RAPORT Z BADAŃ

Politechnika Warszawska | Wydział Administracji i Nauk Społecznych

# Przetwarzanie i ochrona danych osobowych w badaniach naukowych i realizacji projektów badawczych

# Обробка та захист персональних даних у наукових дослідженнях та реалізації науково-дослідних проєктів

**Anna Mrozowska-Wyszyńska**
WSB Merito w Poznaniu

**Warszawa / Варшава, 2025**

Politechnika Warszawska | Wydział Administracji i Nauk Społecznych

Ekspertyza opracowana w ramach Projektu MNiSW-PW
pt. „Polsko-ukraińska współpraca instytucji przedstawicielskich reprezentujących rektorów, na rzecz doskonalenia działania uczelni”,
realizowanej z dotacji celowej MNiSW w 2025 r.

Sfinansowano z dotacji Ministerstwa Nauki i Szkolnictwa Wyższego

PARTNER GŁÓWNY

Ministerstwo Nauki i Szkolnictwa Wyższego

PARTNERZY WSPIERAJĄCY

KRASP
Konferencja Rektorów Akademickich Szkół Polskich

Fundacja Rektorów Polskich

PATRONAT

Міністерство освіти і науки України

Politechnika Warszawska | Wydział Administracji i Nauk Społecznych

# PRZETWARZANIE I OCHRONA DANYCH OSOBOWYCH W BADANIACH NAUKOWYCH I REALIZACJI PROJEKTÓW BADAWCZYCH

Warszawa, 2025

*Anna Mrozowska-Wyszyńska, WSB Merito w Poznaniu*

# ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У НАУКОВИХ ДОСЛІДЖЕННЯХ ТА РЕАЛІЗАЦІЇ НАУКОВО-ДОСЛІДНИХ ПРОЄКТІВ

Варшава, 2025

*Анна Мрозовська-Вишинська, WSB Merito в Познані*

Міністерство освіти і науки України | KRASP Konferencja Rektorów Akademickich Szkół Polskich | Fundacja Rektorów Polskich | Ministerstwo Nauki i Szkolnictwa Wyższego

## Spis treści

## PRZETWARZANIE I OCHRONA DANYCH OSOBOWYCH W BADANIACH NAUKOWYCH I REALIZACJI PROJEKTÓW BADAWCZYCH (ekspertyza w języku polskim)

### WSTĘP

Ochrona danych osobowych w europejskim kręgu kulturowym jest traktowana jako jedno z podstawowych praw człowieka. Jako prawo jednostki (prawo do ochrony danych osobowych) jest ona ujęta zarówno w konstytucjach państw europejskich[1], jak i obowiązujących w Europie aktach międzynarodowych oraz w prawie europejskim[2]. Bardziej szczegółowe zasady ochrony tych danych stanowią przedmiot regulacji na poziomie ustawowym. W państwach należących do Unii Europejskiej regulacje te zostały ujednolicone poprzez przyjęcie wspólnego dla całej wspólnoty aktu prawnego - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (dalej RODO), które stosowane jest od 25 maja 2018 r. i odnosi się również do procesów przetwarzania danych osobowych do celów badań naukowych i realizacji projektów badawczych[3]. Należy podkreślić, że dotyczy to zarówno danych osób, które są zatrudnione w ramach danego projektu, jak i

---

[1] Art. 51 Konstytucji Rzeczypospolitej Polskiej, (Dz.U.1997.78.483):
1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

[2] Dwa kluczowe w tym względzie akty to: Konwencja o ochronie praw człowieka i podstawowych wolności (prawo to zostało wyinterpretowane z art. 8 konwencji) oraz Karta Praw Podstawowych Unii Europejskiej (gdzie jest ono wyrażone wprost w art. 8)

[3] Bezpośrednio do kwestii badan naukowych odnosi się motyw 159 RODO: *„Jeżeli dane osobowe są przetwarzane do celów badań naukowych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania. W niniejszym rozporządzeniu przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. Ponadto należy uwzględnić cel Unii określony w art. 179 ust. 1 TFUE, którym jest utworzenie europejskiej przestrzeni badawczej. Wyrażenie „do celów badań naukowych" powinno obejmować także badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego. Z uwagi na specyfikę przetwarzania danych osobowych do celów badań naukowych zastosowanie powinny mieć specjalne warunki, w szczególności w odniesieniu do publikacji lub innego ujawniania danych osobowych w kontekście celów badań naukowych. Jeżeli wynik badań naukowych, w szczególności w kontekście zdrowotnym, uzasadnia dalsze środki w interesie osoby, której dane dotyczą, do środków tych powinny mieć zastosowanie przepisy ogólne niniejszego rozporządzenia".*

osób, które są podmiotem badań, bez względu na to czy informacje o nich są w jakikolwiek sposób rozpowszechniane, np. w ramach publikacji naukowej. Była Grupa Robocza Art. 29 wskazała już, że pojęcia „badania naukowe" nie można rozszerzać poza jego powszechne znaczenie, i jest zdania, że w tym kontekście „badania naukowe" oznaczają „projekt badawczy zorganizowany zgodnie z normami metodycznymi i etycznymi w danym sektorze oraz zgodnie z dobrymi praktykami"[4]. RODO określa m.in. prawne podstawy dopuszczalności przetwarzania danych osobowych, ogólne zasady dotyczące ich przetwarzania, obowiązki spoczywające na administratorach, a także prawa osób, których dane dotyczą. Podmioty prowadzące badania naukowe lub realizujące projekty badawcze, które do tego celu przetwarzają dane osobowe, są zobowiązane do stosowania ogólnego rozporządzenia regulującego m.in. obowiązki ciążące na administratorach, współadministratorach czy podmiotach przetwarzających, w zależności od roli, która jest im w konkretnym przypadku przypisana. Aby zapewnić zgodność z prawem wszelkich działań związanych z przetwarzaniem danych osobowych kluczowym jest by zarówno podmioty prowadzące badania naukowe, jaki i osoby zaangażowane w ich realizację posiadały niezbędną wiedzę w tym zakresie. W szczególności w aspekcie działań o charakterze międzynarodowym, w tym angażującym podmioty spoza Unii Europejskiej, zagadnienie to nie jest proste.

Celem niniejszego opracowania jest przedstawienie zagadnienia przetwarzania danych osobowych do celów badań naukowych, w szczególności w aspekcie międzynarodowym, w świetle wymogów RODO. Kluczowymi kwestiami, które zostaną poruszone są: zakres zastosowania RODO w aspekcie terytorialnym, zasady przetwarzania danych osobowych, podstawy prawne przetwarzania danych, określanie roli podmiotów przetwarzających dane osobowe (administrator, współadministrator, podmiot przetwarzający), obowiązki formalne zawiązane z przetwarzaniem danych oraz stosowanie odpowiednich zabezpieczeń.

[4] Wytyczne Europejskiej Rady Ochrony Danych 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 byłej Grupy Roboczej Art. 29 z dnia 10 kwietnia 2018 r., WP259 rev.01, 17PL, s. 27 (poparte przez EROD).



## I. Zakres zastosowania RODO w aspekcie terytorialnym

Na wstępie należy zaznaczyć, że RODO obowiązuje na terytorium Unii Europejskiej w szerokim aspekcie podmiotowym. Ochroną prawną tego aktu cieszą się bowiem zarówno obywatele państw członkowskich, jak i obywatele tzw. państw trzecich, którzy przebywają na terenie UE[5].

Artykuł 3 RODO określa jego zakres terytorialny, czyli sytuacje, w których przepisy rozporządzenia mają zastosowanie, nawet jeśli podmiot przetwarzający dane nie ma siedziby na terenie Unii Europejskiej. Jest to jeden z fundamentalnych przepisów, który nadaje RODO charakter eksterytorialny, co oznacza, że jego zasięg wykracza poza granice UE. W kontekście wspólnych badań naukowych lub realizacji projektów badawczych prowadzonych wspólnie przez podmiot z UE (np. polski uniwersytet) i podmiot spoza UE (np. ukraiński uniwersytet), zastosowanie RODO do tego drugiego wynika z kilku kluczowych kryteriów określonych we wskazanym powyżej przepisie:

1. Kryterium „jednostki organizacyjnej" (Art. 3 ust. 1 RODO).

„Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii". Nawet jeśli uczelnia ukraińska nie ma formalnej filii w Polsce, ale jej działalność badawcza jest prowadzona w ramach „efektywnego i rzeczywistego wykonywania działalności – nawet minimalnej – poprzez stabilne uzgodnienia" na terenie UE (np. poprzez stałą współpracę z polską uczelnią, która może być uznana za jej „jednostkę organizacyjną" w szerszym sensie, lub poprzez obecność jej pracowników w Polsce w celach badawczych), może to stanowić podstawę do zastosowania RODO.

[5] Motyw 2 RODO „Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych".
Motyw 14 RODO: „Ochrona zapewniana niniejszym rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych".

2. Kryterium "kierowania działalności" i "monitorowania zachowania" (Art. 3 ust. 2 lit. a i b RODO).

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

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii".

RODO ma zastosowanie do przetwarzania danych osobowych osób fizycznych, które znajdują się w Unii, przez administratora lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii, jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom w Unii. Udział w badaniach naukowych, zwłaszcza tych angażujących uczestników z UE (np. z Polski), może być interpretowany jako „oferowanie usługi" (udziału w badaniu) tym osobom, nawet jeśli nie wiąże się to z płatnością. Jeśli uczelnia ukraińska, samodzielnie lub we współpracy z polską uczelnią, rekrutuje uczestników badania z Polski lub innych krajów UE, to „kieruje działalność" do osób znajdujących się w Unii, co automatycznie włącza ją w zakres RODO. Przepisy rozporządzenia mają zastosowanie również wtedy, gdy czynności przetwarzania wiążą się z monitorowaniem zachowania osób fizycznych, o ile ich zachowanie ma miejsce na terytorium Unii. Wiele badań naukowych, zwłaszcza w dziedzinach takich jak psychologia, socjologia, medycyna czy nauki behawioralne, polega na monitorowaniu zachowań, nawyków, stanu zdrowia czy innych aspektów życia uczestników. Jeśli to monitorowanie dotyczy osób znajdujących się w UE (np. poprzez ankiety online, zbieranie danych z urządzeń noszonych, analizę aktywności w Internecie), to uczelnia ukraińska, jako podmiot uczestniczący w tym monitorowaniu, podlega RODO.

Co również należy podkreślić, nawet jeśli uczelnia ukraińska nie rekrutuje bezpośrednio uczestników z UE, ale otrzymuje dane osobowe od polskiej uczelni (która jako podmiot unijny musi przestrzegać RODO), to przetwarzanie tych danych przez uczelnię ukraińską również podlega RODO. Polska uczelnia, jako administrator danych, ma obowiązek



zapewnić, że wszelkie transfery danych poza Europejski Obszar Gospodarczy (EOG) odbywają się zgodnie z Rozdziałem V RODO, co wymaga zastosowania odpowiednich zabezpieczeń (zwykle będą to Standardowe Klauzule Umowne – SCCs). W praktyce oznacza to, że odbiorca danych spoza UE (uczelnia ukraińska) musi zobowiązać się do przestrzegania europejskich standardów ochrony danych, w tym zasad przetwarzania danych osobowych.

## II. Zasady przetwarzania danych osobowych

Podstawowe zasady przetwarzania danych osobowych znalazły się w początkowej części RODO – w art. 5 (rozdział II), przed innymi fundamentalnymi regulacjami, takimi jak przesłanki legalności przetwarzania danych (art. 6 i 9 RODO). Ten zabieg redakcyjny był zamierzony i jednoznacznie wskazuje kluczowe znaczenie regulacji. Każdy podmiot przetwarzający dane na potrzeby badań naukowych i realizacji projektów badawczych ma obowiązek ich przestrzegać. Karta praw podstawowych Unii Europejskiej wskazuje następujące zasady, którym musi sprostać przetwarzanie danych osobowych: rzetelności,
następnych: przejrzystości, minimalizacji danych, prawidłowości, ograniczoności przechowywania, integralności i poufności oraz rozliczalności.

