

Ochrona danych osobowych studentów na gruncie RODO.

Zagadnienia wybrane z działalności uczelni.

Michał Szczęsny



O autorze



Michał Szczęsny

W 2024 r. ukończył studia prawnicze na Uniwersytecie Śląskim w Katowicach. Obecnie jest ekspertem do spraw studenckich Polskiej Komisji Akredytacyjnej oraz członkiem Rady Wykonawczej Parlamentu Studentów Rzeczypospolitej Polskiej, gdzie odpowiada za opiniowanie projektów aktów prawnych dotyczących szkolnictwa wyższego oraz wsparcie samorządów studenckich w kwestiach prawnych. Na co dzień zajmuje się problematyką prawa szkolnictwa wyższego oraz praw studentów. Wielokrotnie prowadził szkolenia dla studentów z zakresu ich praw i obowiązków.

Spis treści

1. Wprowadzenie	5
1.1. Znaczenie ochrony danych osobowych studentów	5
1.2. Cel i zakres opracowania	5
1.3. Podstawowe akty prawne	5
2. Podstawowe pojęcia z zakresu ochrony danych osobowych	6
2.1. Dane osobowe	6
2.2. Szczególne kategorie danych osobowych	6
2.3. Przetwarzanie danych osobowych	7
2.4. Administrator danych osobowych	8
2.5. Podmiot przetwarzający i odbiorca danych	8
2.6. Inspektor ochrony danych	9
2.7. Naruszenie ochrony danych osobowych	9
3. Zakres stosowania RODO w działalności uczelni	10
3.1. Przetwarzanie danych w ramach działalności instytucjonalnej uczelni	10
3.2. Wyłączenie dotyczące czynności o charakterze osobistym lub domowym	10
3.3. Ustalenie roli podmiotu przetwarzającego dane	10
3.4. Uczelnia jako administrator danych osobowych	11
4. Zasady przetwarzania danych osobowych studentów	12
4.1. Zasada zgodności z prawem, rzetelności i przejrzystości	12
4.2. Zasada ograniczenia celu	12
4.3. Zasada minimalizacji danych	13
4.4. Zasada prawidłowości danych	13
4.5. Zasada ograniczenia przechowywania	13
4.6. Zasada integralności i poufności	13
4.7. Zasada rozliczalności	13
5. Podstawy prawne przetwarzania danych osobowych studentów	14
5.1. Obowiązek prawny ciążyący na uczelni	14
5.2. Wykonywanie zadania realizowanego w interesie publicznym	15
5.3. Zgoda studenta	15
5.4. Wykonanie umowy	15
5.5. Prawnie uzasadniony interes administratora	16
5.6. Podstawy przetwarzania szczególnych kategorii danych	16
5.7. Obowiązek prawny a uprawnienie uczelni	17
6. Obowiązki uczelni jako administratora danych osobowych	17
6.1. Obowiązek informacyjny	17
6.2. Zapewnienie bezpieczeństwa danych	18

6.3. Nadawanie upoważnień do przetwarzania danych	18
6.4. Prowadzenie rejestru czynności przetwarzania	18
6.5. Ocena ryzyka i ocena skutków dla ochrony danych	19
6.6. Powierzenie przetwarzania danych	19
6.7. Okresy przechowywania i usuwanie danych	19
6.8. Współpraca z inspektorem ochrony danych	20
7. Prawa studenta jako osoby, której dane dotyczą	20
7.1. Prawo dostępu do danych	20
7.2. Prawo do sprostowania danych	21
7.3. Prawo do usunięcia danych	21
7.4. Prawo do ograniczenia przetwarzania	21
7.5. Prawo do przenoszenia danych	22
7.6. Prawo do sprzeciwu	22
7.7. Prawo do wniesienia skargi do Prezesa UODO	22
8. Szczególne obszary przetwarzania danych osobowych studentów	23
8.1. Rekrutacja na studia i publikowanie wyników	23
8.2. Dokumentacja przebiegu studiów	23
8.3. Oceny, egzaminy i zaliczenia	24
8.4. Stypendia i inne świadczenia dla studentów	24
8.5. Dane dotyczące zdrowia i niepełnosprawności	24
8.6. Praktyki zawodowe	24
8.7. Wymiana akademicka i mobilność międzynarodowa	25
8.8. Monitoring wizyjny	26
8.9. Komunikacja elektroniczna i poczta e-mail	26
8.10. Systemy informatyczne i platformy e-learningowe	26
8.11. Systemy antyplagiatowe i repozytoria prac dyplomowych	27
8.12. Nagrywanie zajęć i egzaminów zdalnych	27
8.13. Działalność promocyjna uczelni	27
9. Naruszenia ochrony danych osobowych w działalności uczelni	28
9.1. Pojęcie naruszenia ochrony danych osobowych	28
9.2. Ocena ryzyka dla praw i wolności studentów	28
9.3. Zgłoszenie naruszenia Prezesowi UODO	28
9.4. Zawiadomienie osób, których dane dotyczą	29
9.5. Dokumentowanie naruszeń	29
9.6. Przykłady najczęstszych naruszeń w uczelniach	29
9.7. Sprawa Uniwersytetu w G.	30
9.8. Sprawa Y. w B.	31
10. Ochrona danych osobowych w badaniach naukowych i wypowiedzi akademickiej	31

10.1. Pojęcie wypowiedzi akademickiej	32
10.2. Zakres ograniczeń obowiązków wynikających z RODO	32
10.3. Przetwarzanie danych do celów badań naukowych i prac rozwojowych	33
10.4. Szczególne kategorie danych w badaniach naukowych	33
10.5. Ograniczenia praw osób, których dane dotyczą	34
10.6. Pseudonimizacja i anonimizacja danych	34
10.7. Student i doktorant jako osoba prowadząca badania	35
10.8. Wykorzystywanie prac i wypowiedzi studentów	35
11. Samorząd studencki a ochrona danych osobowych	35
11.1. Status prawny samorządu studenckiego	35
11.2. Samorząd jako część uczelni	36
11.3. Samorząd jako potencjalny administrator danych	37
11.4. Współadministrowanie przez uczelnię i samorząd	38
11.5. Upoważnienia do przetwarzania danych	39
11.6. Organizacja wydarzeń i imprez studenckich	39
11.7. Listy mailingowe, formularze i zapisy na wydarzenia	39
11.8. Przetwarzanie danych przez komisje stypendialne i dyscyplinarne	39
11.9. Obowiązki informacyjne i bezpieczeństwo danych	40
12. Zakończenie	40
13. Bibliografia	41
14. Wykaz aktów prawnych	41
15. Wykaz orzecznictwa i decyzji organów nadzorczych	42

1. Wprowadzenie

1.1. Znaczenie ochrony danych osobowych studentów

Ochrona danych osobowych studentów ma istotne znaczenie praktyczne, ponieważ uczelnie realizując zadania związane z kształceniem, rekrutacją, prowadzeniem dokumentacji przebiegu studiów, przyznawaniem świadczeń pomocy materialnej przetwarzają szeroki zakres informacji dotyczących osób studiujących. Dane te mogą obejmować zarówno podstawowe dane identyfikacyjne i kontaktowe, jak również dane dotyczące sytuacji materialnej, zdrowotnej czy rodzinnej studenta, jeżeli ich przetwarzanie wynika z obowiązujących przepisów prawa a nieprawidłowości w tym zakresie mogą prowadzić do realnego naruszenia praw i wolności osób, których dane dotyczą.

1.2. Cel i zakres opracowania

Niniejsze opracowanie poświęcone jest problematyce ochrony danych osobowych studentów w działalności uczelni. Jego celem jest przedstawienie podstawowych pojęć, zasad, podstaw prawnych oraz obowiązków spoczywających na uczelni jako administratorze danych osobowych, a także praw przysługujących studentom jako osobom, których dane dotyczą. Opracowanie obejmuje zarówno ogólne zagadnienia wynikające z RODO, jak i zagadnienia szczególne dla sektora szkolnictwa wyższego, w tym przetwarzanie danych do celów badań naukowych i wypowiedzi akademickiej oraz rolę samorządu studenckiego. Analizę uzupełniają przykłady praktyczne oraz omówienie wybranych decyzji Prezesa Urzędu Ochrony Danych Osobowych i orzeczeń sądów administracyjnych dotyczących uczelni.

1.3. Podstawowe akty prawne

Podstawowym aktem prawnym regulującym zasady ochrony danych osobowych na terenie państw należących do Unii Europejskiej 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/WE¹. RODO posiada rangę rozporządzenia, dlatego jego przepisy stosowane są bezpośrednio i stanowią część polskiego porządku prawnego. Rozporządzenie to uzupełniają przepisy krajowe, w szczególności ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych², określająca m.in.

¹ 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, s. 1, ze zm.), dalej jako: „RODO”.

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2019 r. poz. 1781, ze zm.), dalej jako: „u.o.d.o.” lub „ustawa o ochronie danych osobowych”.

zadania i kompetencje Prezesa Urzędu Ochrony Danych Osobowych oraz tryb postępowania w sprawach naruszeń, a także ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce³, która określa zasady organizacji i funkcjonowania systemu szkolnictwa wyższego i nauki, w tym uczelni, regulując m.in. zasady rekrutacji, przyznawania świadczeń pomocy materialnej, prowadzenia działalności naukowej oraz funkcjonowania samorządu studenckiego, a w wielu przypadkach stanowi podstawę prawną przetwarzania danych osobowych studentów lub doprecyzowuje zasady tego przetwarzania.

2. Podstawowe pojęcia z zakresu ochrony danych osobowych

2.1. Dane osobowe

Zgodnie z art. 4 pkt 1 RODO „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. Za daną osobową będzie mogła zostać uznana każda informacja, jeżeli dzięki niej uda się zidentyfikować daną osobę. Mogą to być zatem np. imię i nazwisko, PESEL, numer dowodu osobistego, numer telefonu komórkowego czy adres e-mail.

W przypadku studenta będą to przede wszystkim imię i nazwisko, PESEL, numer albumu, data urodzenia, adres, e-mail, numer telefonu, zdjęcie, numer legitymacji, numer konta, identyfikatory w systemach uczelni, login, adres IP, a także wszelkie dane przypisane do tej osoby w toku studiów. Jeżeli na podstawie danych informacji można ustalić, o którego studenta chodzi, mamy do czynienia z danymi osobowymi. Wobec powyższego, za dane osobowe mogą zostać uznane informacje o przebiegu studiów, np. kierunek, rok, grupa zajęciowa, oceny, wyniki egzaminów, obecność, decyzje stypendialne, informacje o skreśleniu z listy studentów czy informacje o niepełnosprawności zgłoszonej dla potrzeb organizacji toku studiów.

2.2. Szczególne kategorie danych osobowych

³ Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2024 r. poz. 1571 ze zm.), dalej: „PSWiN”.

Wśród danych osobowych studentów mogą znajdować się również dane należące do szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO. Mogą to być w szczególności dane dotyczące zdrowia, w tym informacje o niepełnosprawności, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, a w wyjątkowych przypadkach także dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe oraz dane dotyczące życia seksualnego lub orientacji seksualnej osoby fizycznej. Takie dane podlegają dalej idącej ochronie na podstawie art. 9 RODO. Co do zasady ich przetwarzanie jest zabronione, jednak ust. 2 wskazuje przypadki, kiedy przetwarzanie takich danych będzie możliwe. Dane takie mogą być przetwarzane, jeżeli osoba, której dotyczą, wyraziła wyraźną zgodę. W kontekście akademickim taka zgoda może się pojawić przy pozyskiwaniu informacji w trakcie tworzenia akt osobowych w organizacjach studenckich, jeśli zachodziłaby konieczność przetwarzania konkretnych danych. Po drugie, dane takie będą przetwarzane, jeśli przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw administratora lub osoby, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (art. 9 ust. 2 lit. b RODO). Podstawa ta znajduje zastosowanie wówczas, gdy obowiązek przetwarzania danych wynika z przepisów prawa powszechnie obowiązującego - przykładowo PSWiN w zakresie obsługi wniosków o przyznanie stypendium specjalnego dla osób z niepełnosprawnością. Wobec powyższego przedstawienie takich danych będzie konieczne dla realizacji normy wynikającej z PSWiN. Po trzecie, przetwarzanie niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy (art. 9 ust. 2 lit. h RODO) - przepis ten jest istotny w przypadku uczelni medycznych oraz innych podmiotów realizujących programy kształcenia wymagające odbywania praktyk w placówkach opieki zdrowotnej, gdzie przetwarzanie danych o stanie zdrowia studenta może być konieczne zarówno z perspektywy ochrony samego studenta, jak i bezpieczeństwa pacjentów.

2.3. Przetwarzanie danych osobowych

Zgodnie z art. 4 pkt 2 RODO przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Wyliczenie operacji składających się na przetwarzanie ma charakter przykładowy, na co wskazuje użyty w treści definicji zwrot „takich jak”, wobec czego katalog jest otwarty, a każda czynność faktyczna lub prawna wykonywana na danych

osobowych może zostać uznana za przetwarzanie, jeżeli tylko wykazuje cechy zbliżone do operacji tam wskazanych.

W środowisku akademickim pojęcie przetwarzania nabiera szczególnej rozległości ze względu na wielość procesów, w których dane studenta są wykorzystywane. Już samo złożenie przez kandydata dokumentów rekrutacyjnych stanowi przetwarzanie, obejmuje ono bowiem co najmniej zbieranie i utrwalanie danych. Przez cały okres kształcenia uczelnia przetwarza dane osobowe studentów w związku z realizacją licznych zadań dydaktycznych, administracyjnych i organizacyjnych, m.in. w ramach obsługi toku studiów przez dziekanat, ewidencjonowania wyników egzaminów, wydawania zaświadczeń, komunikacji mailowej z nauczycielami akademickimi, prowadzenia dokumentacji dotyczącej świadczeń dla studentów oraz rejestrowania obecności na zajęciach. Każda z tych czynności, niezależnie od tego, czy odbywa się w systemie informatycznym, czy w dokumentacji papierowej, mieści się w zakresie definicji z art. 4 pkt 2 RODO i rodzi po stronie uczelni obowiązek zapewnienia zgodności przetwarzania z przepisami RODO. Błędne założenie, że określona czynność nie stanowi przetwarzania np. przeglądanie danych bez ich kopiowania lub zmieniania może prowadzić do naruszenia obowiązków wynikających z RODO. Uchybienie takiego rodzaju może stanowić podstawę do wszczęcia postępowania przez Prezesa Urzędu Ochrony Danych Osobowych i nałożenia administracyjnej kary pieniężnej na podstawie art. 83 RODO.

