczących usługi hotelowe, zapewniających transport uczestników, nie będzie odbywać się co do zasady na podstawie powierzenia przetwarzania danych osobowych, ale na podstawie udostępnienia danych osobowych. Należy pamiętać, żeby zweryfikować, czy istnieje podstawa prawna do przekazania danych osobowych tym podmiotom, a jeżeli tak, dopilnować, aby odbyło się to w sposób bezpieczny, np. przekazanie listy uczestników imprezy w formie zaszyfrowanej na adres mailowy.

8.7. UPUBLICZNIENIE DANYCH OSOBOWYCH

Organizator imprezy sportowej może być zainteresowany tym, aby umożliwić śledzenie przebiegu rywalizacji sportowej na żywo lub upublicznić informację o wynikach osiągniętych przez uczestników imprezy sportowej. Wydaje się uzasadnione informowanie o osobach, które zajęły miejsce na podium imprezy, i osiągniętych przez nich wynikach. Należy jednak zawsze pamiętać o zasadzie minimalizacji danych, a więc udostępnianiu tylko tych, które są niezbędne, np. imienia i nazwiska, przynależności do klubu sportowego, osiągniętego wyniku sportowego oraz zajętego miejsca. Konieczne jest również odpowiednie poinformowanie o tym uczestników imprezy sportowej w treści obowiązku informacyjnego, aby mieli oni świadomość tego, że ich dane będą wykorzystane właśnie w tym celu.

8.8. OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

Dane przetwarzane w ramach organizacji imprezy sportowej powinny być przechowywane jedynie przez okres niezbędny do realizacji celu, w którym są przetwarzane. W przypadku danych niezbędnych do uczestnictwa w imprezie sportowej mogą być one przetwarzane do jej zakończenia.

Jeżeli konieczne są rozliczenia finansowe, np. wystawianie faktur lub paragonów za udział w imprezie, dane przetwarzane w tym celu powinny być przechowywane przez okres niezbędny do realizacji obowiązków wynikających z przepisów prawa, w tym przepisów ustawy o rachunkowości. Co do zasady jest to okres pięciu lat od końca roku kalendarzowego, w którym powstał obowiązek podatkowy.

Organizator imprezy sportowej może również rozważyć przechowywanie danych osobowych przez okres niezbędny do dochodzenia roszczeń i obrony przed roszczeniami związanymi z organizowaną imprezą czy też zapewnienia rzetelności współzawodnictwa sportowego poprzez udostępnianie informacji dotyczących osiągniętych wyników sportowych. Należy jednak w tym zakresie przeprowadzić test równowagi i ustalić, czy interesy organizatora imprezy jako administratora danych osobowych są nadrzędne wobec interesów osoby, której dane dotyczą (patrz: *Przeprowadzenie testu równowagi*).

9. PRZETWARZANIE DANYCH OSOBOWYCH ZAWODNIKÓW PRZEZ KLUB SPORTOWY, ZWIĄZEK SPORTOWY I POLSKI ZWIĄZEK SPORTOWY

Dane osobowe zawodników przetwarzane są na różnych poziomach przez różne podmioty. W zależności od specyfiki podmiotu i relacji łączącej zawodnika z tym podmiotem różne mogą być cele przetwarzania, a co za tym idzie, związane z nimi podstawy prawne ich wykorzystywania. Będzie to również wyznaczać zakres przetwarzanych danych osobowych oraz okres ich przechowywania.

9.1. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ KLUB SPORTOWY

9.1.1. PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH ZAWODNIKÓW

Zawodnicy przynależą do klubów sportowych głównie na podstawie stosunku członkostwa lub stosownej umowy. W zależności od tego, jaki charakter relacji łączy klub sportowy z zawodnikiem, podstawy prawne przetwarzania danych osobowych mogą być różne.

Stosunek łączący klub sportowy z zawodnikiem ma najczęściej charakter umowny. Oznacza to, że w zakresie, w jakim dane osobowe są niezbędne do zawarcia lub realizacji umowy, ich przetwarzanie odbywać się będzie w oparciu o podstawę prawną wskazaną w art. 6 ust. 1 lit. b RODO, tj. konieczność do realizacji umowy. Podstawa ta powinna mieć też zastosowanie w przypadku zawodników na szczeblu amatorskim. Jeżeli uczestnictwo w zawodach opiera się np. na deklaracji gry amatora, to poprzez jej podpisanie i złożenie dochodzi do zawarcia umowy pomiędzy

zawodnikiem a klubem sportowym. Na jej mocy zawodnik zobowiązuje się do reprezentowania barw danego klubu sportowego, natomiast klub sportowy – do zapewnienia mu możliwości uczestnictwa w treningach i zawodach w ramach barw klubowych oraz np. pokrycia kosztów m.in. związanych z dojazdem na treningi, mecze, czy też kosztów zakupu sprzętu sportowego. Podobna sytuacja ma miejsce, gdy zawodnik przystępuje do klubu sportowego poprzez złożenie deklaracji przystąpienia. W takim przypadku również dochodzi do powstania stosunku umownego pomiędzy zawodnikiem a klubem sportowym.

Klub sportowy ma określone obowiązki prawne związane z łączącą go relacją prawną z zawodnikiem. W zależności od statusu prawnego klubu sportowego, jego formy prawnej, zakresu prowadzonej działalności mogą na nim ciążyć określone obowiązki nakładane przez przepisy prawa. W takim przypadku konieczne będzie przetwarzanie danych osobowych w zakresie wynikającym z przepisów prawa lub niezbędnym do realizacji obowiązków określonych w tych przepisach. Będzie się to odbywać na podstawie art. 6 ust. 1 lit. c RODO, tj. niezbędności do spełnienia obowiązku prawnego ciążącego na klubie sportowym jako administratorze danych osobowych.

PRZYKŁADY

- ▶ ustawa z dnia 25 czerwca 2010 r. o sporcie;
- ▶ ustawa z dnia 21 kwietnia 2017 r. o zwalczaniu dopingu w sporcie;
- ▶ ustawa z dnia 7 kwietnia 1989 r. – Prawo o stowarzyszeniach;
- ▶ ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych;
- ▶ ustawa z dnia 29 września 1994 r. o rachunkowości;
- ▶ ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych.