*Pierwszą z zasad jest zgodność z prawem, rzetelność i przejrzystość.* Zasada ta to nic innego jak obowiązek przetwarzania danych osobowych na podstawie przesłanek legalności z art. 6 lub art. 9 RODO (temat został szczegółowo omówiony w kolejnym rozdziale). Na to, jak należy rozumieć rzetelność i przejrzystość, wskazują motywy 39, 58 oraz 60 preambuły RODO. Zasady te będą spełnione poprzez realizację obowiązków informacyjnych względem osób, których dane dotyczą (art. 13 i 14 RODO) w sposób zwięzły, zrozumiały, formułowane jasnym i prostym językiem. Obowiązki informacyjne zostały wyczerpująco omówione w podrozdziale „Obowiązki formalne zawiązane z przetwarzaniem danych" niniejszego opracowania.

[6] Art. 8 ust. 2 Karty praw podstawowych Unii Europejskiej.

*Drugą zasadą jest ograniczenie celu przetwarzania danych*. Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Wyjątkiem jest dalsze przetwarzanie danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Ta zasada ma na celu zapewnienie, że osoby, których dane dotyczą, są świadome, w jakim celu ich dane są zbierane i wykorzystywane. Zapobiega to niekontrolowanemu i nieprzewidywalnemu wykorzystywaniu danych osobowych do celów innych niż te, na które pierwotnie wyrażono zgodę lub które były podstawą prawną przetwarzania. W przypadku badań naukowych RODO wprowadza istotne ułatwienia i pewną elastyczność w stosowaniu tej zasady, co jest kluczowe dla dynamiki i długoterminowego charakteru działalności badawczej. Art. 5 ust. 1 lit. b w zw. z Art. 89 ust. 1 RODO stanowią, iż dalsze przetwarzanie danych osobowych do celów badań naukowych, historycznych lub statystycznych nie jest uznawane za niezgodne z pierwotnymi celami, dla których dane zostały zebrane. Oznacza to, że dane zebrane pierwotnie w innym celu (np. dane medyczne zebrane w celu leczenia, dane administracyjne) mogą być później wykorzystane do badań naukowych bez konieczności uzyskiwania nowej zgody na każdy nowy cel badawczy, o ile spełnione są odpowiednie warunki. Jest to fundamentalne ułatwienie, które pozwala na ponowne wykorzystanie wartościowych zbiorów danych, co jest kluczowe dla postępu naukowego. Elastyczność w zasadzie ograniczenia celu dla badań naukowych wiąże się z bezwzględnym wymogiem wdrożenia odpowiednich zabezpieczeń technicznych i organizacyjnych. Zabezpieczenia te mają na celu ochronę praw i wolności osób, których dane dotyczą. Szerzej tematyka ta zostanie omówiona w dalszej części niniejszego opracowania.

Trzecią z naczelnych zasad, określonych w art. 5 RODO, jest minimalizacja danych. Zgodnie z nią, zakres przetwarzanych danych powinien być taki, jaki jest niezbędny do osiągnięcia określonego celu przetwarzania danych. Przetwarzając dane w celu prowadzenia badań naukowych i realizacji projektów badawczych należy dokonać selekcji danych i wybrać tylko te, które są adekwatne do zrealizowania celu.

Czwartą zasadą jest zasada prawidłowości danych, która wskazuje, iż przetwarzane dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy



opracować odpowiednie rozwiązania techniczne oraz organizacyjne umożliwiające korygowanie nieprawidłowych lub nieaktualnych danych. Zasada jest powiązana z uprawnieniem osoby, której dane przetwarzamy do sprostowania swoich danych[7].

Piątą zasadą, najbardziej problematyczną dla wszystkich podmiotów przetwarzających dane osobowe, jest ograniczenie przechowania danych (zasada ograniczonego czasu). Sprowadza się do tego, aby okres przetwarzania danych był ograniczony do czasu, jaki jest niezbędny do tego, by osiągnąć założony cel przetwarzania danych. Po tym okresie dane należy usunąć – przetwarzane w formie zarówno papierowej, jak i elektronicznej[8]. RODO, a także polskie przepisy krajowe, wprowadzają pewne specyficzne uregulowania dotyczące przechowywania danych w kontekście badań naukowych, które uwzględniają ich długoterminowy charakter i wartość dla społeczeństwa. RODO dopuszcza przechowywanie danych osobowych przez okres dłuższy, niż jest to niezbędne do pierwotnych celów, o ile dane te będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, pod warunkiem wdrożenia odpowiednich środków technicznych i organizacyjnych[9]. Oznacza to, że dane mogą być przechowywane dłużej, jeśli służą kontynuacji badań, weryfikacji wyników, czy też stanowią podstawę dla przyszłych

[7] Zgodnie z art. 16 RODO: „osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia". Możemy wyróżnić dwie formy sprostowania danych: sprostowanie rozumiane jako poprawienie nieprawidłowych danych oraz sprostowanie rozumiane jako uzupełnienie niekompletnych danych. Jednocześnie stanowi on o żądaniu sprostowania i żądaniu uzupełnienia – a nie o sprostowaniu i uzupełnieniu. Sformułowanie tego przepisu w ten sposób jasno wskazuje, że skorelowany z omawianym uprawnieniem obowiązek administratora nie ma charakteru bezwzględnego i administrator w określonych sytuacjach może odmówić uwzględnienia żądań osoby, której dane dotyczą. M. Czerniawski, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, dostęp: LEX. Nieprawidłowość może polegać na niezgodności ze stanem faktycznym, nieaktualności, błędnym zapisie lub innych wadach, które sprawiają, że dane mogą być uznane za nieprawidłowe. Będą to zarówno pomyłki pisarskie, jak i sytuacje utraty aktualności danych (np. zmiana miejsca zamieszkania, zmiana nazwiska, zmiana danych kontaktowych). P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 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)*, [w:] idem, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, dostęp: LEX. Zob. więcej: A. Mrozowska, Dział XIVa *Przetwarzanie danych osobowych*, [w:] Woźnicki J. (red.), *Prawo o szkolnictwie wyższym i nauce. Komentarz*, Wolters Kluwer, Warszawa 2019.

[8] A. Mrozowska, *Ochrona danych osobowych w szkolnictwie wyższym* [w:] J. Woźnicki (red), *Identyfikacja i uzasadnienie kierunków regulacji o kluczowym znaczeniu w ustawie prawo o sokolnictwie wyższym i nauce*, Warszawa–Toruń 2020, s. 174-175.

[9] Art. 5 ust. 1 lit. e RODO.

analiz, pod warunkiem, że są odpowiednio zabezpieczone. Polskie przepisy są w tym zakresie bardziej precyzyjne. Zgodnie z Art. 469b ust. 4 ustawy Prawo o szkolnictwie wyższym i nauce, dane osobowe przetwarzane do celów badań naukowych lub prac rozwojowych poddaje się anonimizacji niezwłocznie po osiągnięciu celu badań naukowych lub prac rozwojowych. W ramach najlepszych praktyk, instytucje badawcze powinny opracowywać szczegółowe plany zarządzania danymi (DMP), które jasno określają polityki retencji i usuwania danych dla każdego projektu badawczego. Zasada ograniczonego czasu przechowywania jest ściśle powiązana z prawem do usunięcia danych ("prawem do bycia zapomnianym")[10]. Co do zasady, osoba, której dane dotyczą, ma prawo żądać usunięcia swoich danych, gdy nie są już niezbędne do celów, w których zostały zebrane, lub gdy wycofała zgodę, a nie ma innej podstawy prawnej. Jednakże, RODO przewiduje wyjątek od prawa do bycia zapomnianym, jeśli przetwarzanie danych jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z Art. 89 ust. 1 RODO, o ile prawdopodobne jest, że realizacja tego prawa uniemożliwi lub poważnie utrudni osiągnięcie celów takiego przetwarzania. Oznacza to, że w pewnych okolicznościach, nawet jeśli uczestnik badania zażąda usunięcia swoich danych, administrator może mieć prawo do ich dalszego przechowywania, jeśli jest to niezbędne dla integralności i celów badania naukowego, pod warunkiem wdrożenia odpowiednich zabezpieczeń.

Kolejną zasadą, którą wyróżniamy w art. 5 RODO, jest integralność i poufność danych. Zgodnie z nią dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Niemniej, na podstawie decyzji Prezesa Urzędu Ochrony Danych Osobowych, dobrych praktyk oraz wytycznych Europejskiej Rady Ochrony Danych, wskazać można zabezpieczania, które w szczególności należy wziąć pod uwagę. Tematyka została omówiona w podrozdziale „Zabezpieczanie danych osobowych w badaniach naukowych i realizacji projektów badawczych" niniejszego opracowania.

[10] Art. 17 ust. 3 lit. d RODO



Zasada rozliczalności stanowi klamrę dla wszystkich powyższych zasad – stwierdza, że administrator jest odpowiedzialny za ich realizację i musi być w stanie wykazać ich przestrzeganie. Każdy podmiot prowadzący badania naukowe i realizujący projekty badawcze musi wdrożyć takie procedury i korzystać z takich narzędzi, które umożliwią spełnienie tego obowiązku.

Poza podstawowymi, ogólnymi zasadami wynikającymi z art. 5 RODO obowiązują dwie nowe zasady, generujące po stronie administratorów obowiązek uwzględniania ochrony danych już w fazie projektowania (*privacy by design*) oraz wdrożenia domyślnych ustawień prywatności *(privacy by default*) – art. 25 RODO. Wprowadzają one obowiązek uwzględniania ochrony danych osobowych i prywatności osób, których dane dotyczą na każdym etapie tworzenia oraz istnienia systemu (procedur, dokumentacji, oprogramowania oraz sprzętu) do przetwarzania danych osobowych. Zasady ochrony prywatności powinny być elementem każdego projektu zakładającego przetwarzanie danych osobowych w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową. RODO nakłada na nas obowiązek prewencji, a nie wyłącznie podejmowania działań naprawczych[11].

## III. Podstawy prawne przetwarzania danych w badaniach naukowych i realizacji projektów badawczych

RODO zawiera dwie grupy przesłanek, których spełnienie warunkuje zgodne z prawem przetwarzanie danych osobowych:

a) pierwsza z nich odnosi się do danych osobowych zwykłych (art. 6),
b) druga – do danych osobowych szczególnych kategorii (art. 9).

Przetwarzanie danych osobowych do celów badań naukowych i realizacji projektów badawczych może wiązać się zarówno z przetwarzaniem „danych zwykłych" i danych szczególnych kategorii[12], jak i danych osobowych dotyczących wyroków skazujących i

[11] Ibidem, s. 176.
[12] Do danych osobowych szczególnych kategorii należy zaliczyć dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do

czynów zabronionych (art. 10 RODO). Ogólne rozporządzenie nie zawiera odrębnych przepisów w zakresie przesłanek legalizujących przetwarzanie danych w postaci wyroków skazujących i czynów zabronionych, a więc znajdzie tu zastosowanie przepis art. 6 ust. 1 ogólnego rozporządzenia. Tym samym podejmując rozważania dotyczące możliwości zastosowania określonych przesłanek legalizujących przetwarzanie danych, należy brać pod uwagę zarówno przepis art. 6 ust. 1, jak i art. 9 ust. 2 RODO[13]. Przetwarzanie danych osobowych podlega zasadzie ogólnego dopuszczenia przetwarzania danych zwykłych, gdy spełniona jest co najmniej jedna z przesłanek z art. 6 ust. 1 RODO, natomiast w przypadku danych osobowych szczególnych kategorii obowiązuje zasada ogólnego zakazu przetwarzania danych wrażliwych, chyba że zachodzi którykolwiek z wyjątków pozwalających na takie przetwarzanie z art. 9 ust. 2 RODO. Katalog przesłanek legalizacyjnych danych osobowych zwykłych i szczególnych kategorii ma charakter zamknięty.