2.4. Administrator danych osobowych

Pojęcie administratora jest kluczowe dla zrozumienia systemu ochrony danych osobowych ustanowionego przez RODO, ponieważ to właśnie na administratora RODO nakłada większość obowiązków związanych z zapewnieniem zgodności przetwarzania danych z prawem, a jego prawidłowa identyfikacja decyduje o tym, na kim spoczywa odpowiedzialność za ewentualne naruszenia. Administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie albo wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Innymi słowy, administratorem jest ten podmiot, który decyduje, po co i w jaki sposób dane osobowe są przetwarzane. W przypadku przetwarzania danych w ramach działalności uczelni funkcję administratora pełni co do zasady sama uczelnia jako osoba prawna, działająca przez swoje organy, a nie konkretny dziekanat, wydział, nauczyciel akademicki czy pracownik administracji.

2.5. Podmiot przetwarzający i odbiorca danych

Poza administratorem w ochronie danych osobowych występują również inne podmioty, do których zaliczamy: podmiot przetwarzający i odbiorcę. Podmiot przetwarzający, w rozumieniu art. 4

pkt 8 RODO, przetwarza dane osobowe w imieniu administratora. W działalności uczelni mogą to być np. dostawcy systemów informatycznych, operatorzy platform e-learningowych, firmy hostingowe, dostawcy poczty elektronicznej, firmy świadczące usługi niszczenia dokumentów czy zewnętrzne podmioty obsługujące ankiety, systemy antyplagiatowe lub narzędzia do rekrutacji elektronicznej. Jeżeli zewnętrzny podmiot przetwarza dane na zlecenie uczelni, konieczne może być zawarcie umowy powierzenia przetwarzania zgodnej z art. 28 RODO.

Odbiorcą danych jest natomiast podmiot, któremu ujawnia się dane osobowe. Odbiorcą może być np. organ publiczny, instytucja przyjmująca studenta na praktyki, uczelnia zagraniczna w ramach wymiany akademickiej czy podmiot realizujący badanie ankietowe. Uczelnia powinna każdorazowo ustalić, czy przekazanie danych ma podstawę prawną, jaki jest jego cel oraz jaki zakres danych jest niezbędny.

2.6. Inspektor ochrony danych

Inspektor ochrony danych (IOD) to osoba wyznaczana przez administratora lub podmiot przetwarzający w celu wspierania prawidłowego stosowania przepisów o ochronie danych osobowych. Zgodnie z art. 37 ust. 1 lit. a RODO wyznaczenie IOD jest obowiązkowe m.in. wtedy, gdy przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania wymiaru sprawiedliwości. RODO nie definiuje jednak pojęcia „organu lub podmiotu publicznego”, pozostawiając to, zgodnie z motywem 97 preambuły, prawu krajowemu. Na gruncie prawa polskiego pojęcie to doprecyzowuje art. 9 ustawy o ochronie danych osobowych, odsyłający do kategorii jednostek sektora finansów publicznych w rozumieniu art. 9 ustawy o finansach publicznych⁴, który w pkt 11 wymienia wprost uczelnie publiczne. Obowiązek wyznaczenia IOD dotyczy zatem uczelni publicznych, jednakże również na uczelniach niepublicznych mogą działać inspektorzy ochrony danych osobowych.

IOD pełni funkcję doradczą i monitorującą: informuje administratora, podmiot przetwarzający oraz pracowników o obowiązkach wynikających z RODO i doradza im w tym zakresie, monitoruje przestrzeganie przepisów, udziela na żądanie zaleceń co do oceny skutków dla ochrony danych, a także pełni funkcję punktu kontaktowego zarówno dla osób, których dane dotyczą, jak i dla organu nadzorczego, czyli Prezesa UODO. Dane kontaktowe IOD powinny być publicznie dostępne, w tym zamieszczane w klauzulach informacyjnych kierowanych do studentów. W przypadku wątpliwości dotyczących przetwarzania danych osobowych na uczelni warto skontaktować się z IOD.

2.7. Naruszenie ochrony danych osobowych

⁴ Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2025 r. poz. 1483).

Naruszenie ochrony danych osobowych zostało zdefiniowane w art. 4 pkt 12 RODO jako 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. Może dojść do niego zarówno przez przypadek (np. zgubienie pendrive'a czy awaria techniczna), jak i w wyniku celowego działania (np. kradzież sprzętu). Naruszenie może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfalszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych chronionych tajemnicą zawodową lub inne znaczne szkody gospodarcze lub społeczne (motyw 85 RODO). Szerzej na temat naruszeń ochrony danych osobowych w działalności uczelni - zob. rozdział 9.

3. Zakres stosowania RODO w działalności uczelni

3.1. Przetwarzanie danych w ramach działalności instytucjonalnej uczelni

Uczelnie w ramach swojej działalności przetwarzają różnorodne dane osobowe wielu kategorii osób, w szczególności kandydatów na studia, studentów, doktorantów oraz pracowników. RODO znajduje zastosowanie do przetwarzania danych osobowych przez uczelnię w związku z realizacją jej zadań publicznych, wykonywaniem obowiązków ustawowych lub osiąganiem innych prawnie uzasadnionych celów. Przykładem takich sytuacji jest przetwarzanie danych kandydatów w procesie rekrutacji, prowadzenie akt osobowych studentów, dokumentowanie osiągnięć akademickich czy obsługa wniosków o stypendia. W każdym z powyższych przypadków będziemy mieli do czynienia z przetwarzaniem, które pociąga za sobą liczne obowiązki opisane szczegółowo poniżej.

3.2. Wyłączenie dotyczące czynności o charakterze osobistym lub domowym

Co istotne, RODO nie znajduje zastosowania do każdej sytuacji, w której osoba fizyczna posługuje się danymi osobowymi innej osoby. Zakresem rozporządzenia nie są objęte czynności o charakterze wyłącznie osobistym lub domowym, niezwiązane z działalnością instytucjonalną. Przykładowo, prywatna wymiana numerów telefonu między studentami tej samej grupy zajęciowej, prowadzona w celu utrzymywania kontaktu lub organizacji wspólnej nauki, mimo iż odbywa się na uczelni, co do zasady nie będzie podlegała reżimowi RODO. Inaczej należałoby jednak ocenić sytuację, w której dane studentów są zbierane lub udostępniane w ramach konkretnej działalności uczelni, samorządu studenckiego albo innego podmiotu działającego w określonej strukturze organizacyjnej.



3.3. Ustalenie roli podmiotu przetwarzającego dane

Analiza ochrony danych osobowych studentów wymaga każdorazowego ustalenia, kto przetwarza ich dane, w jakim celu, na jakiej podstawie prawnej oraz czy przetwarzanie ma charakter prywatny, czy instytucjonalny. Rozstrzygające znaczenie ma kryterium faktyczne i funkcjonalne: kto samodzielnie decyduje o celach i sposobach przetwarzania danych, a kto jedynie wykonuje te decyzje w imieniu innego podmiotu, na podstawie udzielonych mu instrukcji. Ustalenie to nie może opierać się wyłącznie na nazwie umowy czy deklaracji stron, lecz na rzeczywistym rozkładzie decyzyjności. W działalności uczelni pytanie to pojawia się szczególnie często w relacjach z zewnętrznymi dostawcami usług czy podmiotami przyjmującymi studentów na praktyki. W każdym z tych przypadków analiza musi być prowadzona odrębnie dla poszczególnych procesów przetwarzania, ponieważ ten sam podmiot może w jednym zakresie działać jako podmiot przetwarzający, a w innym już jako niezależny administrator. Dopiero odpowiedź na powyższe pytania pozwala określić, czy w danym przypadku zastosowanie znajdą przepisy RODO oraz jakie obowiązki będą ciążyć na konkretnym podmiocie.

3.4. Uczelnia jako administrator danych osobowych

Wewnątrz uczelni mamy do czynienia ze złożoną strukturą, w której poszczególne jednostki (wydziały, dziekanaty, domy studenckie) operują w imieniu jednego administratora. Uczelnia ustala cele i sposoby przetwarzania danych studentów wtedy, gdy decyduje, jakie dane są zbierane w rekrutacji, jakie dane są wymagane w toku studiów, jak prowadzona jest dokumentacja przebiegu studiów, jakie systemy informatyczne są wykorzystywane, kto ma dostęp do danych, jak długo są przechowywane dokumenty oraz kiedy i komu dane są udostępniane. Pracownicy dziekanatu, nauczyciele akademicy, komisje rekrutacyjne, komisje stypendialne, organy uczelni w powyższych działają wówczas w strukturze jednego administratora oraz na jego polecenie.

Co istotne uczelnia nie może uchylić się od odpowiedzialności za błędy spowodowane przez nieprawidłowe działania pracownika czy sprzętu używanego do przetwarzania danych, co obrazuje naruszenie omówione szerzej w rozdziale 9.8.

Pomimo że poszczególne jednostki wydzielone w ramach uczelni nie są administratorem danych osobowych, nie oznacza to, że na ich działanie nie ma wpływu ochrona danych osobowych. Administrator powinien jasno określić zakresy upoważnień, procedury dostępu, odpowiedzialność służbową czy zasady obiegu dokumentów i kanały komunikacji. Zgodnie z zasadą *need to know* dane przetwarzane przez poszczególne jednostki powinny być ograniczone jedynie do tych dla nich potrzebnych. Przykładowo nauczyciel akademicki nie potrzebuje danych dotyczących sytuacji socjalnej studenta, dlatego nie powinien on ich przetwarzać. Za to pracownik komisji stypendialnej może

potrzebować dostępu do danych o sytuacji materialnej studenta, ale dostęp ten powinien być ograniczony do spraw, które rozpatruje.

4. Zasady przetwarzania danych osobowych studentów

Art. 5 RODO określa ogólne zasady przetwarzania danych osobowych, które dotyczą również uczelni. Przepis nie wskazuje konkretnej podstawy prawnej przetwarzania, ale określa reguły, które administrator musi respektować przy każdym przetwarzaniu danych.

4.1. Zasada zgodności z prawem, rzetelności i przejrzystości

Dane powinny być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Na uczelni jako administratorze ciąży w związku z tym obowiązek zapewnienia studentowi wiedzy o tym, kto przetwarza jego dane, w jakim celu, na jakiej podstawie, komu dane mogą być przekazywane i jak długo będą przechowywane. Informacje te powinny być przekazywane w sposób zrozumiały, łatwo dostępny i sformułowany prostym językiem, najczęściej w formie klauzuli informacyjnej udostępnianej przy pozyskiwaniu danych. Realizacja zasady przejrzystości ma umożliwić osobie, której dane są przetwarzane świadome korzystanie z praw przysługujących jej na gruncie RODO, takich jak prawo dostępu do danych, ich sprostowania, usunięcia czy ograniczenia przetwarzania.

4.2. Zasada ograniczenia celu

Zasada ograniczenia celu oznacza, że dane powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nie mogą być następnie przetwarzane w sposób niezgodny z tymi celami. Sam cel przetwarzania powinien zostać określony najpóźniej w chwili pozyskania danych, a jego sformułowanie musi być na tyle precyzyjne, aby osoba, której dane dotyczą, mogła zrozumieć, dlaczego jej dane są przetwarzane. W praktyce uczelnia powinna już na etapie pozyskiwania danych określić, czy są one zbierane w celu przeprowadzenia rekrutacji, realizacji procesu kształcenia, przyznawania świadczeń dla studentów, prowadzenia dokumentacji przebiegu studiów czy wykonywania innych obowiązków wynikających z przepisów prawa. Konsekwencją tej zasady jest zakaz wykorzystywania danych do celów niezgodnych z celem ich pierwotnego zebrania, chyba że dalsze przetwarzanie znajduje odrębną podstawę prawną lub spełnione są przesłanki dopuszczalności dalszego przetwarzania przewidziane w RODO. Przykładowo dane zgromadzone w toku rekrutacji nie powinny być automatycznie wykorzystywane do działań promocyjnych uczelni, jeżeli kandydat lub student nie został o takim celu poinformowany i nie istnieje odpowiednia podstawa prawna. Podobnie

informacje przekazane w związku z ubieganiem się o świadczenia dla studentów nie powinny być wykorzystywane do innych celów administracyjnych bez uprzedniej oceny zgodności takiego przetwarzania z zasadą ograniczenia celu oraz istnienia właściwej podstawy prawnej.

4.3. Zasada minimalizacji danych

Zasada minimalizacji danych wymaga, aby uczelnia przetwarzała dane adekwatne i stosowne do tego, co niezbędne. Naruszeniem może być żądanie nadmiarowych zaświadczeń, publikowanie list z pełnymi danymi identyfikacyjnymi, zbieranie danych zdrowotnych bez realnej potrzeby albo udostępnianie całych akt sprawy osobom, które potrzebują jedynie wybranych informacji.

4.4. Zasada prawidłowości danych

Zasada prawidłowości danych oznacza obowiązek dbania o aktualność, tj. poprawność danych. Ma to znaczenie np. przy zmianie nazwiska, adresu, numeru rachunku bankowego, orzeczenia o niepełnosprawności lub danych kontaktowych.