W przypadku, gdy zawodnik jest zatrudniony w klubie sportowym na umowie o pracę, podstawą przetwarzania jego danych osobowych będzie również obowiązek prawny wynikający z przepisów prawa, w szczególności w zakresie obowiązków wynikających z Kodeksu pracy oraz aktów wykonawczych do tej ustawy. Przepisy te będą również wyznaczać główny zakres możliwych do przetwarzania danych osobowych (należy zwrócić szczególną uwagę na art. 22¹-22³ Kodeksu pracy oraz cele, w których dane mogą być przetwarzane).

W zakresie, w jakim klub sportowy realizuje zadania publiczne, np. korzystając z dotacji, przetwarzanie danych osobowych zawodników będzie odbywać się co do zasady na podstawie art. 6 ust. 1 lit. e RODO, tj. niezbędności do realizacji zadania w interesie publicznym, w zakresie, w jakim jest to niezbędne do realizacji tego celu przetwarzania.

Możliwe, że przetwarzanie danych osobowych zawodników będzie odbywać się w oparciu o prawnie uzasadniony interes klubu sportowego (art. 6 ust. 1 lit. f RODO), np. w kontekście wykorzystywania monitoringu wizyjnego wobec zawodników, udostępnienia informacji o zawodniku i osiągniętych przez niego wynikach czy przetwarzania danych osobowych zawodnika na potrzeby marketingu bezpośredniego klubu sportowego oraz dochodzenia roszczeń lub obrony przed roszczeniami związanymi z prowadzoną przez klub sportowy działalnością.

UWAGA!

W przypadku oparcia przetwarzania danych osobowych na podstawie prawnej w postaci prawnie uzasadnionego interesu klubu sportowego konieczne jest przeprowadzenie testu równowagi. Należy ocenić, czy interesy zawodnika w danej sytuacji nie są nadrzędne wobec interesu klubu sportowego, bowiem w takim przypadku nie będzie możliwe oparcie przetwarzania na tej podstawie prawnej (**patrz: Przeprowadzenie testu równowagi**).

Przetwarzanie danych osobowych zawodników może również opierać się na podstawie zgody zawodnika (art. 6 ust. 1 lit. a RODO), np. gdy jego dane osobowe będą wykorzystywane do działań marketingowych podejmowanych przez klub sportowy. Należy jednak mieć na względzie, że zgoda na przetwarzanie danych osobowych powinna mieć charakter konkretny, tj. wskazywać wprost, w jakim celu dane osobowe będą przetwarzane, a także dobrowolny, tzn. że zawodnik powinien móc wyrazić zgodę lub jej nie wyrazić bez żadnych negatywnych konsekwencji (**patrz: Zgoda osoby, której dane osobowe są przetwarzane**).

W przypadku wykorzystania wizerunku zawodnika w grę mogą wchodzić przede wszystkim podstawy prawne w postaci zgody na rozpowszechnianie wizerunku albo – gdy pomiędzy zawodnikiem a klubem sportowym została zawarta umowa na wykorzystanie wizerunku – będzie on przetwarzany na podstawie art. 6 ust. 1 lit. b RODO, tj. jako niezbędny do realizacji umowy pomiędzy klubem sportowym a zawodnikiem (**patrz: Przetwarzanie danych osobowych w postaci wizerunku**).

UWAGA!

Należy też zwrócić uwagę na praktykę klubów sportowych, które opierają przetwarzanie danych osobowych zawodników w całym zakresie na zgodzie zawodników. Jest to podejście nieprawidłowe z uwagi na fakt, że istnieją inne podstawy prawne przetwarzania danych osobowych zawodników. Zgoda ma mieć przede wszystkim charakter dobrowolny.

Co za tym idzie, jeżeli klub sportowy musi przetwarzać dane osobowe zawodników albo jest to niezbędne do zrealizowania umowy łączącej go z zawodnikiem, to trudno opierać takie przetwarzanie na podstawie zgody. Zgoda powinna mieć co do zasady charakter dodatkowy, być wykorzystywana w zakresie, w jakim nie ma innej podstawy prawnej do przetwarzania danych osobowych zawodników, a klub sportowy oceni, że przetwarzanie danych osobowych jest niezbędne do realizacji określonego celu przetwarzania.

9.1.2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

Zakres przetwarzanych przez klub sportowy danych osobowych dotyczących zawodników będzie wynikać z tego, w jakim celu będą one przetwarzane. Należy pamiętać, że dane powinny być zbierane tylko w takim zakresie, w jakim jest to niezbędne do realizacji danego celu przetwarzania.

UWAGA!

Klub sportowy powinien przeanalizować, w jakich celach będzie przetwarzać dane osobowe, i na tej podstawie ustalić, w jakim zakresie musi zebrać od zawodników dotyczące ich dane. Zawsze należy się kierować zasadą niezbędności (patrz: *Zasada minimalizacji danych*). Nie należy zbierać danych nadmiarowych, „na zapas”.

PRZYKŁADY

W zależności od celu przetwarzania mogą to być w szczególności następujące dane:

- ▶ imię i nazwisko;
- ▶ dane kontaktowe;
- ▶ adres zamieszkania;
- ▶ numer NIP (w przypadku zawodników prowadzących działalność gospodarczą);
- ▶ PESEL;
- ▶ data urodzenia;
- ▶ numer rachunku bankowego;
- ▶ informacje o dotychczasowej karierze sportowej oraz osiągniętych wynikach sportowych;
- ▶ rozmiar noszonych ubrań sportowych.

9.1.3. OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

W zależności od tego, w jakim celu dane osobowe są przetwarzane, należy ustalić okres ich przechowywania. Należy pamiętać, że przechowywanie danych osobowych jest dozwolone, dopóki istnieje cel i podstawa prawna do ich przetwarzania. Klub sportowy powinien zatem ustalić, jak długo konieczne jest przechowywanie danych osobowych zawodników, a po tym okresie trwale je usunąć.