Przesłanki legalizacyjne przetwarzania danych zwykłych to:

a) zgoda osoby, której dane dotyczą, obejmująca przetwarzanie w jednym lub większej liczbie celów;
b) niezbędność przetwarzania do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na wniosek tej osoby przed zawarciem umowy;
c) niezbędność przetwarzania do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) niezbędność przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) niezbędność przetwarzania do celów wynikających z uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji,

związków zawodowych, dane genetyczne, dane biometryczne (przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej), dane dotyczące zdrowia, seksualności lub orientacji seksualnej – art. 9 ust. 1 RODO. Jest to wyliczenie enumeratywne – pozostałe dane uznajemy za „dane zwykłe".

[13] A. Pyka, *Przetwarzanie danych osobowych do celów badań naukowych. Aspekty prawne*, [w:] Studnia Prawa Publicznego 2019 • NR 4 (28), s. 81-82.



w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Szczególną uwagę należy zwrócić na dane szczególnych kategorii, często określane jako dane wrażliwe. Zgodnie z Art. 9 RODO, do tej kategorii należą dane ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej. Dane te są traktowane jako „szczególne" ze względu na ich niezwykle wrażliwy charakter i wysokie ryzyko dyskryminacji, stygmatyzacji lub naruszenia praw człowieka w przypadku ich niewłaściwego przetwarzania. Ich przetwarzanie podlega surowszym wymogom prawnym.

Przesłanki legalizacyjne przetwarzania danych szczególnych kategorii:

a) wyraźna zgoda osoby, której dane dotyczą, na przetwarzanie danych osobowych w jednym lub kilku konkretnych celach – rozporządzenie 2016/679 zakłada, że prawo unijne lub krajowe może wyłączyć możliwość uchylenia zakazu przetwarzania opisywanych danych przez sam podmiot danych;
b) niezbędność przetwarzania do wypełnienia obowiązków i skorzystania ze szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony społecznej, o ile jest to dozwolone prawem Unii lub prawem krajowym, lub umową zbiorową na mocy prawa krajowego, przewidującymi odpowiednią ochronę praw podstawowych i interesów osoby, której dane dotyczą;
c) niezbędność przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody;
d) przetwarzanie danych przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych w ramach uprawnionej działalności takiego podmiotu, prowadzonej z

zachowaniem odpowiednich gwarancji i pod warunkiem, że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu, lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane nie są ujawniane poza tym podmiotem bez zgody osób, których dotyczą;

e) okoliczność, że dane zostały podane do wiadomości publicznej w sposób wyraźny przez samą osobę, której dotyczą;

f) niezbędność przetwarzania do ustalenia, dochodzenia lub obrony roszczeń lub w ramach prawowania wymiaru sprawiedliwości przez sądy;

g) niezbędność przetwarzania ze względów związanych z ważnym interesem publicznym na podstawie prawa UE lub prawa krajowego – względy te muszą być proporcjonalne do wyznaczonego celu, nie mogą naruszać istoty prawa do ochrony danych, muszą również istnieć odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) niezbędność przetwarzania do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub społecznej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub społecznej na podstawie prawa Unii lub prawa krajowego, lub zgodnie z umową z pracownikiem służby zdrowia;

i) niezbędność przetwarzania ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa krajowego, przewidującego odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę służbową;

j) niezbędność przetwarzania do celów archiwizacyjnych w interesie publicznym, do celów badań naukowych i historycznych lub do celów statystycznych na podstawie prawa Unii lub prawa krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.



Przesłanki legalizacyjne zarówno wskazane w art. 6 ust. 1 dla danych osobowych zwykłych, jak i w art. 9 ust. 2 dla danych osobowych szczególnych kategorii, mają charakter:

1. autonomiczny i
2. równoprawny.

Autonomiczność przesłanek przetwarzania jest cechą powodującą, że wystarczające jest oparcie procesu przetwarzania danych osobowych wyłącznie na jednej z przesłanek. Równoprawność oznacza z kolei, że żadna z przesłanek nie ma charakteru uprzywilejowanego w stosunku do pozostałych[14].

Zgoda jest jedną z najczęściej stosowanych podstaw prawnych w badaniach naukowych (Art. 6 ust. 1 lit. a) RODO). Aby była ważna, musi spełniać szereg warunków: musi być dobrowolna, konkretna, świadoma i jednoznaczna. Administrator musi być w stanie wykazać, że zgoda została wyrażona. W badaniach naukowych, gdzie cel przetwarzania danych może nie być w pełni określony w momencie zbierania danych, RODO dopuszcza możliwość uzyskania tzw. zgody szerokiej (*broad consent*). Oznacza to, że osoby, których dane dotyczą, mogą wyrazić zgodę na przetwarzanie danych w ramach pewnych obszarów badań naukowych lub elementów projektów badawczych, o ile badania te są zgodne z uznanymi normami etycznymi. Pozwala to na elastyczność w długoterminowych projektach badawczych[15]. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę, a proces wycofania musi być równie łatwy jak jej wyrażenie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Po wycofaniu zgody administrator nie może dalej przetwarzać danych na tej podstawie i powinien je usunąć, chyba że istnieje inna podstawa prawna, która pozwala na ich dalsze przetwarzanie (np. obowiązek prawny). Wycofanie zgody w badaniach naukowych jest szczególnie problematyczne, ponieważ może podważyć spójność i wiarygodność wyników. Dane w

[14] D. Lubasz (red.), *Meritum. Ochrona danych osobowych*, Wolters Kluwer, Warszawa 2022 r., s. 120-121.

[15] Motyw 33 RODO: „W momencie zbierania danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. Dlatego osoby, których dane dotyczą, powinny móc wyrazić zgodę na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Osoby, których dane dotyczą, powinny móc wyrazić zgodę tylko na niektóre obszary badań lub elementy projektów badawczych, o ile umożliwia to zamierzony cel".

badaniach są często ze sobą powiązane i stanowią część większego zbioru danych przeznaczonego do analizy. Jeśli uczestnik wycofa zgodę, a jego dane są integralną częścią modelu statystycznego lub konkretnego odkrycia, ich usunięcie mogłoby unieważnić lub znacząco zmienić wynik badania. To tworzy napięcie między indywidualnymi prawami do danych a integralnością i użytecznością badań naukowych. Z tego powodu, projektując badania, należy przewidzieć takie sytuacje, na przykład poprzez jak najwcześniejsze anonimizowanie danych lub jasne informowanie uczestników o wpływie wycofania zgody na użyteczność danych (np. dane użyte już w zagregowanej, zanonimizowanej formie mogą nie być praktycznie „usuwalne" z opublikowanych wyników). To również wyjaśnia, dlaczego „interes publiczny" jest często preferowaną podstawą prawną dla niektórych rodzajów badań, ponieważ oferuje większą stabilność.

Przetwarzanie danych jest zgodne z prawem, jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (Art. 6 ust. 1 lit. e) RODO). Wiele badań naukowych, zwłaszcza tych prowadzonych przez instytucje publiczne, takie jak uniwersytety, może opierać się na tej podstawie, jeśli ich cel jest uznany za służący dobru publicznemu. W Polsce, ustawa Prawo o szkolnictwie wyższym i nauce uznaje prowadzenie badań naukowych przez uczelnie za zadanie publiczne. Wybór podstawy prawnej „interesu publicznego" może znacząco uprościć zarządzanie prawami osób, których dane dotyczą, w porównaniu do zgody. Kiedy podstawą jest zgoda, osoby te mają silne prawo do jej wycofania, co wiąże się z obowiązkami usunięcia danych. Natomiast Art. 89 ust. 2 RODO przewiduje, że prawo państwa członkowskiego może wprowadzać wyjątki od niektórych praw osób, których dane dotyczą (prawa dostępu, sprostowania, ograniczenia przetwarzania, sprzeciwu) dla celów badań naukowych, jeśli ich realizacja uniemożliwiłaby lub poważnie utrudniła osiągnięcie celów badawczych. Jest to wyraźnie powiązane z przetwarzaniem w interesie publicznym. Zatem, oparcie się na „interesie publicznym" (często wspieranym przez przepisy krajowe, takie jak Art. 469b Prawa o szkolnictwie wyższym i nauce) zapewnia bardziej stabilne ramy prawne dla długoterminowych lub szeroko zakrojonych projektów badawczych, gdzie wycofanie indywidualnej zgody mogłoby być bardzo zakłócające. Przesuwa to równowagę nieco w stronę celu badawczego, pod warunkiem wdrożenia odpowiednich zabezpieczeń.

Podstawą prawną przetwarzania danych osobowych w ramach realizacji projektów badawczych i prowadzeniu badań naukowych może być również, zgodnie z art. 6 ust. 1 lit. f) RODO, „prawnie uzasadniony interes administratora". Ta podstawa prawna jest mniej powszechnie stosowana w badaniach naukowych, częściej wykorzystują ją podmioty komercyjne. Może być używana, gdy badania służą interesowi prywatnemu, a nie publicznemu, i nie są nadrzędne wobec praw i wolności osoby, której dane dotyczą. Wymaga ona przeprowadzenia testu równowagi między interesem administratora a prawami i wolnościami osób, których dane dotyczą.

*Tabela 1. Podstawą prawną przetwarzania danych osobowych w ramach realizacji projektów badawczych i prowadzeniu badań naukowych*

| **Podstawa Prawna** | **Artykuł RODO** | **Kluczowe warunki/wymagania dla badań naukowych** | **Implikacje dla praw osób, których dane dotyczą** | **Przykłady zastosowania w badaniach** |
|---|---|---|---|---|
| Zgoda | Art. 6 ust. 1 lit. a | Dobrowolna, konkretna, świadoma, jednoznaczna; możliwa zgoda szeroka dla obszarów badawczych; administrator musi wykazać zgodę. | Prawo do wycofania zgody w dowolnym momencie; konieczność usunięcia danych, chyba że jest inna podstawa prawna. | Badania ankietowe, wywiady.. |
| Interes publiczny[16] | Art. 6 ust. 1 lit. e | Przetwarzanie niezbędne do wykonania zadania realizowanego w interesie publicznym; dotyczy w szczególności instytucji publicznych (np. uczelni). | Możliwość ograniczenia praw (dostępu, sprostowania, ograniczenia, sprzeciwu) na | Badania epidemiologiczne, badania społeczne prowadzone np. przez |

[16] Art. 469b upswn wskazuje podmioty, które uprawnione są do przetwarzania danych w celach prowadzenia badań naukowych. Są nimi: uczelnie, instytuty naukowe PAN, instytuty badawcze, działające na podstawie ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2024 r. poz. 534), międzynarodowe instytuty naukowe utworzone na podstawie odrębnych ustaw działające na terytorium Rzeczypospolitej Polskiej, Centrum Łukasiewicz, instytuty działające w ramach Sieci Badawczej Łukasiewicz, Centrum Medycznego Kształcenia Podyplomowego, Polska Akademia Umiejętności.

| | | | | |
|---|---|---|---|---|
| | | | mocy prawa krajowego (Art. 89 ust. 2), jeśli utrudnia to badania. | uniwersytety, PAN. |
| Prawnie uzasadniony interes administratora | Art. 6 ust. 1 lit. f | Przetwarzanie niezbędne do celów wynikających z prawnie uzasadnionych interesów administratora, chyba że nadrzędne są interesy lub prawa osób. | Obowiązek przeprowadzenia testu równowagi; możliwość wniesienia sprzeciwu przez osobę, której dane dotyczą. | Badania rynkowe, badania wewnętrzne w firmach, badania prywatne. |
| Dalsze przetwarzanie do celów naukowych | Art. 5 ust. 1 lit. b w zw. z art. 89 ust. 1 | Dane zebrane pierwotnie w innym celu; uznawane za zgodne z pierwotnymi celami; wymaga odpowiednich zabezpieczeń (pseudonimizacja/ anonimizacja). | Wymaga informowania o dalszym przetwarzaniu (jeśli możliwe); konieczność wdrożenia zabezpieczeń. | Ponowne wykorzystanie danych z rejestrów medycznych, danych administracyjnych, archiwów do nowych projektów badawczych. |

*Źródło: Opracowanie własne*

Co do zasady, przetwarzanie danych szczególnych kategorii jest zabronione ze względu na ich wrażliwy charakter i potencjalne ryzyko dyskryminacji. RODO przewiduje jednak pewne wyjątki od tego zakazu, które są kluczowe dla prowadzenia badań naukowych. Przetwarzanie jest dozwolone, jeśli jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii lub prawa państwa członkowskiego. Prawo to musi być proporcjonalne do wyznaczonego celu, nie naruszać istoty prawa do ochrony danych i przewidywać odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. Alternatywnie, przetwarzanie danych szczególnych kategorii jest również dozwolone, jeśli osoba, której dane dotyczą, wyraziła wyraźną zgodę na ich przetwarzanie w jednym lub kilku konkretnych celach.