4.5. Zasada ograniczenia przechowywania

Zasada ograniczenia przechowywania wymaga, aby dane były przechowywane nie dłużej, niż jest to konieczne. Uczelnia powinna odróżniać dokumentację, którą musi przechowywać przez okres wynikający z odrębnych przepisów, od dokumentów pomocniczych, roboczych, ankietowych lub promocyjnych, które powinny być usuwane we właściwym czasie. Szerzej na temat okresów przechowywania - zob. rozdział 6.7.

4.6. Zasada integralności i poufności

Zasada integralności i poufności wymaga zabezpieczenia danych przed nieuprawnionym dostępem, przypadkową utratą, zniszczeniem lub uszkodzeniem. Przykładem naruszenia w kontekście uczelnianym może być wysłanie wiadomości e-mail do grupy studentów bez ukrycia ich adresów e-mail, pozostawianie list ocen w miejscu publicznym, brak kontroli dostępu w systemie informatycznym albo przechowywanie danych studentów na prywatnym komputerze pracownika bez odpowiednich zabezpieczeń.

4.7. Zasada rozliczalności

Zasada rozliczalności wymaga, aby uczelnia nie tylko przestrzegała przepisów o ochronie danych osobowych, lecz także była w stanie wykazać ich przestrzeganie. Oznacza to w szczególności konieczność odpowiedniego dokumentowania decyzji dotyczących podstaw prawnych przetwarzania,

zakresu przetwarzanych danych, okresów ich przechowywania, przeprowadzonych analiz ryzyka, nadawanych upoważnień, zawieranych umów powierzenia przetwarzania oraz procedur reagowania na naruszenia ochrony danych osobowych.

5. Podstawy prawne przetwarzania danych osobowych studentów

5.1. Obowiązek prawny ciążyący na uczelni

Dane osobowe studentów przetwarzane są przez uczelnie m.in. na podstawie przesłanki określonej w art. 6 ust. 1 lit. c RODO, a więc jako niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Stosowanie tej podstawy wymaga jednak precyzyjnego rozumienia jej struktury i granic, bowiem - wbrew nierzadko spotykanej praktyce - art. 6 ust. 1 lit. c RODO nie stanowi samodzielnej podstawy przetwarzania danych. Przepis ten legalizuje przetwarzanie wyłącznie w połączeniu z konkretną normą prawną nakładającą na administratora określony obowiązek; samo powołanie się na „przepisy prawa” bez wskazania normy szczegółowej jest niewystarczające.

Dla uznania przetwarzania za dopuszczalne na tej podstawie konieczne jest łączne spełnienie dwóch przesłanek: po pierwsze, musi istnieć przepis prawa nakładający na administratora skonkretyzowany obowiązek prawny; po drugie, przetwarzanie danych musi być niezbędne do realizacji tego właśnie obowiązku. Jak wskazuje P. Litwiński, jeżeli okoliczności przetwarzania danych osobowych są regulowane bezpośrednio przepisami prawa, podstawę z art. 6 ust. 1 lit. c RODO należy stosować przed innymi podstawami⁵. Konsekwencją tego stanowiska jest m.in. zakaz zastępowania tej podstawy zgodą studenta w sytuacjach, gdy obowiązek przetwarzania wynika z przepisów prawa.

W kontekście relacji uczelnia-student głównym źródłem obowiązków prawnych uzasadniających przetwarzanie danych są przepisy PSWiN. Na ich podstawie uczelnia zobowiązana jest do prowadzenia szeregu procesów bezpośrednio związanych z tokiem studiów. Przykładowo: ujawnienie danych osobowych kandydatów na studia na listach wyników postępowania rekrutacyjnego znajduje podstawę prawną w art. 6 ust. 1 lit. c RODO w związku z art. 72 ust. 5 PSWiN, zgodnie z którym wyniki postępowania w sprawie przyjęcia na studia są jawne. Podobnie przetwarzanie danych w ramach obsługi wniosków o przyznanie pomocy materialnej opiera się na art. 6 ust. 1 lit. c RODO w powiązaniu z art. 86 PSWiN, który określa formy i zasady udzielania tej pomocy - co zostało potwierdzone wprost w stanowisku Prezesa Urzędu Ochrony Danych Osobowych⁶.

Należy podkreślić, że art. 6 ust. 1 lit. c RODO wyznacza zarazem granice zakresu przetwarzania: uczelnia może przetwarzać wyłącznie te dane i w takim zakresie, jaki jest niezbędny do wypełnienia

⁵ P. Litwiński [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, Warszawa 2021.

⁶ Stanowisko dostępne w archiwum UODO: <https://uodo.gov.pl/pl/674/4215> [dostęp: 2.08.2026 r.].

konkretnego obowiązku ustawowego. Zasada minimalizacji danych z art. 5 ust. 1 lit. c RODO ogranicza możliwość gromadzenia danych wykraczających poza ten zakres, nawet jeśli mogłyby one być użyteczne dla administratora z innych powodów. Naruszenie tej reguły, polegające np. na zbieraniu szerszego zakresu danych niż wymagają przepisy, może stanowić samodzielne naruszenie RODO, niezależnie od tego, czy istnieje ważna przesłanka przetwarzania w odniesieniu do danych objętych obowiązkiem ustawowym.

5.2. Wykonywanie zadania realizowanego w interesie publicznym

Odrębną podstawę przetwarzania danych osobowych studentów stanowi wykonywanie zadania realizowanego w interesie publicznym. Ma ona szczególne znaczenie w działalności uczelni, ponieważ wiele czynności podejmowanych w ramach procesu kształcenia służy realizacji ustawowych zadań szkolnictwa wyższego, choć nie wynika z obowiązku przetwarzania konkretnych danych określonego w przepisach prawa. Art. 6 ust. 1 lit. c RODO nie legalizuje przetwarzania danych niezbędnych do realizacji fakultatywnych uprawnień uczelni - w takich przypadkach właściwą przesłanką może być art. 6 ust. 1 lit. e RODO (wykonanie zadania realizowanego w interesie publicznym). Granica między obowiązkiem a uprawnieniem nie zawsze jest oczywista: przykładowo prowadzenie działalności dydaktycznej przez uczelnię publiczną, w tym organizacja zajęć, ocenianie i przeprowadzanie egzaminów, opiera się przede wszystkim na art. 6 ust. 1 lit. e RODO jako przejaw wykonywania zadania publicznego - nie zaś na lit. c, gdyż przepisy PSWiN określają tu ramy działalności uczelni, nie nakładając obowiązku przetwarzania konkretnych danych wobec konkretnego studenta.

5.3. Zgoda studenta

Zgoda studenta (art. 6 ust. 1 lit. a RODO) jest podstawą przetwarzania, którą uczelnia powinna stosować z ostrożnością. Zgodnie z motywem 43 RODO zgoda nie powinna stanowić ważnej podstawy prawnej, jeżeli między osobą, której dane dotyczą, a administratorem istnieje wyraźny brak równowagi - co może mieć miejsce w relacji uczelnia-student, zwłaszcza gdy odmowa zgody mogłaby realnie wpłynąć na sytuację studenta w toku studiów. Z tego względu zgoda jest właściwą podstawą przede wszystkim w odniesieniu do czynności całkowicie dobrowolnych i niewiążących się z żadnym ryzykiem niekorzystnych konsekwencji w razie jej niewyrażenia lub wycofania - np. zapisu na newsletter, udziału w dodatkowych, nieobowiązkowych badaniach ankietowych czy wykorzystania wizerunku studenta w materiałach promocyjnych (zob. rozdział 8.13). Zgoda musi być dobrowolna, konkretna, świadoma i jednoznaczna, a student musi mieć możliwość jej wycofania w każdym czasie równie łatwo, jak ją wyraził (art. 7 ust. 3 RODO).

5.4. Wykonanie umowy

Podstawa z art. 6 ust. 1 lit. b RODO - niezbędność przetwarzania do wykonania umowy, której stroną jest osoba, której dane dotyczą - znajduje w działalności uczelni ograniczone zastosowanie. Przetwarzanie danych osobowych związane z przyjęciem na studia, przebiegiem kształcenia, dokumentowaniem osiągnięć studenta czy wydawaniem dyplomów wynika przede wszystkim z obowiązków nałożonych na uczelnie przez ustawę - Prawo o szkolnictwie wyższym i nauce oraz przepisy wykonawcze, dlatego jego podstawę stanowi co do zasady art. 6 ust. 1 lit. c lub e RODO. Natomiast art. 6 ust. 1 lit. b RODO może znaleźć zastosowanie w odniesieniu do stosunków o charakterze cywilnoprawnym, takich jak umowa o zakwaterowanie w domu studenckim, rozliczenia wynikające z umowy o odpłatne kształcenie lub inne umowy zawierane pomiędzy uczelnią a studentem, o ile przetwarzanie danych jest rzeczywiście niezbędne do wykonania konkretnego zobowiązania umownego. W każdym przypadku zakres przetwarzanych danych powinien być ograniczony do danych niezbędnych do realizacji celu wynikającego z danej umowy.

5.5. Prawnie uzasadniony interes administratora

Podstawa prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f RODO) nie znajduje zastosowania do przetwarzania danych przez organy publiczne w ramach realizacji ich zadań - a taką rolę pełni uczelnia wobec większości procesów dotyczących studentów, dla których właściwą podstawą pozostaje art. 6 ust. 1 lit. c lub lit. e RODO. Prawnie uzasadniony interes może natomiast znaleźć zastosowanie w węższym zakresie, np. zapewnienia bezpieczeństwa osób i mienia na terenie uczelni w zakresie nieobjętym odrębną podstawą. Zastosowanie tej podstawy każdorazowo wymaga przeprowadzenia testu równowagi, polegającego na zestawieniu interesu administratora z prawami i wolnościami osoby, której dane dotyczą.

5.6. Podstawy przetwarzania szczególnych kategorii danych

Przetwarzanie danych należących do szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO, wymaga spełnienia jednej z przesłanek określonych w art. 9 ust. 2 RODO. W działalności uczelni znaczenie mają w szczególności: wyraźna zgoda osoby, której dane dotyczą (lit. a), niezbędność przetwarzania ze względu na ważny interes publiczny na podstawie prawa Unii lub prawa państwa członkowskiego (lit. g), znajdująca zastosowanie m.in. w przypadkach przewidzianych w ustawie - Prawo o szkolnictwie wyższym i nauce, oraz niezbędność przetwarzania do celów profilaktyki zdrowotnej, medycyny pracy lub zapewnienia opieki zdrowotnej (lit. h), mająca znaczenie zwłaszcza w działalności leczniczej prowadzonej przez uczelnie medyczne. Natomiast przesłanka z art. 9 ust.

2 lit. b RODO znajduje zastosowanie przede wszystkim w odniesieniu do przetwarzania danych pracowników uczelni w zakresie obowiązków wynikających z prawa pracy i zabezpieczenia społecznego. Odrębną podstawę przetwarzania szczególnych kategorii danych do celów badań naukowych stanowi art. 9 ust. 2 lit. j RODO w związku z art. 89 ust. 1 RODO, rozwinęty na gruncie prawa polskiego w przepisach PSWiN - zagadnienie to omówiono szerzej w rozdziale 10.4.

5.7. Obowiązek prawny a uprawnienie uczelni

Kluczowe znaczenie praktyczne ma odróżnienie sytuacji, w których przepisy prawa nakładają na uczelnię obowiązek określonego działania, od przypadków, w których przyznają jej kompetencję do realizacji ustawowych zadań. W pierwszej grupie właściwą podstawę przetwarzania danych osobowych stanowi co do zasady art. 6 ust. 1 lit. c RODO, odnoszący się do wykonania obowiązku prawnego ciążącego na administratorze. Natomiast w drugiej grupie należy ocenić, czy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, co może uzasadniać zastosowanie art. 6 ust. 1 lit. e RODO. Sam fakt przyznania uczelni kompetencji nie przesądza automatycznie o właściwości tej podstawy - decydujące znaczenie ma charakter konkretnego zadania oraz treść przepisów określających jego wykonywanie. Zatem jeżeli przetwarzanie nie wynika ani z obowiązku prawnego, ani z realizacji zadania publicznego, konieczne jest rozważenie innej podstawy przetwarzania, w tym - w odpowiednich przypadkach - zgody osoby, której dane dotyczą. Prawidłowe rozróżnienie tych sytuacji ma znaczenie nie tylko dla wyboru właściwej podstawy prawnej, lecz także dla zakresu praw przysługujących studentowi jako osobie, której dane dotyczą (zob. rozdział 7).

6. Obowiązki uczelni jako administratora danych osobowych

6.1. Obowiązek informacyjny

To, jak administrator danych przetwarza dane, powinno zostać ujęte w klauzuli informacyjnej, która powinna być napisana prostym i przystępnym językiem. Klauzula informacyjna powinna obejmować między innymi dane administratora, dane kontaktowe inspektora ochrony danych osobowych, cele i podstawy prawne przetwarzania, informacje o odbiorcach danych, okres przechowywania, prawa osoby, której dane dotyczą, prawo wniesienia skargi do organu nadzorczego, informacje o obowiązku lub dobrowolności podania danych oraz ewentualne informacje o zautomatyzowanym podejmowaniu decyzji. Co istotne, nie musi być ona podpisywana, ponieważ prawo nie nakłada takiego obowiązku.

W uczelni taka klauzula informacyjna powinna się pojawiać między innymi w procesach rekrutacyjnych, w systemie obsługi studiów, przy ubieganiu się o świadczenia, w związku z odbywaniem praktyk, wymianą zagraniczną, korzystaniem z platformy do kształcenia na odległość, monitoringiem wizyjnym czy działaniami promocyjnymi.

6.2. Zapewnienie bezpieczeństwa danych

Zgodnie z art. 32 RODO administrator jest obowiązany wdrożyć odpowiednie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku związanemu z danym przetwarzaniem, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania. W praktyce uczelni oznacza to w szczególności: kontrolę dostępu do systemów i pomieszczeń, w których przechowywane są dane studentów, szyfrowanie danych wrażliwych, w tym danych o zdrowiu czy orzeczeniach o niepełnosprawności, regularne aktualizowanie i zabezpieczanie haseł, tworzenie kopii zapasowych, a także zdolność do szybkiego przywrócenia dostępności danych w razie incydentu. Środki te powinny być regularnie testowane i oceniane pod kątem skuteczności, a ich dobór powinien wynikać z uprzedniej analizy ryzyka związanego z konkretnym procesem przetwarzania.