W przypadku stosunku umownego łączącego zawodnika z klubem sportowym dane powinny być przechowywane przez okres trwania tego stosunku (umowy o pracę, umowy współpracy). Z kolei gdy klub przetwarza dane osobowe zawodników w celu realizacji obowiązków związanych z przepisami prawa, dane powinny być przechowywane przez okres wynikający z tych przepisów.

PRZYKŁADY

- realizacja obowiązków wynikających z przepisów podatkowych i dotyczących rachunkowości – co do zasady pięć lat od końca roku kalendarzowego, w którym powstał obowiązek podatkowy;
- realizacja obowiązków wynikających z prowadzenia dokumentacji pracowniczej – co do zasady 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygaś, chyba że odrębne przepisy przewidują dłuższy okres.

W przypadku przetwarzania danych osobowych w celu dochodzenia roszczeń lub obrony przed roszczeniami klub sportowy powinien przeanalizować, czy istnieją roszczenia, których zamierza dochodzić lub czy zawodnik dochodzi od niego określonego roszczenia¹⁷⁰. Takie przetwarzanie będzie uzasadnione do czasu zakończenia postępowania. Z kolei jeśli przetwarzanie danych opiera się na podstawie prawnie uzasadnionego interesu, maksymalnym okresem przechowywania będzie zawsze skuteczny sprzeciw wobec przetwarzania danych w danym celu złożony przez zawodnika (patrz: *Prawo do sprzeciwu wobec przetwarzania danych osobowych*).

W przypadku przetwarzania danych na podstawie zgody zawodnika, dane mogą być przetwarzane przez okres, w którym jest to niezbędne, jednak nie dłużej niż do czasu wycofania zgody przez zawodnika. Należy jednak pamiętać, że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano przed jej wycofaniem (patrz: *Zgoda osoby, której dane osobowe są przetwarzane*).

¹⁷⁰ Zob. np. wyrok Naczelnego Sądu Administracyjnego z dnia 8 stycznia 2025 r., sygn. akt II OSK 4868/21; Decyzja PUODO z dnia 3 września 2021 r., DKE.523.20.2021.

9.1.4. UDOSTĘPNIENIE DANYCH OSOBOWYCH ZAWODNIKÓW

Klub sportowy w ramach uczestnictwa w różnego rodzaju współzawodnictwie sportowym, organizacji imprez edukacyjnych czy promocyjnych może być zobowiązany do przekazania danych osobowych zawodników do zewnętrznych podmiotów, np. organizatora zawodów, podmiotu organizującego wyjazd na zawody, linii lotniczych, usługodawców hotelowych itd. W takim przypadku należy każdorazowo zastanowić się, czy i w jakim zakresie możliwe jest udostępnienie tym podmiotom danych osobowych zawodników. Jeżeli podanie określonych danych jest niezbędne w celu zapewnienia zakwaterowania, przelotu, udziału we współzawodnictwie, udostępnia się je na podstawie prawnie uzasadnionego interesu klubu sportowego, zawodnika lub organizatora zawodów (art. 6 ust. 1 lit. f RODO). W zakresie, w jakim przekazanie danych jest obowiązkiem wynikającym z przepisów prawa, np. przekazanie danych do Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego itp., podstawą do udostępnienia danych osobowych będzie konkretny przepis prawa (patrz: **Udostępnienie danych osobowych**). Może się to również odbywać na podstawie art. 6 ust. 1 lit. e RODO lub art. 6 ust. 1 lit. f RODO w zakresie przekazywania danych osobowych zawodników do polskiego związku sportowego celem realizacji określonych reguł organizacyjnych, sportowych oraz dyscyplinarnych, czyli wewnętrznych regulacji ustanowionych przez polski związek sportowy w zakresie, w jakim jest to niezbędne do realizacji celów wynikających z tych regulacji (patrz: **Przetwarzanie danych osobowych zawodników przez polskie związki sportowe**).

UWAGA!

W przypadku, gdy zewnętrzny podmiot potrzebuje danych osobowych zawodników, aby móc zrealizować swoje cele przetwarzania i samodzielnie decydować o tym, w jaki sposób je przetwarza, będzie dochodzić do udostępnienia danych osobowych, a nie powierzenia ich przetwarzania. W takim przypadku przed udostępnieniem danych należy zastanowić się:

- ▶ w jakim celu dane mają być przekazane;
- ▶ czy konieczne jest przekazanie danych osobowych zawodników, czy wystarczające będzie np. podanie jedynie ogólnej liczby osób;
- ▶ jakie dane muszą być przekazane;
- ▶ czy istnieje podstawa prawna do tego, żeby przekazać dane osobowe;
- ▶ w jaki sposób przekazać dane osobowe, żeby było to jak najbardziej bezpieczne (patrz: **Udostępnienie danych osobowych**).

9.2. PRZETWARZANIE DANYCH OSOBOWYCH ZAWODNIKÓW PRZEZ POLSKIE ZWIĄZKI SPORTOWE

9.2.1. PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH ZAWODNIKÓW

Polski związek sportowy jest powołany do organizowania i prowadzenia współzawodnictwa w danym sporcie. Posiada on wyłączne kompetencje przyznane mu w treści art. 13 ustawy o sporcie. Są to:

- ▶ organizowanie i prowadzenie współzawodnictwa sportowego o tytuł Mistrza Polski oraz o Puchar Polski w danym sporcie;
- ▶ ustanawianie i realizacja reguł sportowych, organizacyjnych i dyscyplinarnych we współzawodnictwie sportowym organizowanym przez związek, z wyjątkiem reguł dyscyplinarnych dotyczących dopingu w sporcie;
- ▶ powołanie kadry narodowej oraz przygotowanie jej do igrzysk olimpijskich, igrzysk paralimpijskich, igrzysk głuchych, mistrzostw świata lub mistrzostw Europy;
- ▶ reprezentowanie tego sportu w międzynarodowych organizacjach sportowych.