Dane dotyczące zdrowia stanowią jedną z najczęściej przetwarzanych kategorii danych wrażliwych w badaniach naukowych, zwłaszcza w badaniach klinicznych. Przetwarzanie danych zdrowotnych w badaniach naukowych, choć kluczowe dla postępu medycznego,



stanowi obszar najwyższego ryzyka w kontekście RODO, wymagający wielowymiarowego podejścia prawnego i technicznego. Dane te są z natury wrażliwe, a ich niewłaściwe wykorzystanie może prowadzić do poważnej dyskryminacji, stygmatyzacji lub innych szkód. To sprawia, że jest to działalność przetwarzania „wysokiego ryzyka", często wymagająca przeprowadzenia oceny skutków dla ochrony danych (DPIA). Wytyczne Europejskiej Rady Ochrony Danych[17] precyzują zasady przetwarzania danych zdrowotnych do celów badań naukowych. Wytyczne te wskazują, że przetwarzanie danych zdrowotnych w badaniach naukowych może opierać się na zgodzie lub przepisach krajowych (art. 9 ust. 2 lit. a lub j), z wymogiem odpowiednich zabezpieczeń i tajemnicy zawodowej. Złożoność regulacyjna oznacza, że badacze zajmujący się danymi zdrowotnymi muszą przestrzegań nie tylko RODO, ale także szczegółowe przepisy krajowe (na gruncie polskim w szczególności art. 469b ustawy Prawo o szkolnictwie wyższym i nauce) oraz odpowiednie sektorowe wytyczne. Wymóg „odpowiednich, konkretnych środków ochrony praw i wolności osoby, której dane dotyczą, w szczególności tajemnicy zawodowej" (Art. 9 ust. 2 lit. i) lub „odpowiednich i konkretnych środków" (Art. 9 ust. 2 lit. j) dotyczy nie tylko bezpieczeństwa technicznego, ale także protokołów organizacyjnych, przeglądu etycznego i jasnej komunikacji, co czyni to kompleksowym wyzwaniem w zakresie zgodności.

## IV. Określanie roli podmiotów przetwarzających dane osobowe (administrator, współadministrator, podmiot przetwarzający)

Jednym z kluczowych problemów, z którymi muszą się zmierzyć podmioty przewarzające dane osobowe w badaniach naukowych i realizacji projektów badawczych jest określenie swojej roli, gdyż z każdą z nich związane się odrębne obowiązki wynikające z RODO. Większość obowiązków, o których traktuje kolejny podrozdział, spoczywa na administratorach danych. Nie zawsze jednak podmiot prowadzący badania czy realizujący projekt naukowy będzie występował w tej roli.

[17] Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19

Administratorem jest ten, kto posiada uprawnienia decyzyjne w stosunku do danych osobowych. Podmiot taki może przybrać dowolną postać organizacyjną – może to być osoba fizyczna, osoba prawna, uczelnia, fundacja, stowarzyszenie organ publiczny albo każda inna jednostka organizacyjna, jeżeli samodzielnie lub wspólnie z innymi ustalała cele i sposoby przetwarzania danych osobowych[18].

Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, to mamy do czynienie z relacją współadministrowania danymi. W drodze wspólnych uzgodnień powinni oni określić odpowiednie zakresy swojej odpowiedzialności oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą (art. 26 ust. 1 i 2 RODO). Przepisy RODO nie określają formy właściwej dla uzgodnień dokonanych przez Współadministratorów, w szczególności nie wymagają umowy w formie pisemnej. Współadministratorzy mają swobodę uzgodnienia formy umowy, jednakże musi być ona udokumentowana, po to aby była zgodna z zasadą rozliczalności wskazaną w art. 5 ust. 2 RODO[19].

Z przepisu art. 26 RODO wynikają minimalne, będące równocześnie obligatoryjnymi, elementy umowy współadministratorów. Są to obowiązki stron w zakresie dotyczącym:

1. wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz
2. obowiązki współadministratorów w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO (obowiązki informacyjne, patrz kolejny podrozdział).

W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. Zasadnicza treść umowy jest udostępniana podmiotom, których dane dotyczą (art. 26 ust. 2 RODO). Europejska Rada Ochrony Danych postuluje, aby umowa zawierała również wiele elementów dodatkowych. Postulowana i przykładowa lista takich

[18] Art. 4 pkt 7 RODO: „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania

[19] Zob. P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Legalis 2021, komentarz do art. 26 i powołana tam literatura.



elementów wynika z Wytycznych 7/2020 EROD[20]. Są to postanowienia dotyczące: wdrożenia ogólnych zasad ochrony danych (art. 5 RODO), podstawy prawnej przetwarzania (art. 6 RODO), środków bezpieczeństwa (art. 32 RODO), powiadomień organu nadzorczego i osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 33 i 34 RODO), oceny skutków dla ochrony danych (art. 35 i 36 RODO), podmiotu przetwarzającego (art. 28 RODO), przekazywania danych do państw trzecich (rozdział V RODO), organizacji kontaktu z osobami, których dane dotyczą, i organami nadzorczymi, ograniczenia wykorzystania danych osobowych do innego celu przez jednego ze współadministratorów[21].

Prowadząc badania naukowe samodzielnie, uczelnia będzie administratorem danych. W przypadku prowadzenia wspólnych badań zwykle będziemy mieli do czynienia w relacją współadministrowania. Podobnie w przypadku organizowania konferencji naukowej przez klika uczelni/podmiotów.

Od wskazanych powyżej relacji należy odróżnić sytuację prawną podmiotu przetwarzającego, czyli takiego, któremu administrator powierza przetworzenie danych osobowych. Z przypadkiem takim będziemy mieli do czynienia, gdy administrator zamiast samodzielnie wykonać jakąś czynność przetwarzania, posłużył się w celu jej realizacji jakimś podmiotem zewnętrznym. To właśnie ten ostatni podmiot będzie nazywany przetwarzającym. Podmiot przyjmujący zlecenie nie uzyska statusu administratora, gdyż nie ma uprawnień decyzyjnych w stosunku do danych – może zrobić z nimi tylko to, co nakazał mu administrator. Nie uzyska też statusu współadministratora, gdyż nie bierze udziału w ustalaniu celów i sposobów przetwarzania wspólnie z administratorem. Wręcz przeciwnie, będzie związany ustaleniami w tym względzie powziętymi przez administratora, np. co do czasu, miejsca i sposobu zniszczenia danych. Tym, co łączy podmiot przetwarzający z administratorem, jest umowa lub inny instrument prawny, na podstawie którego administrator zleca przetwarzającemu realizację zadania, które wiążą się z przetworzeniem danych

[20] Wytyczne 7/2020 EROD w sprawie koncepcji administratora i podmiotu przetwarzającego w RODO, przyjęte 7.07.2021 r.,

[21] K. Palka-Bartoszek, *Współadministrowanie danymi osobowymi*, rozdział 8, M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2022 r., s.276-277. Tam też więcej informacji oraz wzór uzgodnień dot. współadministrowania danymi.

osobowych „należących” do administratora[22]. Oznacza to, że podmiot przetwarzający będzie przetwarzać takie dane, które powierzył mu administrator, w celu, jaki wyznaczył administrator, oraz w sposób, jaki on określił. Podmiot przetwarzający nie jest więc samodzielny w zakresie podejmowanych czynności – działa w imieniu administratora[23].

Uczelnia w roli podmiotu przetwarzającego najczęściej występować będzie w przypadku realizacji projektów naukowych finansowanych lub współfinasowanych z zewnętrznych źródeł. Tak jest np. w przypadku Program Operacyjnego Wiedza Edukacja Rozwój (PO WER)[24] czy korzystania z Funduszu Europejskiego Rozwoju Społecznego (FERS)[25]. Z uwagi na różnorodność zewnętrznych źródeł finansowania badań naukowych i projektów badawczych każdorazowo najeży poddać stosownej analizie dokumenty określające ramy prawne danego projektu, w szczególności regulaminy i wytyczne. W niech odnajdziemy odpowiedź na pytanie w jakiej robi występować będzie beneficjent/beneficjenci. Najczęściej zawarta zostanie umowa powierzenia z właściwą Instytucją Zarządzającą lub Pośredniczącą, która szczegółowo określi jakie obowiązki związane z przetwarzaniem i ochroną danych osobowych będzie spoczywać na uczelni/uczelniach. Powierzenie danych może również wstępować w przypadku zlecania części badań czy analizy danych zewnętrznemu podmiotowi (innej uczelni, instytutowi).

Precyzyjne określenie ról (administrator, współadministrator, procesor) w projektach badawczych, zwłaszcza w złożonych, często międzynarodowych współpracach, jest kluczowe dla uniknięcia luk w odpowiedzialności i zapewnienia pełnej zgodności z RODO. Projekty badawcze często angażują wiele podmiotów (np. uniwersytety, szpitale, zewnętrzne laboratoria, indywidualni badacze, sponsorzy). RODO definiuje odrębne role: administratora (określa cele i sposoby), procesora (przetwarza dane w imieniu administratora) i współadministratorów (wspólnie określają cele i sposoby). Brak jasności co do ról prowadzi do niejasnych obowiązków. W przypadku naruszenia danych

[22] Najczęściej będzie to umowa powierzenia przetwarzania danych osobowych.
[23] *Ibidem,* s. 27-28.
Art. 4 pkt 8 RODO: „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
[24] Zob. więcej: *Przewodnik po danych osobowych w projektach PO WER dla Wnioskodawców i Beneficjentów,* https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/przewodnik-po-danych-osobowych-w-projektach-po-wer-dla-wnioskodawcow-i-beneficjentow/ (dostęp 29.06.2025 r.)
[25] https://www.rozwojspoleczny.gov.pl/strony/zasady-przetwarzania-danych-osobowych-w-programie-fundusze-europejskie-dla-rozwoju-spolecznego/ (dostęp z dnia 29.06.2025)



lub niewypełnienia praw osoby, której dane dotyczą, trudno jest ustalić, kto ponosi odpowiedzialność, co może prowadzić do przerzucania odpowiedzialności i niezgodności z przepisami. Zatem, przed rozpoczęciem przetwarzania danych w ramach współpracy badawczej, należy przeprowadzić dokładną analizę prawną w celu precyzyjnego określenia roli każdej ze stron (co wpisuje się w realizację zasady *privacy by design* – art. 25 RODO). Ta klarowność jest kluczowa dla sporządzenia prawnie wiążących umów powierzenia przetwarzania danych (dla relacji administrator-procesor) lub umów o współadministrowanie (dla relacji współadministratorów). Ten proaktywny krok minimalizuje ryzyko prawne, zapewnia rozliczalność i usprawnia działania związane ze zgodnością we wszystkich zaangażowanych podmiotach

## V. Obowiązki formalne zawiązane z przetwarzaniem danych

Jak wskazano, RODO określa zasady, podstawy prawne przetwarzania danych osobowych, jak również kształtuje konkretne rozwiązania prawne (obowiązki formalne), do których zobowiązane są stosować się wszystkie podmioty wykorzystujące w swojej działalności dane osobowe. Podmioty prowadzące naukową działalność naukową i badawczą będą musiały je spełnić, jak wszystkie inne, dostosowując zasady ich realizacji do specyfiki swojej działalności. Obowiązki formalne możemy podzielić na ogólne, dotyczące podmiotu/instytucji oraz szczegółowe, związane z prowadzeniem konkretnego badania czy realizacji projektu.