6.3. Nadawanie upoważnień do przetwarzania danych

Osoby działające z upoważnienia administratora - w tym pracownicy dziekanatów, nauczyciele akademicki, członkowie komisji rekrutacyjnych - mogą przetwarzać dane studentów wyłącznie w zakresie objętym udzielonym im upoważnieniem. Upoważnienie powinno mieć formę imienną i określać zakres danych oraz czynności, do których dana osoba jest uprawniona, zgodnie z zasadą ograniczonego dostępu (*need to know*). Uczelnia jako administrator powinna prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych oraz zapewnić, aby upoważnienia były aktualizowane w razie zmiany zakresu obowiązków danej osoby lub ustania zatrudnienia.

6.4. Prowadzenie rejestru czynności przetwarzania

Zgodnie z art. 30 RODO administrator prowadzi rejestr czynności przetwarzania, obejmujący m.in. cele przetwarzania, opis kategorii osób, których dane dotyczą, i kategorii danych osobowych, kategorie odbiorców danych, planowane terminy usunięcia poszczególnych kategorii danych oraz ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. W uczelni rejestr ten powinien odzwierciedlać wszystkie istotne procesy przetwarzania danych studentów - od rekrutacji, przez obsługę toku studiów, po przyznawanie świadczeń i prowadzenie badań naukowych. Prowadzenie

rejestr stanowi jeden z podstawowych elementów realizacji zasady rozliczalności i ułatwia wykazanie zgodności przetwarzania z RODO w razie kontroli Prezesa UODO.

6.5. Ocena ryzyka i ocena skutków dla ochrony danych

Jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator jest obowiązany dokonać, przed rozpoczęciem przetwarzania, oceny skutków dla ochrony danych (art. 35 RODO). Obowiązek ten może dotyczyć uczelni np. w przypadku wdrażania systemów monitoringu wizyjnego na szeroką skalę, systemów biometrycznej weryfikacji tożsamości studentów czy zautomatyzowanych narzędzi antyplagiatowych analizujących duże zbiory danych. Ocena skutków powinna zawierać systematyczny opis planowanych operacji przetwarzania, ocenę niezbędności i proporcjonalności operacji, ocenę ryzyka dla praw i wolności osób oraz środki planowane w celu zaradzenia temu ryzyku. Jeżeli ocena wykaże wysokie ryzyko, którego nie można ograniczyć odpowiednimi środkami, administrator jest obowiązany skonsultować się z Prezesem UODO przed rozpoczęciem przetwarzania (art. 36 RODO).

6.6. Powierzenie przetwarzania danych

Współpraca uczelni z podmiotami zewnętrznymi wymaga każdorazowo precyzyjnego ustalenia, w jakiej roli podmiot ten występuje wobec przetwarzanych danych, ponieważ od tego zależy właściwa forma prawna organizująca to przetwarzanie. Należy odróżnić trzy sytuacje. Po pierwsze, jeżeli podmiot zewnętrzny przetwarza dane wyłącznie w imieniu uczelni i na jej udokumentowane polecenie, nie ustalając samodzielnie celów tego przetwarzania (np. dostawca zewnętrznego systemu informatycznego obsługującego tok studiów, podmiot świadczący usługi niszczenia dokumentacji), konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych na podstawie art. 28 RODO. Umowa taka powinna określać w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, obowiązki i prawa administratora, a także zasady dalszego podpowierzenia przetwarzania innemu podmiotowi. Po drugie, jeżeli uczelnia i podmiot zewnętrzny wspólnie ustalają cele i sposoby przetwarzania tych samych danych, mamy do czynienia ze współadministrowaniem wymagającym uzgodnienia, o którym mowa w art. 26 RODO. Po trzecie, jeżeli podmiot zewnętrzny, otrzymawszy dane od uczelni, przetwarza je następnie w celach przez siebie samodzielnie ustalonych i na własną odpowiedzialność, dochodzi jedynie do zwykłego udostępnienia danych pomiędzy dwoma odrębnymi administratorami - sytuacja taka nie wymaga zawarcia umowy powierzenia, lecz wymaga zapewnienia właściwej podstawy prawnej udostępnienia oraz spełnienia obowiązku informacyjnego wobec

studenta co do faktu i celu udostępnienia. Praktyczne zastosowanie tego rozróżnienia, na przykładzie podmiotu przyjmującego studenta na praktyki zawodowe, omówiono w rozdziale 8.6.

6.7. Okresy przechowywania i usuwanie danych

Uczelnia powinna odróżniać dokumentację, którą musi przechowywać przez okres wynikający z odrębnych przepisów, w tym przepisów o dokumentacji przebiegu studiów i przepisów archiwalnych (zob. rozdział 8.2), od dokumentów pomocniczych, roboczych, ankietowych lub promocyjnych, które powinny być usuwane niezwłocznie po ustaniu celu, dla którego zostały zebrane. Realizacja tego obowiązku wymaga prowadzenia przez uczelnię odpowiedniej polityki retencji danych, określającej okresy przechowywania poszczególnych kategorii dokumentacji oraz zasady jej niszczenia lub anonimizacji po upływie tych okresów.

6.8. Współpraca z inspektorem ochrony danych

Jak zostało wyżej wspomniane uczelnia publiczna, jako podmiot publiczny w rozumieniu art. 37 ust. 1 lit. a RODO, jest obowiązana wyznaczyć inspektora ochrony danych i zapewnić mu współudział we wszystkich sprawach dotyczących ochrony danych osobowych, w tym na etapie planowania nowych procesów przetwarzania. W praktyce oznacza to obowiązek konsultowania z inspektorem m.in. treści klauzul informacyjnych, umów powierzenia przetwarzania, wdrażanych systemów informatycznych oraz przypadków naruszenia ochrony danych osobowych. Inspektor powinien mieć zapewnione niezbędne zasoby do wykonywania swoich zadań oraz dostęp do danych osobowych i operacji przetwarzania, a jego dane kontaktowe powinny być podane do wiadomości studentów oraz zgłoszone Prezesowi UODO.

7. Prawa studenta jako osoby, której dane dotyczą

Student jako osoba, której dane dotyczą, korzysta z praw przewidzianych w art. 15–22 RODO. Należą do nich: prawo do dostępu do danych, prawo do sprostowania, prawo do usunięcia danych, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu oraz prawa związane z zautomatyzowanym podejmowaniem decyzji.

7.1. Prawo dostępu do danych

Prawo dostępu obejmuje zarówno możliwość uzyskania potwierdzenia, czy uczelnia przetwarza dane osobowe studenta, jak i prawo do uzyskania informacji o zakresie tego przetwarzania oraz kopii danych osobowych. Student może żądać w szczególności informacji o celach przetwarzania, kategoriach przetwarzanych danych, odbiorcach lub kategoriach odbiorców danych, planowanym

okresie ich przechowywania, źródle pochodzenia danych (jeżeli nie zostały zebrane od niego), a także o przysługujących mu prawach oraz o ewentualnym zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu. W praktyce prawo dostępu może obejmować m.in. dane zgromadzone w systemach informatycznych uczelni, dokumentację przebiegu studiów, oceny, akta postępowań stypendialnych, dokumentację dotyczącą indywidualnej organizacji studiów lub postępowań związanych z przyznaniem miejsca w domu studenckim. Student ma również prawo otrzymać kopię swoich danych osobowych przetwarzanych przez uczelnię, przy czym nie może to prowadzić do naruszenia praw i wolności innych osób.

7.2. Prawo do sprostowania danych

Prawo do sprostowania danych (art. 16 RODO) umożliwia studentowi żądanie niezwłocznego poprawienia nieprawidłowych danych osobowych oraz uzupełnienia danych niekompletnych, z uwzględnieniem celów przetwarzania. W praktyce uczelni prawo to ma zastosowanie m.in. do błędnych danych identyfikacyjnych i kontaktowych (np. adresu zamieszkania, numeru telefonu, adresu e-mail czy numeru rachunku bankowego), nieaktualnych informacji o statusie studenta lub innych danych administracyjnych wykorzystywanych w toku studiów. Uczelnia powinna zapewnić przejrzystą procedurę zgłaszania i weryfikacji wniosków o sprostowanie, umożliwiając jednocześnie udokumentowanie dokonanych zmian.

7.3. Prawo do usunięcia danych

Prawo do usunięcia danych, uregulowane w art. 17 RODO, nie ma charakteru absolutnego. W realiach funkcjonowania uczelni możliwość żądania usunięcia danych jest często ograniczona przez przepisy nakładające na uczelnię obowiązek ich dalszego przechowywania. Przykładowo student nie może skutecznie domagać się usunięcia danych zawartych w aktach osobowych studenta czy dokumentach stanowiących podstawę przyjęcia na studia, jeżeli obowiązek ich przechowywania wynika z przepisów Prawa o szkolnictwie wyższym i nauce lub przepisów archiwalnych. W takich przypadkach administrator ma obowiązek odmówić realizacji żądania, wskazując podstawę prawną dalszego przetwarzania. Odmienne należy ocenić dane, których przetwarzanie opiera się wyłącznie na zgodzie studenta lub które są przetwarzane bez ważnej podstawy prawnej. W takich sytuacjach student może domagać się ich usunięcia, o ile nie zachodzi żadna z przesłanek wyłączających stosowanie art. 17 RODO. W praktyce może to dotyczyć przykładowo danych wykorzystywanych do celów promocyjnych czy informacji przetwarzanych na podstawie dobrowolnie udzielonej zgody, która została następnie cofnięta

7.4. Prawo do ograniczenia przetwarzania

Prawo do ograniczenia przetwarzania (art. 18 RODO) pozwala żądać, aby administrator czasowo zaprzestał aktywnego wykorzystywania danych osobowych - np. na czas weryfikacji ich prawidłowości, ustalenia bezprawności przetwarzania czy rozpatrzenia wniesionego sprzeciwu - przy zachowaniu samych danych w celu ich przechowania. W okresie ograniczenia dane mogą być przetwarzane, poza przechowywaniem, jedynie za zgodą studenta albo w celu ustalenia, dochodzenia lub obrony roszczeń. Uczelnia powinna dysponować procedurą pozwalającą oznaczyć dane objęte takim żądaniem, tak aby nie były one wykorzystywane w bieżących procesach do czasu wyjaśnienia sprawy.

7.5. Prawo do przenoszenia danych

Prawo do przenoszenia danych (art. 20 RODO) pozwala żądać otrzymania danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego oraz przesłania ich innemu administratorowi. Prawo to znajduje zastosowanie wtedy, gdy przetwarzanie odbywa się na podstawie zgody lub umowy oraz w sposób zautomatyzowany. W relacji uczelnia–student prawo to ma zatem ograniczone zastosowanie, ponieważ większość danych studenckich przetwarzana jest na podstawie obowiązku prawnego lub zadania realizowanego w interesie publicznym, nie zaś zgody czy umowy. Może ono znaleźć zastosowanie np. wobec danych podanych dobrowolnie w ramach nieobowiązkowych usług oferowanych przez uczelnię za pośrednictwem systemów informatycznych.

7.6. Prawo do sprzeciwu

Prawo do sprzeciwu (art. 21 RODO) przysługuje wobec przetwarzania opartego na podstawie wykonania zadania realizowanego w interesie publicznym lub prawnie uzasadnionego interesu administratora, a więc w praktyce może dotyczyć części procesów przetwarzania prowadzonych przez uczelnię poza sferą ściśle związaną z wypełnianiem obowiązków ustawowych. Po wniesieniu sprzeciwu uczelnia powinna zaprzestać przetwarzania danych w zakwestionowanym zakresie, chyba że wykáže istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności studenta, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

7.7. Prawo do wniesienia skargi do Prezesa UODO

Zgodnie z art. 77 RODO każda osoba, której dane dotyczą, ma prawo wniesienia skargi do organu nadzorczego, jeżeli sądzi, że przetwarzanie jej danych osobowych narusza przepisy RODO. W Polsce organem tym jest Prezes Urzędu Ochrony Danych Osobowych. Prawo to przysługuje

niezależnie od tego, czy student wcześniej zwrócił się bezpośrednio do uczelni lub jej inspektora ochrony danych, choć w praktyce zasadne jest uprzednie podjęcie próby wyjaśnienia sprawy z administratorem. Skarga powinna wskazywać podmiot, którego dotyczy, opis zdarzenia oraz uzasadnienie, na czym - zdaniem skarżącego - polega naruszenie przepisów o ochronie danych osobowych. Wniesienie skargi nie wyłącza możliwości dochodzenia roszczeń na drodze sądowej, w tym odszkodowania na podstawie art. 82 RODO.

8. Szczególne obszary przetwarzania danych osobowych studentów

8.1. Rekrutacja na studia i publikowanie wyników

Rekrutacja jest jednym z pierwszych etapów, na których uczelnia przetwarza szeroki zakres danych osobowych kandydatów. Szczególnym aspektem tego procesu jest jawność jego wyników, wynikająca z art. 72 ust. 5 ustawy PSWiN, która nie oznacza jednak pełnej jawności wszystkich danych kandydatów. Jawność ogranicza się jedynie do wyników postępowania, a nie samego postępowania. „W orzecznictwie ugruntował się pogląd, że wynik stanowi lista osób przyjętych i nieprzyjętych na studia wraz z uzyskaną przez nie ostateczną liczbą punktów”⁷. Pojawia się zatem wątpliwość, jaki zbiór danych może zawierać lista osób. Wydaje się, że uczelnia powinna publikować wyniki w sposób ograniczony do informacji niezbędnych do realizacji celu jawności. Najbezpieczniejszym rozwiązaniem jest wykorzystywanie identyfikatorów rekrutacyjnych, numerów kandydata albo publikacja wyników po zalogowaniu się do indywidualnego konta kandydata. Publikowanie danych takich jak numery PESEL czy adresy kandydatów mogłoby naruszać zasadę minimalizacji wynikającą z RODO. Co istotne, PSWiN nie nakłada na uczelnię wymogu upublicznienia tych danych np. za pomocą Biuletynu Informacji Publicznej.