Mając powyższe na uwadze, w zakresie, w jakim polski związek sportowy będzie przetwarzał dane osobowe zawodników w ramach wyżej wymienionych celów, będzie odbywać się to na podstawie art. 6 ust. 1 lit. e RODO, a więc w zakresie niezbędnym do realizacji zadania w interesie publicznym lub sprawowania władzy publicznej powierzonej administratorowi. Przyjęcie tej podstawy prawnej uzasadnione jest tym, że w ramach aktu o randze ustawy zostały określone kompetencje wyłączne polskiego związku sportowego, a działalność tych organizacji podlega nadzorowi ze strony ministra właściwego do spraw kultury fizycznej (patrz: *Proces licencjonowania zawodników, trenerów i sędziów – podstawa prawna przetwarzania danych osobowych*).

PRZYKŁAD

Głównie będzie tu chodzić o regulacje dotyczące rejestracji zawodników, uprawnienia ich do współzawodnictwa w danym sporcie, przekazywania listy zawodników uprawnionych do gry w meczu lub występowania w zawodach, celów dokumentacyjnych dotyczących rzetelności i uczciwości zawodów sportowych, a także celów związanych z egzekwowaniem reguł dyscyplinarnych.

UWAGA!

Polskie związki sportowe, ustalając reguły organizacyjne, sportowe i dyscyplinarne, powinny mieć na uwadze przepisy o ochronie danych osobowych, w szczególności projektować określone procesy, z którymi wiązać się będzie przetwarzanie danych osobowych, w taki sposób, aby spełniały one wymogi wynikające z RODO oraz innych przepisów prawa regulujących kwestie przetwarzania danych osobowych. Udzielenie kompetencji wyłącznych na rzecz polskiego związku sportowego nie wyłącza obowiązku stosowania się do przepisów o ochronie danych osobowych.

Należy pamiętać, że uzyskanie statusu polskiego związku sportowego jest co do zasady uzależnione od przynależności do właściwej międzynarodowej federacji sportowej działającej w sporcie olimpijskim lub paraolimpijskim albo innej uznanej przez Międzynarodowy Komitet Olimpijski lub ujętej w wykazie wydanym na podstawie przepisów ustawy o sporcie. Jedynym wyjątkiem jest polski związek sportowy działający w sporcie osób niepełnosprawnych, który uzyskał zgodę ministra właściwego do spraw kultury fizycznej w tym zakresie. Powyższe wiązać się może z tym, że określone cele przetwarzania, powiązane z ustalonymi regułami, będą dyktowane przez międzynarodowe federacje sportowe, do których polski związek sportowy będzie zobowiązany się stosować. W takim przypadku możliwe jest rozważenie również powyżej opisanej podstawy prawnej lub przetwarzanie tych danych na podstawie prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit f RODO). W określonych przypadkach można rozważać zgodę jako podstawę przetwarzania danych osobowych, jeśli będą zachowane warunki jej stosowania (**patrz: Zgoda osoby, której dane osobowe są przetwarzane**). Regulacje międzynarodowych federacji sportowych nie mają bowiem rangi przepisów prawa powszechnie obowiązującego, krajowego ani międzynarodowego, dlatego nie jest możliwe przetwarzanie tych danych na podstawie obowiązku prawnego ciążącego na administratorze.

UWAGA!

Przy przekazywaniu danych do międzynarodowych federacji sportowych czy też w związku z międzynarodowymi rozgrywkami sportowymi szczególną uwagę należy zwrócić na to, skąd dany podmiot pochodzi, gdzie ma swoją siedzibę. Jeżeli mamy do czynienia z podmiotem spoza Europejskiego Obszaru Gospodarczego, konieczne jest zweryfikowanie, czy możliwy jest i na jakiej podstawie transfer tych danych (**patrz: Transfer danych poza Europejski Obszar Gospodarczy**).

Polski związek sportowy może również realizować inne niż wskazane powyżej cele przetwarzania. W przypadku prowadzenia działań marketingowych z udziałem zawodników będzie się to głównie odbywać na podstawie zgody zawodnika (art. 6 ust. 1 lit. a RODO). Określone działania mogą również odbywać się na podstawie prawnie uzasadnionego interesu prawnego polskiego związku sportowego, np. działania promujące daną dyscyplinę sportową czy też edukację sportową.

Należy również mieć na względzie szczególne uprawnienie polskiego związku sportowego dotyczące możliwości wykorzystania wizerunku zawodników należących do kadry narodowej w sytuacji określonej w art. 14 ustawy o sporcie (patrz: *Przetwarzanie danych osobowych w postaci wizerunku*).

W zakresie, w jakim przepisy prawa nakładają na polski związek sportowy obowiązek realizacji określonych zadań, przetwarzanie danych osobowych zawodników będzie odbywać się na podstawie art. 6 ust. 1 lit. c RODO, tj. niezbędności do realizacji obowiązku prawnego ciążącego na administratorze. Może to dotyczyć konieczności ubezpieczenia zawodnika od następstw nieszczęśliwych wypadków w związku z udziałem we współzawodnictwie sportowym w ramach kadry narodowej czy też dokonania rozliczeń finansowych z zawodnikiem w przypadku wypłaty premii za uzyskane miejsce w zawodach międzynarodowych.

9.2.2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

Polski związek sportowy powinien przetwarzać dane osobowe zawodników tylko w takim zakresie, jaki jest niezbędny do realizacji ustalonych celów przetwarzania. Mogą to być w szczególności takie dane, jak: imię i nazwisko, dane kontaktowe, adres zamieszkania, data urodzenia, numer rachunku bankowego, przynależność do klubu sportowego, informacje o dotychczasowej karierze oraz osiągniętych wynikach sportowych, rozmiar noszonych ubrań sportowych, warunki umowy zawartej z klubem sportowym, warunki umowy transferowej, informacje o popełnionych czynach dyscyplinarnych.

UWAGA!

Polski związek sportowy powinien każdorazowo przed pozyskaniem danych przeprowadzić analizę, w jakim zakresie dane osobowe zawodnika są mu niezbędne do realizacji danego celu przetwarzania i w oparciu o jaką podstawę prawną jest to możliwe. Nie należy zbierać danych osobowych „na zapas”.