Na poziomie instytucji prowadzącej naukową działalność badawczą (administratora danych, np. uczelni) możemy wyróżnić następujące obowiązki, które mają charakter permanentny, których realizację należy zapewniać w sposób ciągły[26]:

1. wypracowanie procedur oceny ryzyka i oceny skutków dla ochrony danych osobowych (art. 24 ust. 1, art. 32 ust. 1 i art. 35 RODO);

[26] M. Jagielski, *Ochrona danych osobowych jako element oceny etycznej badań naukowych z udziałem ludzi*, [w:] *Diametros - An Online Journal of Philosophy*, 2023, t.76, s. 5.

2. opracowanie dokumentacji ochrony danych osobowych, w szczególności rejestru czynności przetwarzania oraz wzorów innych wymaganych dokumentów (art. 5 ust. 2 i art. 30 RODO);
3. opracowanie zasad postępowania na wypadek naruszenia ochrony danych osobowych (art. 33 RODO);
4. stworzenie infrastruktury spełniającej wymogi bezpieczeństwa danych osobowych (art. 32 RODO);
5. zawarcie umów powierzenia z zewnętrznymi podmiotami obsługującymi administratora (art. 28 RODO);
6. spełnienie obowiązków informacyjnych (art. 13 i 14 RODO);
7. wyznaczenie Inspektora Ochrony Danych (dalej: IOD) (art. 37 RODO);
8. wystawienie pracownikom upoważnień do przetwarzania danych, odpowiednie przeszkolenie pracowników (art. 29, art. 4 ust. 2 i art. 25 RODO)[27].

Drugi typ wymogów to te, które nakierowane są na konkretne działania obejmujące przetwarzanie danych, czyli w kontekście działalności badawczej takie, które odnoszą się do konkretnych projektów badawczych/naukowych. Będą one musiały być zrealizowane w stosunku do każdego pojedynczego projektu:

1. ustalenie podstawy prawnej przetwarzania poszczególnych kategorii danych, w tym ustalenie, czy konieczne będzie pozyskiwanie zgód na przetwarzanie danych oraz czy planuje się ponowne wykorzystanie wcześniej zgromadzonych danych (tzw. *secondary use*) (art. 6-7 RODO);
2. określenie szczególnych kategorii danych (tzw. danych wrażliwych), które będą przetwarzane w ramach projektu (art. 9);
3. określenie relacji poszczególnych podmiotów współpracujących w ramach projektu naukowego (administrator/ współadministratorzy /podmioty przetwarzające) oraz zawarcie stosownych umów/uzgodnień (art. 26 i 28 RODO);
4. legalizacja ewentualnego transferu danych poza Europejski Obszar Gospodarczy (art. 44-49 RODO)
5. przygotowanie obowiązków informacyjnych (art. 13 i 14 RODO);

[27] W zakresie wymaganej dokumentacji zob. więcej: , M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, *op.cit*.



6. dokonanie oceny ryzyka i ew. oceny skutków dla projektu (tzw. DPIA) lub skorzystanie z procedury uprzednich konsultacji (art. 24 ust. 1, art. 32 ust. 1 i art. 35-36 RODO);
7. określenie sposobów zabezpieczeń poszczególnych procesów przetwarzania, w tym zastosowania takich technik jak pseudonimizacja i anonimizacja (art. 34 RODO)[28].

Na potrzeby niniejszego opracowania omówione zostaną dwa zasadnicze wymogi formalne, o które należy zadbać przy realizacji konkretnych projektów badawczych, tzn. legalizacja ewentualnego transferu poza Europejski Obszar Gospodarczy oraz spełnianie obowiązków informacyjnych.

## VI. Transfer danych poza EOG w ramach prowadzonych badań naukowych i realizacji projektów badawczych

Współczesne badania naukowe, zwłaszcza te prowadzone na dużą skalę i w ramach międzynarodowych konsorcjów, w coraz większym stopniu opierają się na gromadzeniu, przetwarzaniu i wymianie ogromnych zbiorów danych. Wiele z tych danych ma charakter osobowy, co stawia przed badaczami i instytucjami naukowymi złożone wyzwania w zakresie zgodności z przepisami o ochronie danych, w szczególności z RODO. Operacje przetwarzania danych osobowych podejmowane na obszarze Unii Europejskiej oraz szerzej – Europejskiego Obszaru Gospodarczego nie wymagają realizacji dodatkowych wymogów ponad te, z którymi mamy do czynienia w odniesieniu do operacji dokonywanych na obszarze pojedynczego państwa członkowskiego (np. w ramach terytorium Polski). Jest to w pełni zrozumiałe pod rządami RODO, które unifikuje zasady przetwarzania danych w ramach UE (EOG), zapewniając swobodę wewnątrzunijnego przekazywania danych osobowych. Z przepisów RODO wyprowadzić można generalny zakaz przekazywania danych osobowych do państw trzecich[29] oraz organizacji

[28] M. Jagielski, *Ochrona danych osobowych (...), Op. cit.*, s. 5-6.

[29] RODO nie zawiera definicji państwa trzeciego, należy jednak uznać, że jako takie traktować należy każde z państw, które nie należy do EOG. Szerzej zob. *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe*. Komentarz, red. P.

międzynarodowych. Zwolnienie z tego zakazu wymaga spełnienia jednej z następujących przesłanek:

- powołania się na decyzję Komisji stwierdzającą odpowiedni stopień ochrony w państwie trzecim lub organizacji międzynarodowej (tzw. decyzja w sprawie adekwatności) – art. 45 RODO[30];
- wykorzystania odpowiednich zabezpieczeń, w szczególności standardowych klauzul ochrony danych lub wiążących reguł korporacyjnych – art. 46 i 47 RODO;
- skorzystania z któregoś z wyjątków (odstępstw od zakazu transferu), przewidzianych w art. 49 RODO, np. powołania się przez eksportera danych na wyraźną zgodę podmiotu danych, którego dane mają podlegać transferowi do państwa trzeciego[31].

Zgodnie z art. 45 ust. 1 RODO przekazanie danych osobowych do państwa trzeciego (organizacji międzynarodowej) może nastąpić, gdy Komisja stwierdzi, że określone państwo trzecie (lub określona organizacja międzynarodowa) zapewnia odpowiedni stopień ochrony danych osobowych. Wydanie przez Komisję decyzji o charakterze pozytywnym (tzw. *positive findings*) w stosunku do określonego państwa trzeciego przesądza, że państwo to zapewnia na swym terytorium adekwatny stopień ochrony danych osobowych w rozumieniu RODO. W praktyce oznacza to, że w sytuacji gdy dane mają zostać przekazane do państwa objętego decyzją Komisji w sprawie adekwatności, zbędne jest korzystanie z innych mechanizmów transferowych, np. umowy transferowej[32].

W przypadku braku decyzji adekwatności dla danego państwa trzeciego, transfer danych osobowych jest możliwy pod warunkiem zastosowania „odpowiednich zabezpieczeń", które zapewniają egzekwowalne prawa i skuteczne środki ochrony prawnej dla osób,

Litwiński, Warszawa 2021, s. 422 i n. oraz P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2022, s. 523.

[30] Obecnie na liście tej znajdują się: Szwajcaria, Argentyna, Guernsey, Wyspa Man, Jersey, Andora, Izrael, Urugwaj, Nowa Zelandia, Kanada (w odniesieniu do operacji przetwarzania podlegających kanadyjskiej ustawie o ochronie informacji osobowych i dokumentów elektronicznych, tzw. PIPEDA), Wyspy Owcze, Japonia, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Korea Południowa. Lista państw trzecich i terytoriów uznanych przez Komisję za spełniające odpowiednie wymogi znajduje się na stronie: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (dostęp z dnia 29.06.2025)

[31] D. Lubasz (red.), *Meritum* (...), ibidem, s. 369.

[32] *Op. cit*., s. 374.



których dane dotyczą (art. 46 i 47 RODO) lub skorzystania z wyjątku wskazanego w art. 49 RODO. W praktyce najczęściej stosowanym i najbardziej adekwatnym w przypadku badań naukowych mechanizmem są Standardowe Klauzule Umowne (SCCs). Są to wzorcowe klauzule umowne przyjęte przez Komisję Europejską, które strony umowy o transferze danych muszą włączyć do swoich umów, co zapewni legalność transferu poza EOG. Obowiązujące klauzule muszą być przyjęte oraz stosowane w całości. Nie ma możliwości wyboru pojedynczych postanowień lub mieszania postanowień z różnych zestawów klauzul. W razie konieczności, wdrożone mogą zostać dodatkowe środki uzupełniające w celu zapewnienia odpowiedniego stopnia ochrony danych podczas transferów do państw trzecich. Od 27 czerwca 2021 r. obowiązuje najnowsza Decyzja Wykonawcza Komisji (UE) 2021/914[33] na temat standardowych klauzul umownych, będąca w zgodności z wyrokiem TSUE w sprawie Schrems II (C-311/18). Klauzule umowne obejmują różne scenariusze przekazywania danych, tj.:

- przekazywanie danych między administratorami,
- przekazywanie danych przez administratora podmiotowi przetwarzającemu w państwie trzecim,
- przekazywanie danych między podmiotami przetwarzającymi,
- przekazywanie danych przez podmiot przetwarzający administratorowi w państwie trzecim[34].

Jednakże, po orzeczeniu Schrems II, samo zastosowanie SCCs nie jest już wystarczające. Eksporter danych jest zobowiązany do przeprowadzenia Oceny Skutków Transferu (TIA - Transfer Impact Assessment). TIA to analiza prawna i faktyczna systemu prawnego państwa trzeciego, mająca na celu ocenę, czy klauzule umowne będą skuteczne w praktyce, zwłaszcza w kontekście możliwości dostępu władz publicznych do danych. Europejska Rada Ochrony Danych określiła sześciostopniowy proces TIA, obejmujący m.in. zrozumienie transferów, identyfikację narzędzia transferu, ocenę jego skuteczności, przyjęcie środków uzupełniających, podjęcie niezbędnych kroków proceduralnych i ponowną ocenę. To pokazuje, że zgodność z RODO w zakresie

[33] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32021D0914&from=EN

[34] https://uodo.gov.pl/pl/535/2506 (dostęp z dnia 29.05.2025)

transferów danych wymaga nie tylko formalnego zastosowania narzędzi, ale także ciągłej, aktywnej oceny ryzyka[35].