8.2. Dokumentacja przebiegu studiów

Jednym z podstawowych obszarów przetwarzania danych osobowych przez uczelnie jest prowadzenie dokumentacji przebiegu studiów. Uczelnia jest obowiązana prowadzić dokumentację przebiegu studiów każdego studenta, obejmującą w szczególności akta osobowe, protokoły egzaminacyjne, indeks lub jego elektroniczny odpowiednik oraz dokumentację związaną z przyznawaniem świadczeń i decyzjami dotyczącymi toku studiów. Zakres i sposób prowadzenia tej dokumentacji określają przepisy wykonawcze do PSWiN. Dokumentacja ta stanowi przetwarzanie danych osobowych w rozumieniu RODO i podlega ogólnym zasadom, w tym zasadzie minimalizacji

⁷M. Dokowicz [w:] Prawo o szkolnictwie wyższym i nauce. Komentarz, red.J. Woźnicki, Warszawa 2019, art. 72. <https://sip-1lex-1pl-15d274slm02a3.han.bg.us.edu.pl/#/commentary/587806916/604356/woznicki-jerzy-red-prawo-o-szkolnictwie-wyzszym-i-nauce-komentarz> (dostęp: 2026-05-13).

oraz ograniczenia przechowywania - z zastrzeżeniem, że dokumentacja przebiegu studiów podlega obowiązkowej archiwizacji przez okresy określone w odrębnych przepisach, niezależnie od tego, czy student kontynuuje studia.

8.3. Oceny, egzaminy i zaliczenia

Publikowanie ocen lub wyników z egzaminu wymaga szczególnej ostrożności, ponieważ ocena stanowi daną osobową, jeżeli można ją powiązać z konkretnym studentem. Dzieje się tak w szczególności wtedy, gdy ocena występuje łącznie z danymi identyfikującymi studenta, takimi jak jego imię i nazwisko, numer albumu lub inne informacje pozwalające ustalić jego tożsamość. Uczelnia powinna unikać wywieszania list ocen w miejscach publicznych lub publikowania ich na ogólnodostępnych stronach internetowych. Właściwsze jest przekazywanie ocen przez indywidualne konto w systemie uczelnianym lub za pomocą indywidualnych numerów studentów.

8.4. Stypendia i inne świadczenia dla studentów

Przyznawanie świadczeń pomocy materialnej - stypendium socjalnego, stypendium rektora, stypendium dla osób z niepełnosprawnością czy zapomogi - może się wiązać z przetwarzaniem szczególnie wrażliwych danych studenta, w tym danych o dochodach, sytuacji rodzinnej, a w przypadku stypendium dla osób z niepełnosprawnością - także danych o stanie zdrowia. Podstawę przetwarzania stanowi art. 6 ust. 1 lit. c RODO w związku z art. 86 i n. PSWiN, określającymi zasady przyznawania świadczeń. Ze względu na wrażliwość tych danych dostęp do dokumentacji stypendialnej powinien być ograniczony do członków komisji stypendialnej oraz pracowników bezpośrednio zaangażowanych w obsługę tych spraw, zgodnie z zasadą *need to know*, a dokumentacja powinna być przechowywana w sposób uniemożliwiający zapoznanie się z nią osobom nieuprawnionym.

8.5. Dane dotyczące zdrowia i niepełnosprawności

Dane dotyczące zdrowia i niepełnosprawności studenta należą do szczególnych kategorii danych osobowych w rozumieniu art. 9 RODO i podlegają wzmocnionej ochronie. Uczelnia przetwarza takie dane m.in. w związku z przyznawaniem świadczeń dla osób z niepełnosprawnością, dostosowywaniem warunków studiowania i zdawania egzaminów do potrzeb studenta, a w przypadku kierunków medycznych - także w związku z odbywaniem praktyk w placówkach ochrony zdrowia. Przetwarzanie takich danych wymaga istnienia jednej z podstaw wskazanych w art. 9 ust. 2 RODO. Dokumentacja medyczna i orzeczenia o niepełnosprawności powinny być przechowywane odrębnie

od pozostałej dokumentacji studenckiej i udostępniane wyłącznie osobom, dla których jest to niezbędne do wykonywania obowiązków.

8.6. Praktyki zawodowe

Kierowanie studenta na praktyki zawodowe jest sytuacją, w której uczelnia musi ustalić, jakie podmioty będą przetwarzały jego dane osobowe oraz w jakim charakterze będą występowały. Konieczne zatem będzie zastosowanie rozróżnienia ról opisanego w rozdziale 6.6. Samo przekazanie danych studenta podmiotowi przyjmującemu na praktykę nie przesądza bowiem jeszcze o powierzeniu przetwarzania, a kwalifikacja tej relacji zależy od tego, kto określa cele i sposoby wykorzystywania tych danych. Prezes UODO w wyjaśnieniach dotyczących kierowania studentów na praktyki wskazał, że umowa powierzenia przetwarzania danych osobowych (art. 28 RODO) byłaby potrzebna jedynie wtedy, gdyby podmiot przyjmujący na praktykę przetwarzał dane studenta wyłącznie w imieniu i na polecenie uczelni, nie ustalając samodzielnie celu tego przetwarzania. W typowym stanie faktycznym sytuacja taka jednak nie zachodzi: podmiot przyjmujący na praktykę przetwarza dane studenta we własnych celach - prowadzenia ewidencji obecności, zapewnienia bezpieczeństwa i higieny pracy, nadawania upoważnień do systemów i pomieszczeń - wynikających z umowy o praktykę, przepisów prawa pracy lub regulacji wewnętrznych tego podmiotu, a nie z polecenia uczelni. Podmiot ten działa zatem jako odrębny administrator danych, a nie jako podmiot przetwarzający w imieniu uczelni, w związku z czym zawarcie umowy powierzenia nie jest w tym zakresie właściwym rozwiązaniem⁸. Przekazanie uczelni danych o przebiegu i zaliczeniu praktyki przez podmiot przyjmujący stanowi w tym układzie zwykle udostępnienie danych pomiędzy dwoma odrębnymi administratorami, wymagające zapewnienia właściwej podstawy prawnej po obu stronach oraz odpowiedniej realizacji obowiązku informacyjnego wobec studenta, nie zaś zawarcia porozumienia współadministratorów, które byłoby właściwe dopiero w razie wspólnego ustalania celów i sposobów przetwarzania przez uczelnię i podmiot przyjmujący (zob. rozdział 6.6).

8.7. Wymiana akademicka i mobilność międzynarodowa

Udział studenta w programach wymiany akademickiej, takich jak Erasmus+, wiąże się z przekazywaniem jego danych osobowych uczelni przyjmującej, a niekiedy także instytucjom pośredniczącym w organizacji wymiany. W przypadku gdy uczelnia przyjmująca znajduje się na terytorium państwa członkowskiego Unii Europejskiej lub innego państwa Europejskiego Obszaru Gospodarczego, przekazanie danych odbywa się w ramach jednolitego obszaru stosowania RODO i nie

⁸Urząd Ochrony Danych Osobowych, *Czy w przypadku kierowania studenta na praktyki zawodowe konieczne jest powierzenie?*, <https://uodo.gov.pl/pl/675/4225> [dostęp: 2.08.2026 r.].

stanowi transferu danych do państwa trzeciego. W takiej sytuacji uczelnia powinna jedynie zapewnić, aby przekazywany zakres danych był zgodny z zasadą minimalizacji oraz opierał się na właściwej podstawie przetwarzania. Jeżeli natomiast uczelnia przyjmująca znajduje się poza Europejskim Obszarem Gospodarczym, przekazanie danych stanowi transfer danych do państwa trzeciego w rozumieniu rozdziału V RODO i wymaga zapewnienia odpowiedniego stopnia ochrony - na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony, standardowych klauzul umownych albo innego mechanizmu przewidzianego w art. 46 RODO. Uczelnia wysyłająca powinna każdorazowo ustalić, jaki zakres danych jest rzeczywiście niezbędny do organizacji wymiany i ograniczyć przekazywane informacje do tego zakresu, informując jednocześnie studenta o warunkach transferu jego danych za granicę.

8.8. Monitoring wizyjny

Obecnie większość uczelni stosuje monitoring wizyjny na swoim terenie, w tym w budynkach dydaktycznych, bibliotekach czy domach studenckich, w celu zapewnienia bezpieczeństwa osób i mienia. Podstawą takiego przetwarzania jest zazwyczaj art. 6 ust. 1 lit. e RODO w związku z przepisami wewnętrznymi uczelni określającymi cele i zasady stosowania monitoringu. Nagrania z monitoringu stanowią dane osobowe, jeżeli umożliwiają identyfikację studenta, a ich wykorzystywanie - w tym udostępnianie - powinno być ograniczone wyłącznie do celu, dla którego monitoring został wprowadzony. Nagrania powinny być przechowywane przez czas nie dłuższy niż jest to niezbędne, chyba że stanowią dowód w toczącym się postępowaniu. Studenci powinni zostać poinformowani o stosowaniu monitoringu, jego zasięgu oraz celu za pomocą odpowiednich oznaczeń oraz klauzuli informacyjnej.

8.9. Komunikacja elektroniczna i poczta e-mail

Studiowanie wiąże się z intensywną komunikacją pomiędzy uczelnią a studentami, co powoduje, że poczta elektroniczna stanowi jedno z podstawowych narzędzi przetwarzania danych osobowych. Warto zatem aby proces ten nie naruszał ochrony danych osobowych studentów. Częstym naruszeniem ochrony danych osobowych jest wysyłanie wiadomości do wielu studentów z ujawnieniem adresów e-mail w polu DO lub DW zamiast UDW. W zależności od kontekstu sam adres e-mail może ujawniać przynależność do określonej grupy, kierunku, roku, sprawy stypendialnej, postępowania dyscyplinarnego albo wsparcia psychologicznego. Uczelnia w tym zakresie powinna szkolić pracowników, stosować listy dystrybucyjne, systemy mailingowe i domyślne ustawienia ograniczające ryzyko ujawnienia danych.

8.10. Systemy informatyczne i platformy e-learningowe

Systemy informatyczne wykorzystywane przez uczelnie, takie jak USOS, platformy e-learningowe czy systemy obsługi dziekanatów, służą do przetwarzania szerokiego zakresu danych osobowych studentów. Obejmują one nie tylko dane identyfikacyjne i informacje o przebiegu studiów, w tym uzyskane oceny, lecz także dane dotyczące aktywności użytkowników, historię logowań, przesyłane pliki, treść komunikacji, wyniki testów, komentarze prowadzących oraz dane techniczne związane z korzystaniem z systemu. Do najistotniejszych zagrożeń związanych z wykorzystywaniem tych systemów należą w szczególności: nadmiernie szerokie uprawnienia użytkowników, brak okresowych przeglądów kont i dostępów, nieaktualne lub niewłaściwie zabezpieczone hasła, błędna konfiguracja dostępu do kursów i zasobów, możliwość pobierania plików przez osoby nieuprawnione, dokonywanie zbyt szerokich eksportów danych, a także brak odpowiednich umów powierzenia przetwarzania danych z zewnętrznymi dostawcami usług.

8.11. Systemy antyplagiatowe i repozytoria prac dyplomowych

Zgodnie z przepisami PSWiN uczelnie są obowiązane sprawdzać prace dyplomowe z wykorzystaniem Jednolitego Systemu Antyplagiatowego przed egzaminem dyplomowym, a także przekazywać prace do Ogólnopolskiego Repozytorium Pisemnych Prac Dyplomowych. Procesy te wiążą się z przetwarzaniem danych osobowych autora pracy oraz treści samej pracy, która może zawierać dane osobowe osób trzecich, jeżeli praca oparta jest na badaniach z ich udziałem (zob. rozdział 10.7). Administratorem danych przetwarzanych w tych systemach jest w odpowiednim zakresie minister właściwy do spraw szkolnictwa wyższego, natomiast uczelnia pozostaje administratorem danych w zakresie własnej dokumentacji dotyczącej procesu dyplomowania. Student przygotowujący pracę dyplomową powinien zostać poinformowany o obowiązku poddania jej kontroli antyplagiatowej oraz o zasadach przechowywania pracy w repozytorium.

8.12. Nagrywanie zajęć i egzaminów zdalnych

Prowadzenie zajęć i egzaminów w formie zdalnej częstokroć wiąże się z nagrywaniem obrazu i dźwięku uczestników, co stanowi przetwarzanie ich danych osobowych. Uczelnia powinna z góry określić cel takiego nagrywania (np. weryfikację samodzielności pracy podczas egzaminu, udostępnienie materiału studentom nieobecnym na zajęciach), poinformować o nim uczestników przed rozpoczęciem nagrania oraz zapewnić, aby dostęp do nagrań miały wyłącznie osoby uprawnione, a nie każda osoba dysponująca linkiem do materiału. Nagrania powinny być usuwane

niezwłocznie po ustaniu celu, dla którego zostały sporządzone, chyba że stanowią element dokumentacji przebiegu egzaminu wymagany odrębnymi przepisami.