9.2.3. OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

W zależności od tego, w jakim celu dane osobowe są przetwarzane, należy ustalić okres ich przechowywania. Należy pamiętać, że przechowywanie danych osobowych jest dozwolone, dopóki istnieje cel i podstawa prawna do ich przetwarzania. Polski związek sportowy powinien uwzględnić te kwestie, ustalając reguły obowiązujące w danym sporcie, w szczególności organizacyjne lub dyscyplinarne. Po upływie okresu przechowywania dane osobowe powinny zostać trwale usunięte.

W przypadku przetwarzania danych osobowych zawodników w celu organizacji współzawodnictwa sportowego zasadne jest przechowywanie danych osobowych zawodników przez okres, w którym zawodnik uczestniczy w takim współzawodnictwie sportowym. Przechowywanie danych może być również uzasadnione możliwością dochodzenia roszczeń lub obrony przed roszczeniami związanymi z prowadzoną przez polski związek sportowy działalnością.

Gdy polski związek sportowy przetwarza dane osobowe zawodników w celu realizacji obowiązków wynikających z przepisów prawa, dane te powinny być przechowywane przez okres wynikający z przepisów prawa.

Uzasadnione wydaje się również przechowywanie danych osobowych zawodnika związanych z uzyskiwanymi przez niego osiągnięciami i wynikami sportowymi w celach budowania historii danej dyscypliny sportowej czy prowadzenia kronik sportowych.

Należy pamiętać, że w przypadku przetwarzania danych osobowych na podstawie zgody zawodnika, może się to odbywać maksymalnie do czasu, kiedy zawodnik wycofa zgodę na przetwarzanie jego danych osobowych.

9.3. PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ ZWIĄZKI SPORTOWE

9.3.1. PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

W strukturach organizacyjnych poszczególnych dyscyplin sportowych oprócz klubów sportowych i polskich związków sportowych niekiedy funkcjonują również regionalne (wojewódzkie) związki sportowe. Podmiotom tym nie przysługuje jednak szczególny status i uprawnienia, tak jak w przypadku polskich związków sportowych.

Zgodnie z przepisami ustawy o sporcie kluby sportowe w liczbie co najmniej trzech mogą tworzyć związki sportowe, które działają w formie stowarzyszenia lub

związku stowarzyszeń. Co istotne, członkami związku sportowego są kluby sportowe, a nie zawodnicy. Co za tym idzie, nie jest możliwe oparcie przetwarzania danych osobowych zawodników przez związki sportowe na podstawie niezbędności do realizacji stosunku umownego. W związku z tym możliwe jest rozważenie podstawy w postaci prawnie uzasadnionego interesu związku sportowego (art. 6 ust. 1 lit. f RODO), ewentualnie w zakresie, w jakim przetwarzanie danych osobowych wynika z regulacji wewnętrznych ustanowionych przez polskie związki sportowe, można rozważać podstawę w postaci niezbędności do realizacji zadania w interesie publicznym (art. 6 ust. 1 lit. e RODO). Może to dotyczyć w szczególności uprawnienia zawodnika do gry czy też organizacji rozgrywek sportowych na niższych szczeblach, np. szczeblu regionalnym/wojewódzkim.

Określone cele przetwarzania mogą być również realizowane na podstawie prawnie uzasadnionego interesu związku sportowego, takiego jak dochodzenie roszczeń i obrona przed roszczeniami związanymi z działalnością związku sportowego czy też działania promujące rozgrywki sportowe.

W przypadku realizacji działań marketingowych wykorzystujących dane osobowe zawodników może w tym zakresie mieć również uzasadnienie podstawa prawna w postaci zgody zawodnika (art. 6 ust. 1 lit. a RODO).

W przypadku obowiązków wynikających z przepisów prawa, np. rozliczeń finansowych związanych z udziałem zawodnika w zawodach, przetwarzanie danych będzie się odbywać na podstawie obowiązku prawnego (art. 6 ust. 1 lit. c RODO).

9.3.2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

Związek sportowy powinien przetwarzać dane osobowe zawodników tylko w takim zakresie, jaki jest niezbędny do realizacji ustalonych celów przetwarzania. Mogą to być w szczególności takie dane, jak: imię i nazwisko, dane kontaktowe, adres zamieszkania, data urodzenia, numer rachunku bankowego, przynależność do klubu sportowego, informacje o dotychczasowej karierze sportowej oraz osiągniętych wynikach sportowych, rozmiar noszonych ubrań sportowych, warunki umowy zawartej z klubem sportowym, informacje o popełnionych czynach dyscyplinarnych.

UWAGA!

Związek sportowy powinien każdorazowo przed pozyskaniem danych przeprowadzić analizę, w jakim zakresie dane osobowe zawodnika są mu niezbędne do realizacji danego celu przetwarzania i w oparciu o jaką podstawę prawną jest to możliwe. Nie należy zbierać danych osobowych „na zapas”.

9.3.3. OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

W zależności od tego, w jakim celu dane osobowe są przetwarzane, należy ustalić okres ich przechowywania. Należy pamiętać, że przechowywanie danych osobowych jest dozwolone, dopóki istnieje cel i podstawa prawna do ich przetwarzania. Po upływie okresu przechowywania dane osobowe powinny zostać trwale usunięte.

W przypadku przetwarzania danych osobowych zawodników w celu organizacji współzawodnictwa sportowego zasadne jest przechowywanie danych osobowych zawodników przez okres, w którym uczestniczą oni w takim współzawodnictwie sportowym. Ewentualnie przechowywanie danych może być również uzasadnione możliwością dochodzenia roszczeń lub obrony przed roszczeniami związanymi z prowadzoną przez związek sportowy działalnością.

Gdy związek sportowy przetwarza dane osobowe zawodników w celu realizacji obowiązków wynikających z przepisów prawa, dane te powinny być przechowywane przez okres wynikający z przepisów prawa.