## VII. Obowiązki informacyjne

Koleją kwestią jest spełnienie przez administratora obowiązków informacyjnych, które są kluczowe dla zapewnienia przejrzystości i poszanowania praw osób, których dane są przetwarzane. Obowiązek ten ma zastosowanie niezależnie od podstawy prawnej przetwarzania, obejmując wszystkie przesłanki z art. 6 i art. 9 RODO. Co istotne, dotyczy on również danych uzyskiwanych w sposób pasywny, takich jak pliki cookies czy inne technologie śledzące, które mogą być wykorzystywane w badaniach naukowych (np. analiza zachowań użytkowników na platformach badawczych). RODO rozróżnia dwie główne sytuacje, w których powstaje obowiązek informacyjny: gdy dane są zbierane bezpośrednio od osoby, której dotyczą (art. 13 RODO) oraz gdy dane pozyskiwane są w inny sposób, np. od osoby trzeciej lub z publicznie dostępnych źródeł (art. 14 RODO). Jeśli dane osobowe do celów badań naukowych są zbierane bezpośrednio od uczestników, administrator (podmiot prowadzący badania, np. uczelnia, instytut) ma obowiązek przekazać im szereg informacji w momencie pozyskiwania danych:

- Tożsamość i dane kontaktowe administratora (oraz, jeśli ma zastosowanie, jego przedstawiciela).
- Dane kontaktowe inspektora ochrony danych (IOD), jeśli został powołany.
- Cele przetwarzania danych osobowych – należy jasno określić, w jakim celu dane będą wykorzystywane w badaniu naukowym. W przypadku badań naukowych RODO (motyw 33) dopuszcza pewną elastyczność w określeniu celu, ponieważ często nie da się go w pełni zidentyfikować na etapie zbierania danych. W takich przypadkach osoby badane powinny móc wyrazić zgodę na "niektóre obszary badań naukowych", o ile badania są zgodne z uznanymi normami etycznymi.
- Podstawa prawna przetwarzania – np. należy pamiętać, że zgoda na przetwarzanie danych osobowych do celów badań naukowych powinna być wyraźnie oddzielona od zgody na udział w samym badaniu.
- Prawa przysługujące osobie, której dane dotyczą:
    - Prawo dostępu do danych (art. 15 RODO).
    - Prawo do sprostowania danych (art. 16 RODO).
    - Prawo do usunięcia danych ("prawo do bycia zapomnianym") (art. 17 RODO) – z uwzględnieniem wyjątków dla celów badawczych (art. 17 ust. 3 lit. d RODO).
    - Prawo do ograniczenia przetwarzania (art. 18 RODO).
    - Prawo do sprzeciwu wobec przetwarzania (art. 21 RODO – jeżeli przetwarzanie odbywa się na podstawie interesu publicznego lub prawnie uzasadnionych interesów administratora – art. 6 ust. 1 lit. e) lub f)) – w przypadku badań naukowych należy pamiętać o specyfice, ponieważ dane te często są niezbędne dla integralności badań.
    - Prawo do przenoszenia danych (art. 20 RODO) – raczej rzadko ma zastosowanie w badaniach naukowych.
    - Prawo do cofnięcia zgody w dowolnym momencie (jeżeli przetwarzanie odbywa się na podstawie zgody), bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
    - Prawo do wniesienia skargi do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych).
- Okres, przez który dane osobowe będą przechowywane, a jeśli nie jest to możliwe – kryteria ustalania tego okresu (np. 5 lat po zakończeniu projektu badawczego).
- Informacje o tym, czy podanie danych jest wymogiem ustawowym lub umownym oraz konsekwencjach ich niepodania.
- Informacje o odbiorcach danych osobowych (np. instytucje finansujące, podmioty przetwarzające administratora).

[35] Zob. Zalecenia EROD 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, przyjęte 18 czerwca 2021 r., dostępne na stronie: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_pl

- Informacje o zamiarze przekazania danych do państwa trzeciego (spoza Europejskiego Obszaru Gospodarczego) lub organizacji międzynarodowej. Należy również poinformować o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony danych w danym państwie, lub o zastosowanych zabezpieczeniach (np. standardowych klauzulach umownych)
- Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (o którym mowa w Art. 22 ust. 1 i 4 RODO), oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Artykuł 13 ust. 4 RODO przewiduje istotne zwolnienie z obowiązku informacyjnego: zwolnienie dotyczy sytuacji, gdy osoba, której dane dotyczą, dysponuje już wszystkimi wymaganymi informacjami. Administrator musi być w stanie wykazać, że osoba faktycznie posiada wszystkie wymagane informacje; samo przypuszczenie czy domniemanie, że osoba może posiadać informacje, nie jest wystarczające. Zwolnienie to może dotyczyć całości lub części obowiązku informacyjnego. Ciężar dowodu spoczywa na administratorze, co oznacza, że poleganie na tym wyjątku jest ryzykowne, chyba że istnieje niezaprzeczalny dowód wcześniejszego, pełnego ujawnienia informacji.

Przykładowa klauzula informacyjna:

*Uprzejmie informujemy, że w związku z Państwa udziałem w badaniu naukowym pt. „Edukacja w Polsce: Analiza poziomu wykształcenia mieszkańców obszarów wiejskich i miejskich", Państwa dane osobowe będą przetwarzane zgodnie z przepisami Rozporządzenia 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, dalej: RODO). Administratorem Państwa danych osobowych przetwarzanych w ramach niniejszego badania naukowego jest Uniwersytet Warszawski, ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa. Mogą się Państwo z nami skontaktować mailowo na adres badania@uw.edu.pl.*



*Państwa dane osobowe będą przetwarzane w celu udziału w badaniu naukowym „Edukacja w Polsce: Analiza poziomu wykształcenia mieszkańców obszarów wiejskich i miejskich" oraz anonimowej publikacji wyników badań. Podstawą prawną przetwarzania Państwa danych osobowych jest art. 6 ust. 1 lit. e RODO a zw. z art. Art. 469b upswn, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym (prowadzenie badań naukowych przez publiczną uczelnię). Odbiorcami danych będą Politechnika Warszawska z siedzibą przy Placu Politechniki 1 w Warszawie (analiza danych) oraz Google LLC z siedzibą w Mountain View. Badanie realizujemy z wykorzystaniem formularzy i dysków udostępnionych przez firmę Google (usługa Google G-Suite dla edukacji), z którą Uniwersytet Warszawski ma podpisaną umowę powierzenia przetwarzania danych osobowych. W związku z tym Państwa dane osobowe mogą być przetwarzane w centrach przetwarzania danych firmy Google, które mogą znajdować się poza Europejskim Obszarem Gospodarczym (EOG) – w USA. W takim przypadku transfer danych odbywa się na podstawie standardowych klauzul umownych zatwierdzonych przez Komisję Europejską, zapewniających odpowiedni poziom ochrony danych. Państwa dane osobowe w związku z udziałem w badaniu będą przetwarzane przez czas trwania badania – 12 miesięcy. Po zakończeniu badania dane osobowe zostaną usunięte lub zanonimizowane w taki sposób, aby niemożliwe było zidentyfikowanie Państwa osoby. Wyniki badań będą publikowane wyłącznie w formie anonimowej. Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować mailowo pod adresem: iod@adm.uw.edu.pl. Z IOD mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania Państwa danych osobowych przez Uniwersytet Warszawski oraz korzystania z przysługujących Państwu praw związanych z przetwarzaniem danych osobowych. Do zadań IOD nie należy natomiast udzielanie informacji na temat samego badania.*

*Przysługują Państwu następujące prawa:*

- *Prawo dostępu do danych (art. 15 RODO) – mają Państwo prawo uzyskać potwierdzenie, czy przetwarzamy Państwa dane osobowe, a jeśli tak, to uzyskać do nich dostęp oraz informacje o ich przetwarzaniu.*

- *Prawo do sprostowania danych (art. 16 RODO) – mają Państwo prawo żądać niezwłocznego sprostowania nieprawidłowych danych osobowych lub uzupełnienia niekompletnych danych.*
- *Prawo do usunięcia danych („prawo do bycia zapomnianym") (art. 17 RODO) – mają Państwo prawo żądać usunięcia swoich danych osobowych w określonych sytuacjach. Informujemy jednak, że prawo to nie ma zastosowania, jeżeli przetwarzanie jest niezbędne do celów badań naukowych, o ile prawdopodobne jest, że realizacja tego prawa uniemożliwiłaby lub poważnie utrudniła realizację celów takiego przetwarzania.*
- *Prawo do ograniczenia przetwarzania (art. 18 RODO) – mają Państwo prawo żądać ograniczenia przetwarzania danych w określonych sytuacjach (np. gdy kwestionują Państwo prawidłowość danych).*
- *Prawo do sprzeciwu wobec przetwarzania (art. 21 RODO) – mają Państwo prawo wnieść sprzeciw wobec przetwarzania Państwa danych osobowych, jeśli podstawą przetwarzania jest interes publiczny lub prawnie uzasadniony interes administratora. W takim przypadku administrator może kontynuować przetwarzanie, jeśli wykaże istnienie ważnych prawnie uzasadnionych podstaw, nadrzędnych wobec Państwa interesów, praw i wolności.*
- *Mają Państwo również prawo wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, że przetwarzanie Państwa danych osobowych narusza przepisy RODO.*

*Podanie danych osobowych w formularzu jest dobrowolne, jednakże jest niezbędne do wzięcia udziału w badaniu naukowym. Odmowa podania danych uniemożliwi Państwu udział w projekcie. Państwa dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.*

Artykuł 14 RODO reguluje obowiązki informacyjne, gdy danych osobowych nie pozyskano bezpośrednio od osoby, której dane dotyczą, lecz z innych źródeł. Może to mieć miejsce w badaniach naukowych, gdy dane są pozyskiwane z publicznie dostępnych baz i rejestrów (np. CEIDG), od innych administratorów (np. z rejestrów



medycznych, danych archiwalnych) lub od innej osoby. Oprócz informacji wymaganych na podstawie Art. 13 RODO, administrator musi podać osobie, której dane dotyczą, następujące dodatkowe informacje:

- Kategorie odnośnych danych osobowych (np. dane demograficzne, dane zdrowotne, dane behawioralne, dane genetyczne). Należy wskazać, jakiego rodzaju dane zostały pozyskane.
- Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. Jest to kluczowa informacja, odróżniająca Art. 14 od Art. 13, i jest niezbędna dla pełnej transparentności.

Skuteczność obowiązku informacyjnego zależy w dużej mierze od sposobu jego realizacji, co reguluje Art. 12 RODO. Przepis ten określa ogólne zasady przekazywania informacji, które mają zastosowanie zarówno do danych zbieranych bezpośrednio (Art. 13), jak i pośrednio (Art. 14). Informacje muszą być przekazywane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, z użyciem jasnego i prostego języka. Jest to szczególnie istotne w badaniach naukowych, gdzie często występują skomplikowane terminy medyczne, psychologiczne czy techniczne. Język powinien być dostosowany do potrzeb i możliwości odbiorców, tak aby każdy uczestnik badania, niezależnie od swojego wykształcenia czy znajomości specjalistycznej terminologii, mógł w pełni zrozumieć, na co wyraża zgodę i jakie są konsekwencje przetwarzania jego danych.

Obowiązki informacyjne wynikające z Art. 13 i 14 RODO stanowią fundamentalny element ochrony danych osobowych i są kluczowe dla zapewnienia transparentności i kontroli nad danymi w badaniach naukowych. Prawidłowe ich wypełnienie jest nie tylko wymogiem prawnym, ale także etycznym, budującym zaufanie między badaczami a uczestnikami. Naruszenie przepisów w tym zakresie może skutkować nałożeniem wysokich kar finansowych przez organy nadzorcze. Urząd Ochrony Danych Osobowych w Polsce nałożył już znaczącą karę (943 470,00 zł) za naruszenie art. 14 ust. 1 i 2 RODO[36]. Poza sankcjami finansowymi, brak zgodności może prowadzić do poważnych szkód reputacyjnych dla instytucji badawczych i poszczególnych badaczy. Utrata

[36] Decyzja PUODO ZSPR.421.3.2018 z dnia 15 marca 2019 r.

zaufania publicznego może utrudnić rekrutację uczestników do przyszłych badań i negatywnie wpłynąć na możliwości współpracy.

W kontekście realizacji obowiązków formalnych należy pamiętać, że RODO zawiera szczególną regulację odnoszącą się do przetwarzania danych w celu prowadzenia badań naukowych, tzw. wyjątki badawcze. Ich istota polega na tym, że w zamian za wprowadzenie odpowiednich zabezpieczeń dla praw i wolności osób, których dane dotyczą, zwalnia się podmioty wykorzystujące dane w celach badawczych z konieczności realizacji pewnych obowiązków i spełniania niektórych wymogów[37]. Przy czym zarówno wymagane zabezpieczenia, jak i zakres zwolnień regulowane są jednocześnie przez RODO i przepisy prawa krajowego w Polsce: ustawę Prawo o szkolnictwie wyższym i nauce. Najważniejsze przywileje określone w ramach tego rozwiązania to:

1. możliwość wykorzystania w celach badawczych danych zebranych wcześniej w innych celach (tzw. *secondary use)* (art. 5 ust. 1 lit. b RODO);
2. możliwość wydłużenia okresu przechowywania danych (art. 5 ust. 1 lit. e RODO);
3. możliwość pozyskania zgody podmiotu danych na wykorzystanie danych mimo braku możliwości precyzyjnego określenia celu ich wykorzystania (tzw. zgoda obszarowa) (art. 4 pkt. 11 i art. 7 RODO, w związku z motywem 33 RODO);
4. możliwość skorzystania ze specjalnej, badawczej podstawy prawnej przetwarzania szczególnych kategorii danych (art. 9 ust. 2 lit. j. RODO oraz art. 469b ust. 2 Prawo o szkolnictwie wyższym i nauce);
5. możliwość uniknięcia konieczności realizacji obowiązku informacyjnego (art. 14 ust. 5 lit. b RODO);
6. możliwość odmowy usunięcia danych (art. 17 ust. 3 lit. d RODO); możliwość uniknięcia konieczności realizacji obowiązków wynikających z następujących praw podmiotów danych: prawa dostępu do danych (art. 15), prawa do sprostowania (art. 16), prawa do ograniczenia przetwarzania (art. 18) oraz prawa sprzeciwu (art. 21) (art. 89 ust. 2 RODO i art. 469b ust. 1 Prawo o szkolnictwie wyższym i nauce)[38].