8.13. Działalność promocyjna uczelni

Wykorzystywanie wizerunku, wypowiedzi lub osiągnięć studentów w materiałach promocyjnych uczelni - na stronie internetowej, w mediach społecznościowych czy materiałach rekrutacyjnych - stanowi przetwarzanie danych osobowych wymagające odrębnej, zazwyczaj dobrowolnej podstawy prawnej w postaci zgody studenta (zob. rozdział 5.3). Zgoda ta powinna być odrębna od innych zgód i klauzul, a jej zakres - w tym czas wykorzystywania materiału oraz kanały jego publikacji - jasno określony. Wykorzystanie wizerunku pozostaje ponadto pod odrębną regulacją prawa autorskiego, w szczególności art. 81 ustawy o prawie autorskim i prawach pokrewnych, zgodnie z którym rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. Studentowi przysługuje możliwość wycofania zgody na wykorzystywanie jego danych w materiałach promocyjnych w każdym czasie, co powinno skutkować zaprzestaniem dalszego rozpowszechniania materiału w zakresie, w jakim jest to możliwe.

9. Naruszenia ochrony danych osobowych w działalności uczelni

9.1. Pojęcie naruszenia ochrony danych osobowych

Nieprawidłowe przetwarzanie danych osobowych może prowadzić do naruszenia ochrony danych osobowych, które zostało zdefiniowane w rozdziale 2.7. Może do niego dojść zarówno przez przypadek, jak i w wyniku celowego działania. Dla stwierdzenia naruszenia ochrony danych osobowych nie jest konieczne wykazanie, że osoby fizyczne rzeczywiście poniosły szkodę lub inne negatywne konsekwencje - wystarczające jest samo wystąpienie zdarzenia, które mogło narazić prawa lub wolności osób fizycznych na ryzyko.

9.2. Ocena ryzyka dla praw i wolności studentów

Uczelnia jako administrator danych ma obowiązek rzetelnie ocenić charakter naruszenia, zakres ujawnionych informacji oraz możliwe konsekwencje dla osób, których dane dotyczą. Należy przy tym podkreślić, że obowiązek reakcji po stronie administratora powstaje już wtedy, gdy naruszenie może prowadzić do ryzyka naruszenia praw lub wolności osób fizycznych - nie jest zatem konieczne wykazanie, że dane zostały rzeczywiście wykorzystane przez osoby nieuprawnione. W realiach funkcjonowania uczelni ma to szczególne znaczenie przy organizacji egzaminów zdalnych,

nagrywaniu zajęć, weryfikacji tożsamości studentów oraz udostępnianiu materiałów na platformach e-learningowych.

9.3. Zgłoszenie naruszenia Prezesowi UODO

Zgodnie z art. 33 RODO administrator, który stwierdził naruszenie ochrony danych osobowych mogące skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, jest obowiązany zgłosić je Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin od stwierdzenia naruszenia. Zgłoszenie powinno zawierać opis charakteru naruszenia, kategorie i przybliżoną liczbę osób, których dane dotyczą, opis możliwych konsekwencji naruszenia oraz opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu. Niedopełnienie tego obowiązku, jak pokazuje sprawa omówiona w rozdziale 9.7, może samodzielnie stanowić podstawę nałożenia administracyjnej kary pieniężnej, niezależnie od oceny samego naruszenia.

9.4. Zawiadomienie osób, których dane dotyczą

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator jest dodatkowo obowiązany, na podstawie art. 34 RODO, zawiadomić bez zbędnej zwłoki osoby, których dane dotyczą. Zawiadomienie powinno być sformułowane jasnym i prostym językiem oraz opisywać charakter naruszenia, a także zawierać informacje analogiczne do tych przekazywanych Prezesowi UODO, w tym zalecane środki minimalizujące potencjalne negatywne skutki. Obowiązek ten nie powstaje, jeżeli administrator wdrożył odpowiednie środki zabezpieczające dane objęte naruszeniem lub podjął działania eliminujące wysokie ryzyko.

9.5. Dokumentowanie naruszeń

Niezależnie od obowiązku zgłoszenia naruszenia Prezesowi UODO administrator jest obowiązany dokumentować wszystkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze (art. 33 ust. 5 RODO). Dokumentacja ta powinna umożliwiać Prezesowi UODO weryfikację przestrzegania tego przepisu i stanowi element realizacji zasady rozliczalności. W praktyce uczelnie powinny prowadzić wewnętrzny rejestr incydentów i naruszeń, obejmujący również zdarzenia, które - po przeprowadzeniu oceny ryzyka - nie zostały zgłoszone Prezesowi UODO, wraz z uzasadnieniem takiej decyzji.

9.6. Przykłady najczęstszych naruszeń w uczelniach



Do najczęstszych naruszeń ochrony danych osobowych w działalności uczelni należą: wysyłanie korespondencji do grupy studentów z ujawnieniem adresów e-mail w polu DO lub DW zamiast UDW, pozostawianie list z ocenami lub wynikami rekrutacji w miejscach ogólnodostępnych, przechowywanie danych studentów na prywatnych urządzeniach pracowników bez odpowiednich zabezpieczeń, udostępnianie nagrań z zajęć lub egzaminów zdalnych bez ograniczenia dostępu do uprawnionych osób, a także błędna konfiguracja uprawnień w systemach informatycznych uczelni, umożliwiającą dostęp do danych osobom nieuprawnionym. Wspólną cechą tych zdarzeń jest to, że wynikają one najczęściej nie z celowego działania, lecz z niedopatrzenia, braku odpowiednich procedur lub niedostatecznego przeszkolenia pracowników - co nie zwalnia jednak uczelni jako administratora z odpowiedzialności za ich wystąpienie.

9.7. Sprawa Uniwersytetu w G.⁹

Sprawa dotyczyła udostępnienia nagrania z przebiegu egzaminów praktycznych. Studenci przystępujący do egzaminu zostali w większości wylegitymowani za okazaniem legitymacji studenckiej lub dowodu osobistego, co zostało zapisane na nagraniu. Studenci nie wiedzieli, że nagrania z tego procesu będą następnie udostępnione na platformie online. Co istotniejsze, dostęp do nich był również możliwy bez wcześniejszego logowania. Prezes UODO na podstawie przesłanych zgłoszeń wszczął postępowanie w tej sprawie i zwrócił się do uczelni z prośbą o wyjaśnienie. Uczelnia w odpowiedzi na pismo Prezesa UODO nie dopatrzyła się konieczności zgłoszenia zaistniałej nieprawidłowości do organu nadzoru i poinformowania studentów o zaistniałym naruszeniu. Wobec powyższego Prezes UODO nałożył na uczelnię karę w wysokości 25 000 złotych za naruszenie ochrony danych osobowych (decyzja Prezesa UODO, znak DKN.5131.6.2020). Zobowiązał również uczelnię do poinformowania o naruszeniu wszystkich osób, których dane stały się ofiarą, czego uczelnia wcześniej nie uczyniła. Zdaniem organu nadzoru działanie uczelni spowodowało wysokie ryzyko dla praw lub wolności studentów.

Uczelnia zaskarżyła decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie, który w swoim orzeczeniu nie podzielił argumentacji uczelni i oddalił skargę. Sąd wskazał, że dla powstania obowiązku zgłoszenia naruszenia i zawiadomienia osób, których dane dotyczą, nie trzeba czekać na materializację szkody, wystarczy samo ryzyko naruszenia praw lub wolności. Następnie sprawa trafiła do Naczelnego Sądu Administracyjnego. NSA oddalił skargę kasacyjną i podtrzymał stanowisko Prezesa UODO. Sąd zaakcentował, że ocena ryzyka należy do administratora, ale jeśli administrator oceni ryzyko błędnie, może wtedy ponosić odpowiedzialność. NSA wskazał też, że Prezes UODO jako

⁹ Nazwa uczelni została celowo zanonimizowana w sposób analogiczny do tego zastosowanego w decyzji Prezesa UODO, znak DKN.5131.6.2020.

wyspecjalizowany organ nie musiał w tej sprawie powoływać biegłego do oceny, czy dane z nagrań mogły być możliwe do odczytania.

Powyższa sprawa dobrze pokazuje, że w razie incydentu dotyczącego danych osobowych uczelnia nie może poprzestać na ogólnym założeniu, że brak jest dowodów na wyrządzenie szkody albo faktyczne wykorzystanie danych studentów – jak wskazano w rozdziale 9.2, ocena ryzyka musi być przeprowadzona rzetelnie, zanim administrator podejmie decyzję o niezgłaszaniu naruszenia.

9.8. Sprawa Y. w B.¹⁰

Pracownik naukowy uczelni, pełniący jednocześnie funkcję sekretarza uczelnianej komisji rekrutacyjnej, w ramach udzielonego mu upoważnienia do przetwarzania danych systematycznie pobierał z uczelnianego systemu obsługi kandydatów dane osób ubiegających się o przyjęcie na studia (m.in. imiona i nazwiska, numer PESEL, adres zamieszkania, serię i numer dokumentu tożsamości) i zapisywał je na swoim prywatnym komputerze, wykorzystywanym zarówno do celów służbowych, jak i prywatnych. Komputer ten został skradziony, w wyniku czego doszło do naruszenia ochrony danych obejmującego - jak ustalono w toku postępowania - dane nawet około 100 tys. kandydatów na studia z ostatnich pięciu lat. Uczelnia sama zgłosiła zdarzenie Prezesowi UODO. Organ nadzorczy, po przeprowadzeniu postępowania, stwierdził brak należytego nadzoru nad procesem przetwarzania oraz niewystarczającą ocenę zastosowanych środków technicznych i organizacyjnych, i nałożył na uczelnię jako administratora danych karę w wysokości 50 tys. złotych, uwzględniając przy jej wymiarze m.in. dobrą współpracę uczelni z organem oraz wdrożenie działań naprawczych.

Decyzję tę uczelnia zaskarżyła do WSA w Warszawie (sygn. akt II SA/Wa 2129/20), podnosząc, że to pracownik powinien być uznany za administratora danych skopiowanych na prywatny nośnik, ponieważ działał bez wiedzy i zgody pracodawcy, z naruszeniem wewnętrznych regulacji bezpieczeństwa. WSA nie podzielił tej argumentacji, wskazując, że w stosunkach zewnętrznych działania pracownika są działaniami pracodawcy, który ponosi za nie odpowiedzialność, zachowując jedynie wewnętrzny regres wobec pracownika. Sprawa trafiła następnie do Naczelnego Sądu Administracyjnego, który 7 lutego 2025 r. oddalił skargę kasacyjną uczelni (sygn. akt III OSK 6801/21). NSA podkreślił, że autonomiczne pojęcie administratora danych z RODO obejmuje podmiot, który samodzielnie lub wspólnie z innymi ustala cele przetwarzania - pracownik wykonujący czynności przetwarzania w ramach udzielonego upoważnienia, nawet jeśli przekroczył jego granice, celu tego przetwarzania samodzielnie nie ustalał, w związku z czym nie stał się przez to odrębnym administratorem. Zdaniem NSA to uczelnia jako administrator powinna była sprawować pełną

¹⁰ Nazwa uczelni została celowo zanonimizowana w sposób analogiczny do tego zastosowanego w decyzji Prezesa UODO, znak ZSOŚS.421.25.2019.

kontrolę nad tym, w jaki sposób dane mogą być przenoszone z jej systemów informatycznych na inne nośniki, a brak takiego nadzoru przesądził o jej odpowiedzialności.

10. Ochrona danych osobowych w badaniach naukowych i wypowiedzi akademickiej

Odrębnym zagadnieniem, powiązaniem z wcześniej omówionymi podstawami przetwarzania danych studentów, jest zakres obowiązków RODO w sytuacji, gdy przetwarzanie następuje w związku z prowadzeniem badań naukowych, pracami rozwojowymi lub tzw. wypowiedzią akademicką. RODO w art. 85 i art. 89 pozostawia państwom członkowskim możliwość wprowadzenia w prawie krajowym odrębnych, węższych obowiązków administratora w tych obszarach, o ile jest to konieczne do pogodzenia ochrony danych osobowych z wolnością wypowiedzi, informacji oraz wolnością nauki. Ustawodawca polski skorzystał z tej możliwości w PSWiN, przewidując dwa odrębne reżimy: dla wypowiedzi akademickiej oraz dla badań naukowych i prac rozwojowych. Rozróżnienie to ma praktyczne znaczenie także dla studentów, którzy mogą występować w tych procesach zarówno jako osoby, których dane dotyczą (np. gdy wykładowca odwołuje się w publikacji do przykładu z zajęć), jak i jako podmioty samodzielnie prowadzące badania w ramach pracy dyplomowej.

10.1. Pojęcie wypowiedzi akademickiej

PSWiN nie definiuje wprost pojęcia „wypowiedzi akademickiej”, w związku z czym przyjmuje się jego szerokie, funkcjonalne rozumienie. W praktyce przyjmuje się, że mieści się w nim każda forma aktywności naukowej związana z prowadzeniem badań, upowszechnianiem ich rezultatów czy działalnością dydaktyczną, bez względu na to, w jakiej formie, gdzie i w jaki sposób została wyrażona.¹¹ Podstawą takiego ujęcia jest wolność nauczania, prowadzenia badań naukowych i ogłaszania ich wyników (art. 4 ust. 1–3 PSWiN), z której korzystają m.in. nauczyciele akademicy. Ilustruje to orzecznictwo Europejskiego Trybunału Praw Człowieka, który telewizyjny wywiad udzielony przez profesora uczelni, dotyczący jego pracy badawczej, zakwalifikował właśnie jako wypowiedź akademicką¹². Pojęcie to nie obejmuje natomiast całej działalności uczelni. Nie mieści się w nim np. prowadzenie akt osobowych studentów czy obsługa procesu rekrutacyjnego, które podlegają ogólnym zasadom RODO omówionym w rozdziałach poprzedzających¹³.

¹¹ N. Zawadzka [w:] MERITUM. Ochrona danych osobowych, red. D. Lubasz, Warszawa 2020, rozdział VII, s. 943–944.

¹² Wyrok ETPC z dnia 19 czerwca 2018 r. w sprawie 20233/06, Kula przeciwko Turcji, <https://hudoc.echr.coe.int> [dostęp: 2.08.2026 r.].

¹³ N. Zawadzka, op. cit., s. 944.