Uzasadnione wydaje się również przechowywanie danych osobowych zawodnika związanych z uzyskiwanymi przez niego osiągnięciami i wynikami sportowymi w celach budowania historii danej dyscypliny sportowej czy prowadzenia kronik sportowych.

Należy pamiętać, że w przypadku przetwarzania danych osobowych na podstawie zgody zawodnika, może się to odbywać maksymalnie do czasu, kiedy zawodnik wycofa zgodę na przetwarzanie jego danych osobowych.

9.4. PRZEKAZYWANIE DANYCH OSOBOWYCH NA RÓŻNYCH SZCZEBŁACH STRUKTUR ORGANIZACYJNYCH (KLUB SPORTOWY – ZWIĄZEK SPORTOWY – POLSKI ZWIĄZEK SPORTOWY – MIĘDZYNARODOWA FEDERACJA SPORTOWA)

W sporcie często dochodzi do przekazywania danych osobowych w ramach struktur organizacyjnych danej dyscypliny sportowej. W takiej sytuacji istotne jest, kto ustala cele i sposoby przetwarzania danych osobowych:

- ▶ jeżeli podmiotem decydującym o celach i sposobach przetwarzania będzie zarówno polski związek sportowy, jak i działające w jego ramach związki sportowe, to możliwe jest przyjęcie w tym zakresie współadministrowania danymi osobowymi, jeśli faktycznie procesy te są wspólnie przez nich ustalane (patrz: Współadministrator);

- ▶ w przypadku gdy każdy z podmiotów ma swoje cele i sposoby przetwarzania, dochodzić będzie do udostępnienia danych osobowych, co wiąże się z koniecznością zapewnienia odpowiedniej podstawy prawnej do udostępnienia danych osobowych (patrz: Udostępnienie danych osobowych);
- ▶ jeżeli natomiast określony podmiot, np. związek sportowy, przetwarza dane w imieniu i na rzecz celów określonych i realizowanych przez polski związek sportowy, to może być wtedy podmiotem przetwarzającym, co będzie powodować konieczność zawarcia umowy powierzenia przetwarzania danych osobowych (patrz: Podmiot przetwarzający).

10. SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH SPORTOWCÓW MONITORING ZAWODNIKÓW NOWOCZESNE TECHNOLOGIE

ART. 9 RODO. PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH¹⁷¹

„Zabrania się przetwarzania danych osobowych szczególnej kategorii, takich jak dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby”.

Dane osobowe szczególnych kategorii odnoszące się do sportowców uprawiających określone dyscypliny stanowią szeroki zakres informacji, nie tylko skatalogowanych w art. 9 RODO, ale także odnoszących się do identyfikacji i analityki sportowców za pomocą systemów biometrycznych. Identyfikacja biometryczna odpowiada nie tylko na pytanie, „kim jestem”, ale także „jaki jestem”. Rozwijające się technologie i narzędzia z wykorzystaniem technik biometrycznych mogą już skutecznie monitorować zawodników w oparciu o unikalne dane osobowe i w takim znaczeniu należałoby rozważać przetwarzanie danych sportowców. Odnajdujemy tu takie informacje, jak dane dotyczące zdrowia, dane fizjologiczne, wydajnościowe, płeć, informacje dźwiękowe, wizualne lub elektroniczne, w tym głos, zdjęcia, skany twarzy i obrazy sportowców, analizy wyciągnięte z danych osobowych zgromadzonych w celu utworzenia profilu (patrz: Dane biometryczne, Dane dotyczące zdrowia).

¹⁷¹ P. Fajgielski, *Ogólne rozporządzenie...*, *op.cit.*, art. 9.

10.1. WARUNKI LEGALNEGO PRZETWARZANIA DANYCH DOTYCZĄCYCH ZDROWIA SPORTOWCA

Zgodnie z przepisami przetwarzanie danych osobowych szczególnych kategorii co do zasady jest niedopuszczalne, jednak istnieją wyjątki legalizujące przetwarzanie tych danych. I tak, przetwarzanie danych o stanie zdrowia jest dopuszczalne m.in. w sytuacji, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

PRZYKŁAD

Przepisami zezwalającymi na przetwarzanie danych szczególnych kategorii są przepisy, na podstawie których sportowiec musi przedstawić zaświadczenie zawierające orzeczenie lekarskie o braku przeciwwskazań do uprawiania określonej dyscypliny sportu¹⁷². Biorąc powyższe pod uwagę, należy stwierdzić, iż przepisy wprost zezwalają klubowi lub związkowi sportowemu na przetwarzanie danych osobowych zawartych w zaświadczeniu zawierającym orzeczenie lekarskie o braku przeciwwskazań do uprawiania sportu, w związku z czym takie działanie jest legalne z punktu widzenia przepisów o ochronie danych osobowych.

10.2. WARUNKI LEGALNEGO PRZETWARZANIA DANYCH BIOMETRYCZNYCH SPORTOWCA

Przetwarzanie danych biometrycznych może być oparte na jednej z przesłanek opisanych w art. 9 ust. 2 RODO.

Najczęściej wykorzystywanymi przesłankami legalizującymi przetwarzanie danych biometrycznych będzie zgoda podmiotu danych (art. 9 ust. 2 lit. a RODO) lub wypełnienie obowiązków i wykonywanie szczególnych praw przez administratora lub podmiot danych w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, pod warunkiem że jest to dozwolone prawem unijnym, prawem państwa członkowskiego lub porozumieniem zbiorowym zawartym zgodnie z przepisami krajowymi (art. 9 ust. 2 lit. b RODO). Z perspektywy administratora najlepiej

¹⁷² Ustawa z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2024 r. poz. 1488), art. 37 (orzeczenia lekarskie dla zawodników).

jest wtedy, kiedy możliwość przetwarzania danych biometrycznych wynika wprost z przepisów. Istnieje wówczas wyraźna podstawa prawna, na której administrator może oprzeć przetwarzanie szczególnej kategorii danych osobowych. W przypadku sportowców podstawę tę często odnajdujemy w art. 9 ust. 1 lit a lub w art. 9 ust. 2 lit. a, gdzie zgoda jest niezbędna do prawidłowej realizacji umowy z zawodnikiem. W tym przypadku może mieć zastosowanie art. 7 ust. 4 RODO, który wskazuje, że oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy m.in. od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy. A więc jeżeli w ramach realizacji umowy konieczne jest przetwarzanie danych szczególnej kategorii i nie ma innej podstawy prawnej do przetwarzania danych, to ta zgoda może mieć zastosowanie jako konieczna do realizacji umowy/kontraktu z zawodnikiem. Podstawa prawna będzie zależała od celów, w których dane te są gromadzone i przetwarzane dla efektywniejszego uprawiania sportu i osiągania wyników przez osobę, której dane dotyczą.