[37] Art. 89 ust. 1 RODO
[38] M. Jagielski, *Ochrona danych osobowych(...) ibidem,* s. 5.



Przedstawione zwolnienia tworzą szczególny reżim przetwarzania danych osobowych dla celów badawczych, będący wyrazem uprzywilejowanej pozycji tej działalności w ramach regulacji RODO. Jego ideą jest ułatwienie prowadzenia badań naukowych, przy jednoczesnym zapewnieniu ochrony praw i wolności podmiotów danych. Właśnie dlatego możliwość skorzystania ze wskazanych wyjątków zawsze obarczona jest koniecznością spełnienia wymogów zabezpieczających prawa i wolności uczestników badań. Są one określone we wskazanych wyżej przepisach. Dla lepszej ochrony podmiotów danych przepisy te muszą być interpretowane ściśle i nie mogą być nadużywane. Ich zastosowanie nie może bowiem pozbawić tych podmiotów przynależnej im ochrony.

Podsumowując, zauważmy, że konstrukcja rozwiązań regulujących prowadzenie działalności badawczej w RODO jest dwuwarstwowa. Podmioty prowadzące taką działalność w pierwszej kolejności muszą spełnić ogólne wymagania RODO dotyczące przetwarzania danych osobowych (pierwsza warstwa). Chodzi zarówno o takie wymagania, które mają charakter instytucjonalny, czyli odnoszą się do sposobu działania instytucji badawczej, jak i poświęcone konkretnym przedsięwzięciom, czyli np. projektom badawczym, realizowaniem badań naukowych. Jakkolwiek realizacja tych wymogów musi być dostosowana do typu prowadzonej działalności, to wymagania te mają charakter generalny, czyli podmioty prowadzące badania są w zakresie ich spełnienia traktowane jak wszystkie inne podmioty zobowiązane do stosowania RODO. Regulacje unijne, jak i prawo krajowe zawiera także rozwiązania szczególne, opracowane specjalnie na potrzeby przetwarzania danych osobowych do celów badawczych – tzw. wyjątki badawcze (druga warstwa). Ich celem jest ułatwienie prowadzenia działalności naukowej, a zatem są tak pomyślane, by można było z nich skorzystać wtedy, gdy spełnia się wymogi prowadzenia takiej działalności[39].

[39] *Ibidem*, s 7.

## VIII. Zabezpieczanie danych osobowych w badaniach naukowych i realizacji projektów badawczych

RODO zmieniło podejście do ochrony danych osobowych na proaktywne, oparte na ryzyku. Nie ma uniwersalnych rozwiązań, które można zastosować – każdy administrator danych, czyli obecnie każda uczelnia, musi indywidualnie pochylić się nad swoim systemem przetwarzania danych osobowych w celu odpowiedniego dostosowania zabezpieczeń, procedur oraz dokumentacji do unijnej regulacji. Pewne wytyczne dotyczące badań naukowych odnajdziemy w art. 469b ustawy Prawo o szkolnictwie wyższym i nauce, który wskazuje, że administrator danych wdraża odpowiednie zabezpieczenia techniczne i organizacyjne praw i wolności osób fizycznych. W szczególności obejmuje to pseudonimizację albo szyfrowanie danych, nadawanie uprawnień do ich przetwarzania minimalnej liczbie osób niezbędnych, kontrolę dostępu do pomieszczeń, w których przechowywane są dokumenty zawierające dane osobowe, oraz opracowanie procedury określającej sposób zabezpieczenia danych. Dodatkowo, dane osobowe poddaje się anonimizacji niezwłocznie po osiągnięciu celu badań naukowych lub prac rozwojowych. Do tego czasu dane identyfikujące zapisuje się osobno i łączy z informacjami szczegółowymi tylko, jeśli wymaga tego cel badań.

*Analiza konkretnych decyzji Prezesa Urzędu Ochrony Danych Osobowych (PUODO)* dostarcza praktycznych wskazówek dotyczących oczekiwanych zabezpieczeń i obszarów, w których uczelnie najczęściej popełniają błędy. Poniżej przedstawiono wybrane przypadki, które ilustrują typowe problemy w sektorze szkolnictwa wyższego.

*Decyzja PUODO wobec Szkoły Głównej Handlowej (SGH) – Sygn. DKN.5131.26.2023 (z 30 listopada 2023 r.)*[40]

*Decyzja dotyczyła niezamierzonej publikacji i nieuprawnionego uzyskania dostępu do bazy danych osobowych około 1000 osób, przetwarzanych w aplikacji do rekrutacji na wymiany studenckie. Naruszenie trwało 27 dni. Przyczyną był błąd programisty podczas przenoszenia systemu na nowy serwer, który doprowadził do przypadkowego włączenia możliwości nieautoryzowanego wywoływania podstron panelu administratora i wdrożenia tej zmiany na serwerze produkcyjnym. Adres URL z danymi został zaindeksowany przez wyszukiwarkę internetową, co uczyniło dane ogólnodostępnymi. Kluczowe przyczyny naruszenia z perspektywy PUODO wskazywały na głębsze, systemowe problemy. Uczelnia przyznała, że analiza ryzyka dla operacji przetwarzania danych, w ramach których doszło do naruszenia, została przeprowadzona dopiero po wystąpieniu incydentu, a wcześniej „nie była prowadzona w sposób sformalizowany". Dodatkowo, procedury testowania i wdrażania były niewystarczające. Testowanie zmian na serwerze deweloperskim było wykonywane przez „samego programistę", a po umieszczeniu w repozytorium „druga osoba z zespołu (...) sprawdziła, czy aplikacja działa poprawnie", ale bez odwołania do obowiązujących procedur. Uczelnia po naruszeniu dopiero przygotowywała procedury wykonywania testów, scenariuszy testowych i code review przez innego programistę przed przekazaniem na produkcję. To zdarzenie uwydatniło, że problem nie polegał na pojedynczym błędzie ludzkim, ale na fundamentalnych brakach w zarządzaniu danymi. Brak sformalizowanej analizy ryzyka przed incydentem, niewystarczające procedury testowania i brak przeglądu kodu przez innych programistów wskazują na systemowe niedociągnięcia w zarządzaniu procesami IT i bezpieczeństwem danych. PUODO w swoich decyzjach często analizuje nie tylko bezpośrednią przyczynę naruszenia, ale także szerszy kontekst organizacyjny i procesowy, który do niego doprowadził. Oznacza to, że od uczelni oczekuje się wdrożenia kompleksowych, udokumentowanych i regularnie weryfikowanych systemów zarządzania ochroną danych, a nie tylko reagowania na już zaistniałe incydenty. PUODO nałożył na SGH karę w wysokości 35 tys. zł. Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę SGH, potwierdzając, że nie jedynie błąd ludzki, ale przede wszystkim przetwarzanie danych niezgodne z RODO, doprowadziło do wycieku danych. PUODO uznał, że uczelnia naruszyła Art. 5 ust. 1 lit. f RODO (zasada integralności i poufności) oraz Art. 32 RODO (obowiązek wdrożenia odpowiednich środków bezpieczeństwa przetwarzania). Sąd podkreślił, że Art. 32 ust. 1 RODO wymaga wdrożenia środków adekwatnych, a nie jakichkolwiek.*

[40] https://uodo.gov.pl/pl/138/3483

*Decyzja PUODO wobec Szkoły Głównej Gospodarstwa Wiejskiego (SGGW) – Sygn. ZSOŚS.421.25.2019 (z 21 sierpnia 2020 r.)*[41]

*W 2019 r. doszło do kradzieży prywatnego laptopa pracownika SGGW, na którym znajdowały się dane osobowe kandydatów na studia (szacunkowo do 100 tys. osób). Pracownik skopiował te dane na urządzenie przenośne, działając wbrew obowiązującym na uczelni procedurom. PUODO nałożył na SGGW karę finansową w wysokości 50 tys. zł. Uczelnia zaskarżyła decyzję, argumentując, że nie ponosi odpowiedzialności za działania pracownika wykraczające poza jego upoważnienie. Zarówno Wojewódzki Sąd Administracyjny, jak i Naczelny Sąd Administracyjny (7 lutego 2025 r.) oddaliły skargi uczelni. NSA nie zgodził się ze stanowiskiem SGGW, uznając uczelnię za administratora danych i stwierdzając, że nie dopełniła ona swoich obowiązków w zakresie weryfikacji zachowania pracowników pod kątem przestrzegania zasad ochrony danych osobowych. Ta decyzja jasno określa, że uczelnia, jako administrator danych, ponosi pełną odpowiedzialność za ochronę danych, nawet gdy działania pracownika naruszają wewnętrzne procedury. Samo istnienie procedur nie jest wystarczające; uczelnia musi aktywnie weryfikować ich przestrzeganie przez pracowników, co może wymagać wprowadzenia dodatkowych kontroli technicznych (np. blokujących kopiowanie danych na nieautoryzowane urządzenia) oraz regularnych szkoleń i audytów. Administrator jest odpowiedzialny za skuteczność wdrożonych środków organizacyjnych, a nie tylko za ich formalne istnienie.*

[41] https://uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019



*Decyzja PUODO wobec Uczelni Łazarskiego - DKN.5110.14.2022 z dnia 2 kwietnia 2025*[42]

*PUODO nałożył upomnienie na Uczelnię Łazarskiego za opóźnienie we wprowadzeniu wewnętrznych regulacji dotyczących zasad współpracy administratora z Inspektorem Ochrony Danych (IOD). Uczelnia początkowo nie wdrożyła rozwiązań gwarantujących, że IOD będzie właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, będzie posiadał odpowiednie zasoby do utrzymania wiedzy fachowej, nie będzie otrzymywał instrukcji dotyczących wykonywania swoich zadań, nie popadnie w konflikt interesów ze względu na inne zadania i obowiązki, oraz że jego praca będzie kontrolowana (brak regulacji dotyczących planu pracy IOD lub planu audytów). Mimo że nieprawidłowości zostały usunięte (uczelnia znowelizowała politykę ochrony danych i wdrożyła dodatkowy regulamin), opóźnienie w ich wprowadzeniu skutkowało upomnieniem. Ta decyzja podkreśla, że PUODO przywiązuje dużą wagę do prawidłowego statusu i funkcjonowania IOD, uznając go za kluczowy element systemu ochrony danych. Przypadek ten wyraźnie pokazuje, że PUODO postrzega prawidłowe funkcjonowanie IOD (jego niezależność, dostęp do zasobów, włączanie w procesy decyzyjne, brak konfliktu interesów i nadzór nad jego pracą) jako fundament zgodności z RODO. Opóźnione lub niewłaściwe wdrożenie tych aspektów bezpośrednio prowadzi do działań regulacyjnych. To oznacza, że IOD nie jest jedynie formalnością, ale kluczowym elementem skutecznego systemu ochrony danych. Uczelnie, które marginalizują rolę IOD lub nie zapewniają mu odpowiedniego wsparcia, zwiększają ryzyko niezgodności, ponieważ rola IOD polega na doradzaniu i monitorowaniu przestrzegania przepisów o ochronie danych.*

Inne istotne decyzje PUODO dotyczące bezpieczeństwa danych w sektorze publicznym/uczelniach

PUODO regularnie nakłada kary finansowe na administratorów (w tym z sektora publicznego) za niezgłoszenie naruszenia ochrony danych organowi nadzorczemu w terminie 72 godzin oraz za niezawiadomienie o naruszeniu osób, których dane dotyczą, bez zbędnej zwłoki. Jest to powtarzający się problem, wskazujący na braki w procedurach zarządzania incydentami. Decyzje PUODO (często upomnienia, ale też kary pieniężne) są wydawane wobec podmiotów, które nie zapewniają Prezesowi Urzędu dostępu do danych osobowych i informacji niezbędnych do realizacji jego zadań w

[42] https://orzeczenia.uodo.gov.pl/document/urn:ndoc:gov:pl:uodo:2022:dkn_5110_14/content

postępowaniu. Jest to naruszenie podstawowych obowiązków administratora w ramach współpracy z organem nadzorczym. Przykładem jest kara nałożona na burmistrza za brak odpowiednich środków organizacyjnych, które zapobiegłyby skopiowaniu danych osobowych przez pracownika urzędu. PUODO podkreśla, że podmioty publiczne są zobligowane do stosowania wyższych standardów w zakresie bezpieczeństwa przetwarzanych danych. Ten przypadek, choć nie dotyczy bezpośrednio uczelni, wskazuje na ogólny trend w egzekwowaniu przepisów przez PUODO: podmioty sektora publicznego, w tym uczelnie, są traktowane z większą surowością w kwestii bezpieczeństwa danych. Wynika to z ich roli w społeczeństwie i zaufania publicznego, jakim są obdarzone. Oznacza to, że uczelnie nie mogą poprzestać na minimalnych wymaganiach RODO, ale muszą dążyć do wzorowych praktyk w ochronie danych, ponieważ każde uchybienie może być ocenione bardziej rygorystycznie niż w sektorze prywatnym.