10.2. Zakres ograniczeń obowiązków wynikających z RODO

W odniesieniu do wypowiedzi akademickiej ustawodawca przewidział zwolnienie o zauważalnie węższym zakresie niż to, które dotyczy wypowiedzi dziennikarskich, literackich i artystycznych. Do przetwarzania danych w ramach wypowiedzi akademickiej stosuje się niemal wszystkie przepisy RODO, w tym zasady podstawowe z art. 5, podstawy prawne przetwarzania z art. 6 i 9, obowiązki administratora w zakresie bezpieczeństwa danych czy przepisy o transferze danych poza Europejski Obszar Gospodarczy. Wyłączeniu podlegają jedynie: obowiązek informacyjny przy zbieraniu danych bezpośrednio od osoby (art. 13), niektóre elementy prawa dostępu (art. 15 ust. 3 i 4), prawo do ograniczenia przetwarzania (art. 18), obowiązek wyznaczenia przedstawiciela przez administratorów spoza Unii Europejskiej (art. 27), część obowiązków podmiotu przetwarzającego (art. 28 ust. 2–10) oraz obowiązek rejestrowania czynności przetwarzania (art. 30)¹⁴. Jak uzasadnia N. Zawadzka wyłączenie obowiązku informacyjnego uzasadnia się względami praktycznymi - w przypadku otwartych wykładów czy zajęć dla szerokiego grona słuchaczy realizacja pełnego obowiązku z art. 13 wobec każdego uczestnika byłaby nieproporcjonalnym obciążeniem, niewspółmiernym do niewielkiego ryzyka dla praw osób, które z reguły znają cel i okoliczności zbierania swoich danych. Z kolei wyłączenie prawa do ograniczenia przetwarzania ma zapobiegać sytuacji, w której realizacja tego prawa prowadziłaby do zniekształcenia materiału źródłowego wykorzystywanego w pracy naukowej lub dydaktycznej.¹⁵ Nie oznacza to jednak, że pozostałe prawa studentów - w tym prawo do sprostowania, usunięcia danych czy sprzeciwu - doznają w tym kontekście ograniczenia; podlegają one ochronie na zasadach ogólnych.

10.3. Przetwarzanie danych do celów badań naukowych i prac rozwojowych

Odrębną podstawę przetwarzania stanowią przepisy art. 469a i 469b PSWiN, dotyczące danych przetwarzanych do celów badań naukowych i prac rozwojowych. „Badania naukowe” obejmują zarówno badania podstawowe - prace empiryczne lub teoretyczne nastawione na zdobywanie nowej wiedzy o podstawach zjawisk, bez nastawienia na bezpośrednie zastosowanie komercyjne, jak i badania aplikacyjne - nastawione na opracowywanie nowych produktów, procesów lub usług (art. 4 ust. 2 PSWiN). Do „prac rozwojowych” zalicza się natomiast nabywanie, łączenie i wykorzystywanie dostępnej wiedzy i umiejętności do planowania oraz tworzenia nowych lub ulepszonych produktów, procesów i usług, z wyłączeniem rutynowych i okresowych zmian (art. 4 ust. 3 PSWiN).

¹⁴ Ibidem, s. 945.

¹⁵ Ibidem, s. 944–945.

10.4. Szczególne kategorie danych w badaniach naukowych

W zakresie niezbędnym do prowadzenia badań naukowych lub prac rozwojowych dopuszczalne jest przetwarzanie danych osobowych należących do szczególnych kategorii w rozumieniu art. 9 RODO, a więc m.in. danych o zdrowiu, pochodzeniu etnicznym czy przekonaniach. Stanowi to samodzielny wyjątek od ogólnego zakazu przetwarzania takich danych, oparty na art. 9 ust. 2 lit. j RODO w związku z art. 89 ust. 1 RODO oraz rozwijających je przepisach PSWiN. Warunkiem jest jednak, aby publikowanie wyników badań następowało w sposób uniemożliwiający identyfikację osób, których dane zostały przetworzone, a dane - niezwłocznie po osiągnięciu celu badawczego - zostały poddane anonimizacji¹⁶ (zob. rozdział 10.6). Regulacja ta ma bezpośrednie znaczenie dla studentów i doktorantów przygotowujących prace dyplomowe lub rozprawy doktorskie oparte na własnych badaniach empirycznych (np. ankietach czy wywiadach przeprowadzanych wśród innych studentów), ponieważ krąg podmiotów uprawnionych do korzystania z tego wyłączenia obejmuje - obok uczelni, instytutów naukowych Polskiej Akademii Nauk, instytutów badawczych i Centrum Łukasiewicz - również osoby przygotowujące pracę dyplomową lub rozprawę doktorską wymaganą do uzyskania dyplomu ukończenia studiów lub stopnia naukowego.¹⁷

10.5. Ograniczenia praw osób, których dane dotyczą

Art. 469b PSWiN - będący realizacją upoważnienia z art. 89 ust. 2 RODO - pozwala wyłączyć wobec przetwarzania danych do celów badań naukowych i prac rozwojowych stosowanie prawa dostępu (art. 15), prawa do sprostowania (art. 16), prawa do ograniczenia przetwarzania (art. 18) oraz prawa do sprzeciwu (art. 21). Ustawodawca uzależnił to wyłączenie od spełnienia dwóch przesłanek łącznie: musi zachodzić prawdopodobieństwo, że korzystanie z tych praw uniemożliwiłoby lub istotnie utrudniło osiągnięcie celu badawczego, a samo wyłączenie musi być niezbędne do jego realizacji. Zakres tego zwolnienia różni się od omówionego wyżej zwolnienia dotyczącego wypowiedzi akademickiej - w przypadku badań naukowych i prac rozwojowych ustawodawca nie wyłączył ani obowiązku informacyjnego z art. 13 RODO, ani obowiązku rejestrowania czynności przetwarzania z art. 30 RODO. Krąg podmiotów mogących skorzystać z tego wyłączenia jest przy tym węższy niż ogólny krąg administratorów - obejmuje wyłącznie uczelnie, instytuty naukowe Polskiej Akademii Nauk, instytuty badawcze, międzynarodowe instytuty naukowe, Centrum Łukasiewicz wraz z instytutami Sieci Łukasiewicz oraz Polską Akademię Umiejętności, a także - jak wskazano wyżej - osoby przygotowujące pracę dyplomową lub rozprawę doktorską.¹⁸

¹⁶ Ibidem s. 947.

¹⁷ Ibidem s. 946–947.

¹⁸ Ibidem s. 947.

10.6. Pseudonimizacja i anonimizacja danych

Pseudonimizacja oraz anonimizacja danych stanowią kluczowe środki ograniczające ryzyko związane z przetwarzaniem danych do celów badań naukowych. Pseudonimizacja, zdefiniowana w art. 4 pkt 5 RODO, polega na przetworzeniu danych w taki sposób, by nie można ich było już przypisać konkretnej osobie bez użycia dodatkowych informacji, przechowywanych oddzielnie i zabezpieczonych - dane spseudonimizowane pozostają jednak danymi osobowymi w rozumieniu RODO. Anonimizacja natomiast polega na takim przekształceniu danych, które trwale uniemożliwia identyfikację osoby, także przy użyciu wszelkich rozsądnie dostępnych środków - dane w pełni zanonimizowane nie podlegają już przepisom RODO. W kontekście badań naukowych prowadzonych przez studentów i pracowników uczelni istotne jest, aby publikacja wyników następowała dopiero po anonimizacji danych uczestników badania, chyba że wyrazili oni wyraźną zgodę na ujawnienie swojej tożsamości, a materiał roboczy zawierający dane umożliwiające identyfikację był zabezpieczony i usuwany niezwłocznie po osiągnięciu celu badawczego.

10.7. Student i doktorant jako osoba prowadząca badania

Student występuje w opisanych wyżej procesach nie tylko jako osoba, której dane dotyczą, lecz sam jako podmiot przetwarzający dane innych osób, na którym spoczywają obowiązki wynikające z ochrony danych osobowych, w tym w zakresie odpowiedniego zabezpieczenia danych (pseudonimizacji lub szyfrowania) oraz ograniczenia dostępu do zebranego materiału. Ma to szczególne znaczenie w przypadku przygotowywania artykułów naukowych, prac dyplomowych i rozpraw doktorskich opartych na badaniach empirycznych prowadzonych wśród innych studentów lub osób trzecich, ponieważ to student lub doktorant, a nie uczelnia, decyduje wówczas samodzielnie o sposobie zbierania, przechowywania i wykorzystania zebranych danych, co czyni go administratorem danych osobowych w tym zakresie.

10.8. Wykorzystywanie prac i wypowiedzi studentów

Odrębnym zagadnieniem jest wykorzystywanie przez nauczycieli akademickich prac, wypowiedzi lub przykładów pochodzących od studentów w publikacjach naukowych, podręcznikach czy materiałach dydaktycznych. Jeżeli materiał taki został odpowiednio zanonimizowany - tak, aby nie było możliwe powiązanie go z konkretnym studentem - jego wykorzystanie pozostaje poza zakresem RODO. Jeżeli natomiast student pozostaje możliwy do zidentyfikowania, np. poprzez cytowanie fragmentu jego pracy zaliczeniowej wraz z imieniem i nazwiskiem, konieczne jest ustalenie właściwej podstawy prawnej takiego przetwarzania - w praktyce najczęściej będzie to zgoda studenta, o ile wykorzystanie materiału wykracza poza to, co niezbędne do realizacji zadań dydaktycznych uczelni.

Niezależnie od wymogów RODO takie wykorzystanie podlega także ograniczeniom wynikającym z prawa autorskiego, jeżeli praca studenta stanowi utwór w rozumieniu ustawy o prawie autorskim i prawach pokrewnych.

11. Samorząd studencki a ochrona danych osobowych

11.1. Status prawny samorządu studenckiego

W polskim systemie szkolnictwa wyższego status prawny samorządu studenckiego regulują przepisy PSWiN. Zgodnie z art. 110 ust. 1 tej ustawy samorząd studencki tworzą wszyscy studenci danej uczelni, co oznacza, że jego członkiem jest z mocy prawa każdy student tej uczelni. Ustawa przyznaje samorządowi status wyłącznego reprezentanta ogółu studentów danej instytucji. Samorząd studencki działa przez swoje organy, w tym przewodniczącego oraz organ uchwałodawczy (art. 110 i n. PSWiN).

Z punktu widzenia dogmatyki prawa cywilnego samorząd studencki nie posiada osobowości prawnej ani tzw. ułomnej osobowości prawnej - nie jest więc odrębnym od uczelni podmiotem prawa cywilnego, mogącym we własnym imieniu nabywać prawa i zaciągać zobowiązania. Funkcjonuje on w strukturze uczelni, która ma ustawowy obowiązek zapewnienia warunków niezbędnych do jego działania, w tym infrastruktury oraz środków finansowych, którymi samorząd dysponuje w ramach swojej działalności (art. 110 ust. 4–5 PSWiN). To szczególne powiązanie z uczelnią ma istotne znaczenie dla oceny statusu samorządu na gruncie RODO, ponieważ - jak wskazano w rozdziale 11.3 - ustalenie, kto jest administratorem danych, nie może opierać się wyłącznie na deklaracyjnych oświadczeniach samego samorządu, lecz wymaga zbadania, kto w rzeczywistości i w sposób wiążący decyduje o celach oraz sposobach przetwarzania. Jednocześnie samorząd nie jest organem uczelni w ścisłym znaczeniu tego pojęcia - jest ustawowo wyodrębnioną formą reprezentacji wspólnoty studentów, posiadającą własne demokratycznie wyłaniane organy oraz kompetencje wynikające z ustawy i regulaminu samorządu. W doktrynie i praktyce nie ma zgody co do jednolitej kwalifikacji tej pozycji. Kwestię tę należy zatem rozstrzygać odrębnie dla każdego konkretnego procesu przetwarzania danych, a nie w sposób generalny dla całej działalności samorządu.

11.2. Samorząd jako część uczelni

Punktem wyjścia do analizy powinno być założenie, że w typowej działalności samorządu to uczelnia pozostaje administratorem danych osobowych, a organy samorządu - działając w ramach uczelni - przetwarzają dane jako część jej struktury organizacyjnej, a nie jako odrębny, samodzielny podmiot. Ten model znajduje zastosowanie przede wszystkim tam, gdzie działalność członków

samorządu jest ściśle powiązana z realizacją zadań ustawowych uczelni - np. udziałem przedstawicieli studentów w postępowaniach dotyczących przyznawania świadczeń, w komisjach dyscyplinarnych czy w organach kolegialnych uczelni (zob. rozdział 11.8) - a samorząd nie dysponuje przy tym własną, niezależną infrastrukturą techniczną ani organizacyjną do przetwarzania danych. W takim ujęciu uczelnia jest bez wątpienia administratorem danych osobowych w odniesieniu do systemowych procesów kształcenia, czy przyznawania świadczeń socjalnych z funduszu stypendialnego - przetwarzanie to opiera się na wypełnieniu obowiązku prawnego ciążącego na uczelni w związku z przepisami PSWiN, niezależnie od tego, czy w danym procesie biorą udział również przedstawiciele samorządu.

Za przyjęciem uczelni jako administratora w tych procesach przemawia dodatkowo argumentacja zbliżona do tej, którą Naczelny Sąd Administracyjny przedstawił w sprawie opisywanego wyżej naruszenia (zob. rozdział 9.8) – sam fakt wykonywania czynności przetwarzania przez osobę fizyczną lub gremium działające w ramach struktury organizacyjnej administratora nie czyni tej osoby lub gremium odrębnym administratorem, jeżeli to nie ona, lecz podmiot nadrzędny, ustala cel przetwarzania i ponosi za nie odpowiedzialność instytucjonalną. Analogicznie, udział przedstawicieli samorządu w gremiach działających na podstawie kompetencji przyznanych przez PSWiN nie powoduje sam przez się powstania po stronie samorządu odrębnej podmiotowości administratora danych.