10.3. KOMU MOŻNA UDOSTĘPNIAC DANE OSOBOWE ORAZ GDZIE I JAK NALEŻY JE PRZECHOWYWAĆ?

ART. 32 RODO. BEZPIECZEŃSTWO PRZETWARZANIA¹⁷³

„1. Uwzględniając stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym m.in. w stosownym przypadku:

- a) pseudonimizację i szyfrowanie danych osobowych;
- b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania”.

¹⁷³ P. Fajgielski, *Ogólne rozporządzenie...*, op.cit., art. 32.

Dane osobowe szczególnych kategorii sportowców powinny zostać odpowiednio zabezpieczone i przechowywane w miejscach, do których dostęp posiadają jedynie upoważnione przez administratora osoby (pracownicy/współpracownicy klubu/związku). Zgodnie z art. 32 RODO administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku. Każdy podmiot sportowy będzie miał inne możliwości. Udostępnianie takich danych innym podmiotom dozwolone jest tylko w sytuacjach, w których umożliwiają to przepisy prawa, w tym wewnątrz powiązanych ze sobą podmiotów sportowych lub medycznych, określonych uzasadnionym celem. W pewnych sytuacjach podmioty sportowe mogą być zobowiązane do ujawnienia takich danych osobowych na żądanie stosownych organów.

Informacje o sportowcach należy przechowywać przez okres, który uzasadnia cel ich przetwarzania, a czasami przez dłuższy okres, jeżeli jest to konieczne ze względów prawnych, operacyjnych lub z innych uzasadnionych powodów. Okres ten określany jest zgodnie z wymogami wynikającymi z przepisów o ochronie danych osobowych.

10.4. PODANIE DANYCH OSOBOWYCH SPORTOWCA NA DOPINGU DO INFORMACJI PUBLICZNEJ A RODO

Organ antydopingowy, który publikuje w internecie dane osobowe sportowca na doping, nie narusza RODO. Publikacja danych osobowych takiego sportowca może mieć bowiem cel prewencyjny. Sprawa ta nie została jeszcze rozstrzygnięta przez Trybunał Sprawiedliwości UE, niemniej jednak wypowiedziała się o niej rzecznik generalna TSUE¹⁷⁴.

UWAGA!

Sprawa, która będzie rozpatrywana przez Trybunał Sprawiedliwości UE, dotyczy austriackiego sportowca, którego uznano za winnego naruszenia krajowych przepisów antydopingowych. Austriacka komisja antydopingowa (ÖADR) cofnęła nagrody przyznane temu sportowcowi, unieważniła jego wyniki i zakazała mu udziału we wszelkich zawodach sportowych przez cztery lata. Niezależna austriacka organizacja antydopingowa (NADA) opublikowała w internecie imię i nazwisko sportowca, a także informacje o naruszeniach przepisów antydopingowych i okresie zawieszenia.

¹⁷⁴ Opinia rzecznik generalnej w sprawie C-115/22 | NADA i in. Antydoping i ochrona danych.

Sportowiec zażądał rewizji orzeczenia przez Niezależną Komisję Arbitrażową (Unabhängige Schiedskommission, USK). Organ ten zwrócił się z kolei z pytaniem prejudycjalnym do Trybunału Sprawiedliwości UE. Dotyczyło ono kwestii, czy publikacja w internecie danych osobowych sportowca na doping jest zgodna z RODO.

Publikacja danych osobowych sportowca na doping w celach prewencyjnych

Przed wydaniem wyroku rzecznik generalna TSUE przedstawiła w tej kwestii swoje stanowisko. Otóż w jej ocenie publikacja danych osobowych sportowca na doping jest dopuszczalna w świetle RODO. Przede wszystkim jej zdaniem RODO nie ma zastosowania do takiej publikacji. Alternatywnie rzecznik wskazała, że takie przetwarzanie danych osobowych może być uzasadnione celami prewencyjnymi. Chodzi mianowicie o odstraszenie młodych sportowców przed stosowaniem doping. Ważne jest też informowanie opinii publicznej o takich nagannych działaniach. Z tego względu publikacja może być uzasadniona interesem osób trzecich. Dodatkowo rzecznik zwróciła uwagę na fakt, że publikacja danych sportowca offline byłaby w obecnych realiach niewystarczająca. Z kolei udostępnienie ich w internecie spełni swój cel, jakim jest poinformowanie opinii publicznej o stosowaniu przez niego doping.

10.5. MONITORING ZAWODNIKÓW. NOWOCZESNE TECHNOLOGIE

W zakresie danych osobowych szczególnych kategorii sportowców na przeanalizowanie zasługuje aspekt danych biometrycznych w kontekście nowych technologii.

ART. 4 PKT. 14 RODO

„Dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne”¹⁷⁵.

Zakres definicyjny pojęcia danych biometrycznych jest szeroki, gdyż obejmuje dane o różnym charakterze. Przykładowo informacje biometryczne można pozyskać z analizy linii papilarnych, siatkówki oka, kształtu twarzy lub ucha, głosu, wzoru DNA, pisma,

¹⁷⁵ P. Fajgielski, *Ogólne rozporządzenie...*, *op.cit.*, art. 4 pkt. 14.

sposobu zachowania itp. Nie oznacza to jednak, że każde utrwalenie głosu lub wizerunku twarzy będzie stanowiło przetwarzanie danych biometrycznych. Niezbędne jest zastosowanie wspomnianych w przepisie specjalnych technik przetwarzania, dzięki którym można jednoznacznie zidentyfikować konkretną osobę. W praktyce sprowadza się to do pobrania od konkretnej osoby danej zawierającej informację biometryczną (np. odcisku palca, próbki pisma), a następnie poddania tej danej przetwarzaniu za pomocą odpowiedniej techniki biometrycznej. W ten sposób powstaje wzorzec, który jest zapisywany w postaci cyfrowej i przechowywany w bazie danych lub bezpośrednio na urządzeniu umożliwiającym odczyt danych biometrycznych. Wzorzec ten jest później wykorzystywany w procesach identyfikacyjnych – jeśli poddana analizie dana zawierająca cechy biometryczne jest zgodna z daną utrwaloną za pomocą wzorca, dochodzi do identyfikacji lub potwierdzenia tożsamości osoby fizycznej¹⁷⁶.

Dane biometryczne nie wymagają ani zapamiętywania, ani aktualizacji, są trwałe, niezienne, niezależnie od wieku czy zmian fizycznych oraz nie podlegają modyfikacjom, tak jak inne dane osobowe, mają też unikalny charakter, ponieważ pozwalają na jednoznaczne rozróżnienie osób. Ich przetwarzanie, oprócz wspomnianych zalet i udogodnień, może jednak także powodować długotrwałe, negatywne skutki dla podmiotu danych, wynikające właśnie z ich unikalnego i trwałego charakteru.

Rozwój nowoczesnych technologii sprawia, że na co dzień w sportowej pracy/treningach coraz częściej korzysta się z narzędzi wyposażonych w funkcje biometrycznego przetwarzania danych. Nowe technologie są wykorzystywane do udoskonalania treningów i opracowywania zoptymalizowanych planów działań, a także wykorzystywane przez zawodników i trenerów do monitorowania postępów w osiągnięciu celów i rozwoju poprzez analizę danych.

Dzisiejsze technologie oferują wiele narzędzi do monitorowania wysiłku i aktywności fizycznej sportowców. Opaski, koszulki śledzące ciśnienie i tętno, oddychanie, kroki i spalane kalorie, chipy, smartfony i inne urządzenia pozwalają na dokładne pomiary wielu parametrów, takich jak np. dystans pokonany podczas treningu. Dane te mogą pomóc sportowcom chcącym monitorować swój wysiłek w ocenie efektywności ćwiczeń i dostosowaniu planu treningowego, by poprawić wyniki i indywidualizować obciążenia treningowe.

Do technologii sportowych, dzięki którym możliwe jest skuteczne monitorowanie zawodników z wykorzystaniem ich danych biometrycznych, można zaliczyć m.in. wagi Bluetooth lub monitory pracy serca, które dają podstawowe informacje o pojedynczych parametrach wysiłkowych, platformy dynamometryczne, fotokomórki, systemy do oceny biomechanicznej, analizatory składu ciała czy gazów oddechowych, zapewniające dane o wielu parametrach, które w połączeniu ze sobą dają kompleksowy obraz osoby i pomagają ocenić jej mocne i słabe strony.

¹⁷⁶ A. Michałowicz, *Przetwarzanie danych biometrycznych przez przedsiębiorców. Jak zrobić to legalnie?*, <https://www.parp.gov.pl/component/content/article/73676> [dostęp: 20.08.2025].

UWAGA!

- ▶ **analizowane dane zawodników:** tętno, poziom nawodnienia, wyniki testów wydolnościowych, skuteczność.
- ▶ **źródła:** monitory fitness, czujniki GPS, systemy telemetryczne, kamery, drony, czujniki na ubraniach sportowców;
- ▶ **zastosowanie:** optymalizacja treningów, zapobieganie kontuzjom, personalizacja planów regeneracji, identyfikacja słabych punktów sportowca.

Szczegółowy wgląd w stan zdrowia, samopoczucie i ogólne wyniki sportowca rozumiane tutaj jako dane osobowe szczególnych kategorii możliwe są dzięki rozszerzonym rozwiązaniom do monitorowania, obejmującym dane medyczne i treningowe, które zapewniają trenerom, szkoleniowcom i personelowi sportowemu rozbudowany zestaw narzędzi do przygotowywania sportowców i zespołów. System ten pomaga unikać kontuzji i zwiększać wyniki na treningach, co przekłada się na lepsze rezultaty.

UWAGA!

Przy wdrażaniu rozwiązań opartych na nowoczesnych technologiach konieczne jest przeanalizowanie ich działania pod kątem przepisów o ochronie danych osobowych, w tym odpowiednie zaprojektowanie procesów przetwarzania danych, uwzględniające zakres, cel i sposób oraz systematyczne analizowanie ryzyk z tym związanych, a także wprowadzenie odpowiednich zabezpieczeń fizycznych, organizacyjnych, technicznych i informatycznych mających na celu ochronę praw i wolności sportowców.

Aktualnie coraz większa liczba podmiotów sportowych przetwarza dane osobowe w formie elektronicznej, zatem ryzyko ataków i naruszeń jest coraz większe. Ochrona danych osobowych i ich bezpieczeństwo stają się najważniejszymi wyzwaniami dla branży sportowej. Wprowadzane w sporcie nowoczesne technologie, takie jak czujniki, wideoanaliza czy systemy do badania stanu zdrowia sportowców, również wymagają zabezpieczenia adekwatnego do ryzyka utraty ochrony danych. Wprowadzanie monitoringu, narzędzi treningowych czy analizy wideo może naruszać prywatność zawodników, zwłaszcza jeśli dane te trafią do nieuprawnionych podmiotów. Odpowiednia kontrola i ochrona tych danych jest ważna, aby sportowcy mogli czuć się bezpiecznie i swobodnie korzystać z innowacji technologicznych z zachowaniem odpowiednich standardów bezpieczeństwa, na co powinny w szczególności zwrócić uwagę organizatorzy sportu w Polsce.



www.insp.pl

  **Instytut Sportu - PIB**