11.3. Samorząd jako potencjalny administrator danych

Przepisy RODO określają administratora danych osobowych jako osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Definicja ta ma charakter autonomiczny i funkcjonalny wobec krajowych przepisów o osobowości prawnej, co oznacza, że dla jej zastosowania nie jest konieczne posiadanie osobowości prawnej - decydujące jest kryterium faktyczne, czyli realny i samodzielny wpływ na decydowanie o celach oraz sposobach i środkach przetwarzania. Brak osobowości prawnej samorządu studenckiego, o którym mowa w rozdziale 11.1, nie wyklucza więc *a priori* uznania go za administratora w rozumieniu RODO.

Należy jednak zachować ostrożność przy automatycznym przypisywaniu samorządowi tego statusu. Sam fakt, że dany podmiot posługuje się w swojej polityce prywatności sformułowaniem, iż jest „administratorem danych osobowych”, nie przesądza jeszcze o rzeczywistym istnieniu tej roli w rozumieniu art. 4 pkt 7 RODO - ocena ta ma charakter obiektywny i musi być każdorazowo zweryfikowana w oparciu o to, kto faktycznie i samodzielnie ustala cel oraz sposób przetwarzania danego zbioru danych, a nie w oparciu o treść jednostronnej deklaracji zamieszczonej w dokumencie

o charakterze informacyjnym. Wskazać przy tym należy, że polityki prywatności publikowane przez poszczególne organy samorządów studenckich bywają w tym zakresie niejednolite i nie zawsze odzwierciedlają prawidłową kwalifikację prawną - z tego względu nie powinny stanowić samodzielnej i wystarczającej podstawy do formułowania ogólnych wniosków co do statusu samorządu studenckiego jako administratora danych.

Niezależnie od powyższego zastrzeżenia, w określonych, wyodrębnionych procesach przetwarzania samorząd studencki może zostać uznany za administratora danych, jeżeli organy samorządu samodzielnie i niezależnie od struktur administracyjnych uczelni decydują o celu oraz sposobach przetwarzania danych, a uczelnia nie ma na te decyzje rzeczywistego wpływu. Dotyczy to w szczególności działalności organizacyjnej wykraczającej poza zadania ustawowe uczelni, np. samodzielnie organizowanych przez samorząd wydarzeń kulturalnych lub rozrywkowych (zob. rozdział 11.6) czy prowadzenia własnych kanałów komunikacji z uczestnikami tych wydarzeń (zob. rozdział 11.7), o ile samorząd dysponuje w tym zakresie własnymi narzędziami i faktycznie samodzielnie podejmuje decyzje co do zbieranych danych, sposobu ich przechowywania oraz zabezpieczenia. Przykładem deklarowanego przyjęcia takiej roli jest polityka prywatności Samorządu Studenckiego Politechniki Śląskiej dotycząca organizacji projektu „Igrzy”¹⁹; podkreślić jednak trzeba, że taka deklaracja stanowi jedynie punkt wyjścia do oceny, a nie jej ostateczne potwierdzenie - decydujące znaczenie ma to, czy w praktyce to organy samorządu, a nie uczelnia, faktycznie kontrolują dany proces przetwarzania.

11.4. Współadministrowanie przez uczelnię i samorząd

Pomiędzy skrajnymi modelami opisanymi w rozdziałach 11.2 i 11.3 mieści się sytuacja, w której uczelnia i samorząd studencki wspólnie ustalają cele i sposoby przetwarzania danych osobowych, co - zgodnie z art. 26 RODO - prowadzi do powstania współadministrowania. Model ten wydaje się szczególnie adekwatny dla wielu typowych sytuacji z praktyki akademickiej, w których trudno jednoznacznie przypisać wyłączną kontrolę nad przetwarzaniem jednej ze stron np. przy wspólnie organizowanym wydarzeniu łączącym cele instytucjonalne uczelni (promocja, integracja studentów) z operacyjną realizacją przez organy samorządu. Współadministrowanie powstaje wówczas, gdy oba podmioty w sposób rzeczywisty i uzgodniony współdecydują o danym procesie przetwarzania - nie jest do tego wystarczające samo współistnienie dwóch podmiotów przy tej samej czynności faktycznej, jeżeli jeden z nich nie ma żadnego wpływu na ustalenie celów lub sposobów przetwarzania.

Współadministratorzy są obowiązani, w drodze przejrzystego uzgodnienia (art. 26 ust. 1 RODO), określić zakres swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających

¹⁹<https://igry.polsl.pl/privacy-policy/> [dostęp: 2.08.2026 r.].

z RODO, w tym w szczególności podział zadań związanych z realizacją obowiązku informacyjnego oraz obsługą praw osób, których dane dotyczą, a także wyznaczyć punkt kontaktowy dla osób, których dane dotyczą. Zasadnicza treść tych uzgodnień powinna zostać udostępniona studentom, których dane dotyczą (art. 26 ust. 2 RODO), niezależnie od wewnętrznego podziału ról ustalonego między uczelnią a samorządem. W praktyce oznacza to, że przed rozpoczęciem wspólnie organizowanego przedsięwzięcia uczelnia i samorząd powinny w pierwszej kolejności ustalić, który z trzech opisanych w niniejszym rozdziale modeli - wyłączna administracja uczelni, wyłączna administracja samorządu, czy współadministrowanie - znajduje zastosowanie do konkretnego procesu przetwarzania danych, a dopiero następnie wdrożyć odpowiednie do tego modelu obowiązki.

11.5. Upoważnienia do przetwarzania danych

Aby członkowie organów samorządu mogli legalnie i prawidłowo przetwarzać dane innych studentów w ramach wykonywania swoich zadań w modelu opisanym w rozdziale 11.2, uczelnia powinna udzielić im imiennych upoważnień do przetwarzania danych osobowych. Praktykę tę wdrożyła m.in. Uczelnia Łazarskiego, której regulamin samorządu studenckiego wprost stanowi, że uczelnia jako administrator danych osobowych upoważnia członków samorządu biorących udział w przetwarzaniu danych do wykonywania tych operacji w ramach realizacji zadań statutowych²⁰.

11.6. Organizacja wydarzeń i imprez studenckich

Organizacja wydarzeń studenckich, takich jak juwenalia, wyjazdy adaptacyjne czy bale studenckie, wiąże się zwykle ze zbieraniem danych uczestników za pośrednictwem formularzy zgłoszeniowych – imienia i nazwiska, danych kontaktowych, a niekiedy danych o preferencjach żywieniowych czy stanie zdrowia istotnych dla bezpieczeństwa uczestnika. Samorząd organizujący takie wydarzenie powinien ustalić, czy występuje w roli niezależnego administratora, czy działa w ramach struktury uczelni (zob. rozdziały 11.2–11.3), oraz odpowiednio do tego zrealizować obowiązek informacyjny wobec uczestników. Dane zebrane w celu organizacji wydarzenia powinny zostać usunięte niezwłocznie po jego zakończeniu i rozliczeniu, chyba że ich dalsze przechowywanie jest uzasadnione np. celami rozliczeniowymi lub dochodzeniem roszczeń.

11.7. Listy mailingowe, formularze i zapisy na wydarzenia

Samorząd studencki może przetwarzać dane osobowe w sposób w pełni niezależny od uczelni, na przykład prowadząc listę mailingową studentów, którzy dobrowolnie przekazali swoje adresy

²⁰Regulamin Samorządu Studentów Uczelni Łazarskiego w Warszawie z dnia 22 lutego 2021 r., https://www.lazarski.pl/fileadmin/user_upload/dokumenty/Regulamin_samorządu_studenckiego.pdf [dostęp: 2.08.2026 r.].

e-mail w celu otrzymywania informacji o ofertach, wydarzeniach lub inicjatywach kierowanych do społeczności studenckiej. W takim przypadku właściwą podstawą do przetwarzania danych osobowych powinna być udzielona zgoda.

11.8. Przetwarzanie danych przez komisje stypendialne i dyscyplinarne

Działalność w ramach ruchu studenckiego może wiązać się z dostępem do danych osobowych o szczególnie wrażliwym charakterze, zaliczanych do szczególnych kategorii danych w rozumieniu art. 9 RODO. Sytuacje takie występują przede wszystkim wtedy, gdy studenci uczestniczą w pracach organów lub komisji wykonujących ustawowe zadania uczelni. Przykładem jest opiniowanie i przyznawanie świadczeń dla studentów z niepełnosprawnościami, które wymaga analizy dokumentacji potwierdzającej stan zdrowia lub stopień niepełnosprawności. W takim przypadku to jednak nie samorząd studencki jako organizacja przetwarza te dane, lecz komisja stypendialna działająca jako organ uczelni, wykonujący zadania powierzone jej na podstawie przepisów PSWiN. Student będący członkiem komisji uzyskuje dostęp do danych wyłącznie w zakresie niezbędnym do wykonywania powierzonych obowiązków i jest zobowiązany do zachowania ich poufności. Podobnie sytuacja wygląda w przypadku komisji dyscyplinarnych, w których również zasiadają przedstawiciele studentów. W toku prowadzonych postępowań mogą oni zapoznawać się z informacjami dotyczącymi zdrowia, sytuacji rodzinnej czy innych okoliczności istotnych dla rozstrzygnięcia sprawy. Dostęp ten nie wynika jednak z pełnienia funkcji w samorządzie studenckim, lecz z udziału w organie uczelni realizującym zadania określone przepisami prawa i regulacjami wewnętrznymi.

11.9. Obowiązki informacyjne i bezpieczeństwo danych

Gdy samorząd występuje jako niezależny administrator (zob. rozdział 11.3) lub współadministrator (zob. rozdział 11.4), przejmuje wynikające z RODO obowiązki administratora danych. Oznacza to konieczność samodzielnego określenia celów i podstaw przetwarzania, realizacji obowiązku informacyjnego wobec osób, których dane dotyczą, wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych oraz ustalenia okresów ich przechowywania - analogicznie do obowiązków spoczywających na uczelni jako administratorze (zob. rozdziały 6.1 i 6.2). Samorząd powinien również zapewnić procedury umożliwiające realizację praw osób, których dane dotyczą, w szczególności prawa dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, jeżeli znajdują one zastosowanie w danym przypadku. Istotnym elementem jest także wyznaczenie osoby odpowiedzialnej za kwestie związane z ochroną danych

osobowych lub wskazanie punktu kontaktowego, za pośrednictwem którego studenci będą mogli wykonywać swoje prawa i uzyskiwać informacje dotyczące przetwarzania ich danych.

12. Zakończenie

Ochrona danych osobowych studentów w uczelni stanowi zagadnienie o dużym znaczeniu praktycznym i wielowymiarowym charakterze. Uczelnia, realizując swoje zadania ustawowe, występuje najczęściej jako administrator danych osobowych i jako taka ponosi pełną odpowiedzialność za zgodność przetwarzania z RODO - niezależnie od tego, czy konkretne uchybienie wynika z decyzji jej organów, błędu pracownika, czy nieprawidłowego zabezpieczenia systemu informatycznego, co potwierdzają omówione w opracowaniu decyzje Prezeasa UODO oraz orzeczenia sądów administracyjnych.

Jednocześnie działalność uczelni charakteryzuje się szczególną różnorodnością procesów przetwarzania - od rekrutacji, przez bieżącą obsługę toku studiów i przyznawanie świadczeń, po prowadzenie badań naukowych i działalność samorządu studenckiego - z których każdy wymaga odrębnej analizy podstawy prawnej, zakresu danych oraz zakresu praw przysługujących studentowi. Szczególną uwagę należy zwrócić na obszary graniczne, w których zastosowanie znajdują odrębne, węższe reżimy ochrony - takie jak wypowiedź akademicka czy badania naukowe - oraz na sytuacje, w których to sam student, jako badacz lub członek samorządu, staje się podmiotem odpowiedzialnym za przetwarzanie danych innych osób.

Świadomość tych zależności, zarówno po stronie uczelni, jak i studentów, pozostaje warunkiem koniecznym rzetelnego wypełniania obowiązków wynikających z RODO w środowisku akademickim.

13. Bibliografia

Litwiński P. [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, Warszawa 2021.

Dokowicz M. [w:] Prawo o szkolnictwie wyższym i nauce. Komentarz, red. J. Woźnicki, Warszawa 2019.

Zawadzka N. [w:] MERITUM. Ochrona danych osobowych, red. D. Lubasz, Warszawa 2020.

14. Wykaz aktów prawnych

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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze zm.).

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

Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (tekst jedn. Dz.U. z 2024 r. poz. 1571 ze zm.).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn. Dz.U. z 2022 r. poz. 2509 ze zm.).

15. Wykaz orzecznictwa i decyzji organów nadzorczych

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 19 czerwca 2018 r., skarga nr 20233/06, Kula przeciwko Turcji.

Decyzja Prezesa Urzędu Ochrony Danych Osobowych, znak DKN.5131.6.2020, dotycząca Uniwersytetu w G. – utrzymana w mocy wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie oraz wyrokiem Naczelnego Sądu Administracyjnego oddalającym skargę kasacyjną uczelni.

Wyrok Naczelnego Sądu Administracyjnego z dnia 7 lutego 2025 r., sygn. akt III OSK 6801/21, dotyczący Uczelni w Y. (utrzymujący w mocy wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie, sygn. akt II SA/Wa 2129/20, oraz poprzedzającą je decyzję Prezesa UODO).

Stanowisko Prezesa Urzędu Ochrony Danych Osobowych dotyczące zasad udzielania pomocy materialnej studentom, <https://uodo.gov.pl/pl/674/4215>.

Wyjaśnienia Prezesa Urzędu Ochrony Danych Osobowych dotyczące kierowania studentów na praktyki zawodowe, <https://uodo.gov.pl/pl/675/4225>



Parlament Studentów
Rzeczypospolitej Polskiej



Ministerstwo Nauki
i Szkolnictwa Wyższego

Projekt Studenckie Prawa - Jasna Sprawa finansowany jest ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego



Parlament Studentów
Rzeczypospolitej Polskiej