Na podstawie analizy przepisów RODO, Prawa o szkolnictwie wyższym i nauce oraz kluczowych decyzji PUODO, można wyodrębnić szereg zabezpieczeń, które uczelnie oraz inne podmioty badawcze powinny wdrożyć lub wzmocnić, aby zapewnić zgodność z przepisami o ochronie danych osobowych.

1. Pseudonimizacja i anonimizacja:
    - Pseudonimizacja: Jest to kluczowy środek bezpieczeństwa. Polega na przetworzeniu danych osobowych w taki sposób, że nie można ich przypisać konkretnej osobie bez użycia dodatkowych informacji (klucza), które są przechowywane oddzielnie i zabezpieczone. Dane pseudonimizowane wciąż są danymi osobowymi, ale ryzyko ich naruszenia jest znacznie mniejsze. Jest to często złoty środek w badaniach, gdy pełna anonimizacja uniemożliwiłaby analizę.
    - Anonimizacja: Oznacza nieodwracalne przekształcenie danych osobowych w sposób uniemożliwiający identyfikację osoby fizycznej. Dane zanonimizowane przestają być danymi osobowymi i nie podlegają RODO. Jeśli cel badawczy to dopuszcza, jest to najlepsze rozwiązanie.



2. Kontrola dostępu:
    - Zasada minimalnego uprawnienia: Dostęp do danych osobowych mają tylko te osoby, dla których jest to absolutnie niezbędne do wykonania zadania w ramach projektu.
    - Role i uprawnienia: Definiowanie konkretnych ról z przypisanymi uprawnieniami dostępu (np. badacz, statystyk, osoba zarządzająca danymi).
    - Silne uwierzytelnianie: Wymóg silnych haseł, uwierzytelniania dwuskładnikowego (2FA) wszędzie tam, gdzie to możliwe.
    - Monitorowanie dostępu: Systematyczne rejestrowanie i przeglądanie logów dostępu do danych.
3. Szyfrowanie:
    - Szyfrowanie danych w spoczynku: Szyfrowanie dysków (całych, partycji), folderów, plików, a także baz danych, w których przechowywane są dane badawcze.
    - Szyfrowanie danych w przesyle: Stosowanie bezpiecznych protokołów (SSL/TLS, HTTPS, VPN) do przesyłania danych, zwłaszcza poza sieć wewnętrzną instytucji.
4. Bezpieczeństwo infrastruktury IT:
    - Zabezpieczenia sieciowe: Firewall, systemy wykrywania i zapobiegania włamaniom (IDS/IPS).
    - Regularne aktualizacje: Systemów operacyjnych, oprogramowania, baz danych i aplikacji badawczych, aby chronić przed znanymi lukami bezpieczeństwa.
    - Oprogramowanie antywirusowe i antymalware: Bieżąca ochrona stacji roboczych i serwerów.
    - Kopie zapasowe i odzyskiwanie danych: Regularne tworzenie zaszyfrowanych kopii zapasowych i testowanie procedur odzyskiwania danych.

5. Procedury i polityki:
    - Polityka ochrony danych: Dokumentacja wewnętrzna określająca zasady przetwarzania i ochrony danych.
    - Zasady czystego biurka/ekranu: Ograniczenie widoczności danych na ekranach i w formie papierowej.
    - Procedury zarządzania incydentami: Plan postępowania w przypadku naruszenia ochrony danych (zgłaszanie, reagowanie, dokumentowanie, informowanie osób, których dane dotyczą).
    - Umowy powierzenia przetwarzania: Gdy dane są przetwarzane przez podmioty zewnętrzne (np. firmy statystyczne, dostawcy oprogramowania), niezbędne są umowy powierzenia zgodne z RODO.
6. Szkolenia i świadomość:
    - Obowiązkowe szkolenia: Regularne szkolenia dla całego personelu badawczego i wsparcia, dotyczące zasad ochrony danych i bezpieczeństwa.
    - Budowanie świadomości: Promowanie kultury bezpieczeństwa danych w zespole badawczym.
7. Fizyczne zabezpieczenia:
    - Ochrona pomieszczeń, w których znajdują się dane (serwery, archiwa papierowe) przed nieuprawnionym dostępem (np. kontrola dostępu, monitoring).

Skuteczne zabezpieczenie danych osobowych w badaniach naukowych jest procesem ciągłym i wymaga zintegrowanego podejścia, łączącego rzetelną analizę ryzyka i DPIA z wdrożeniem adekwatnych środków technicznych i organizacyjnych. Decyzje UODO, choć często ogólne, jasno wskazują, że niewystarczająca analiza ryzyka i brak podstawowych zabezpieczeń są głównymi przyczynami incydentów. Naruszenia często wynikają również z błędów ludzkich. UODO konsekwentnie podkreśla znaczenie



regularnych szkoleń dla wszystkich osób mających dostęp do danych, w tym personelu naukowego i technicznego.

## PODSUMOWANIE

Ochrona danych osobowych stanowi współcześnie jedną z kluczowych kwestii prowadzenia badań naukowych. Wiąże się to z faktem rosnącego znaczenia przetwarzania tych danych w ramach współczesnych badań naukowych, a co za tym idzie, pogłębiającej się interakcji pomiędzy zagadnieniami wykorzystywania danych osobowych i prowadzenia działalności naukowej. Kluczowe jest zapewnienie, że cele badawcze są realizowane w sposób, który jednocześnie chroni prawa i wolności osób fizycznych, których dane dotyczą, oraz buduje zaufanie publiczne do nauki. Wymaga to precyzyjnego zrozumienia i stosowania odpowiednich ram prawnych. Wyzwania związane z RODO w badaniach naukowych często wykraczają poza samą zgodność z przepisami. Wielokrotnie podkreśla się obciążenia administracyjne i brak jasnych wytycznych. Taka powtarzalność tych obserwacji wskazuje na problem o charakterze systemowym. Nie chodzi wyłącznie o złożoność samego aktu prawnego, lecz o trudności w jego praktycznej interpretacji i wdrażaniu, zwłaszcza w specyficznym kontekście badań naukowych.

W celu uproszczenia obowiązków formalnych związanych z przetwarzaniem danych osobowych należy opracować ustandaryzowane narzędzia i szablony, które wykorzystywać będą badacze, bez konieczności ciągłego tworzenia dokumentacji od nowa. Należy opracować modułowe szablony formularzy zgody oraz obowiązków informacyjnych, które można dostosować do różnych typów badań (np. ankiety, badania kliniczne, badania obserwacyjne), wzory umów powierzenia, listy kontrolne, które pozwolą dokonać wstępnej analizy ryzyka i określić czy potrzebna będzie np. ocena skutków dla ochrony danych (DPiA). Stworzenie wzorów pozwoli badaczom szybko tworzyć zgodne dokumenty dostosowane do ich konkretnych potrzeb projektowych, zmniejszając błędy i czas administracyjny, jednocześnie zapewniając spójność w podstawowym przekazie RODO w całej instytucji. Aby powyższe było możliwe niezbędne są również, tak często podkreślane przez PUODO, szkolenia personelu. Szkolenia powinny mieć na celu wdrożenie proaktywnej kultury ochrony danych, w której zgodność jest postrzegana jako integralna część etycznego prowadzenia badań, a nie

tylko przeszkoda regulacyjna. Zaangażowanie kierownictwa i wsparcie IOD są kluczowe w kształtowaniu tej kultury.

## BIBLIOGRAFIA


**Monografie i opracowania**

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

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.

Jagielski M. (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2022.

Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Legalis 2021.

Litwiński P. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz,* Warszawa 2021.

Lubasz D. (red.), *Meritum. Ochrona danych osobowych*, Wolters Kluwer, Warszawa 2022.

Woźnicki J. (red.), *Prawo o szkolnictwie wyższym i nauce. Komentarz*, Wolters Kluwer, Warszawa 2019.

Woźnicki J. (red), *Identyfikacja i uzasadnienie kierunków regulacji o kluczowym znaczeniu w ustawie prawo o sokolnictwie wyższym i nauce*, Warszawa–Toruń 2020.

**Artykuły w czasopismach, publikacjach nieperiodycznych**

Jagielski M., *Ochrona danych osobowych jako element oceny etycznej badań naukowych z udziałem ludzi*, [w:] Diametros - An Online Journal of Philosophy, 2023, t.76.





Pyka A., *Przetwarzanie danych osobowych do celów badań naukowych. Aspekty prawne*, [w:] Studnia Prawa Publicznego 2019 • NR 4 (28).

**Źródła www**

https://www.rozwojspoleczny.gov.pl/strony/zasady-przetwarzania-danych-osobowych-w-programie-fundusze-europejskie-dla-rozwoju-spolecznego/ (dostęp 29.06.2025 r.)

https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/przewodnik-po-danych-osobowych-w-projektach-po-wer-dla-wnioskodawcow-i-beneficjentow/ (dostęp 29.06.2025 r.)

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (dostęp: 29.06.2025 r.)

https://uodo.gov.pl/pl/535/2506 (dostęp 29.05.2025 r.)

https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_pl (dostęp 29.05.2025 r.)

**Decyzje Prezesa Urzędu Ochrony Danych Osobowych**

ZSPR.421.3.2018 z dnia 15 marca 2019 r.

ZSOŚS.421.25.2019 (z 21 sierpnia 2020 r.)

DKN.5131.26.2023 z 30 listopada 2023 r.

**Wytyczne i Opinie Europejskiej Rady Ochrony Danych**

Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19

Wytyczne 7/2020 EROD w sprawie koncepcji administratora i podmiotu przetwarzającego w RODO, przyjęte 7.07.2021 r.,

Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, przyjęte 18.06.2021 r.

**Wytyczne i Opinie Grupy Roboczej Art. 29**

Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 z dnia 10 kwietnia 2018 r., WP259 rev.01, 17PL

**Akty prawne**

Karta Praw Podstawowych Unii Europejskiej, Dz.Urz.UE 2016 C 202

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 nr 78 poz. 483

Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1, ze sprost.) – RODO

Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce, Dz.U. 2018 poz. 1668



## ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У НАУКОВИХ ДОСЛІДЖЕННЯХ ТА РЕАЛІЗАЦІЇ НАУКОВО-ДОСЛІДНИХ ПРОЄКТІВ

**(переклад з польської мови)**

### ВСТУП

Захист персональних даних у європейському культурному середовищі розглядається як одне з базових прав людини. Як право особи (право на захист персональних даних) воно включено як до конституцій європейських країн, так[43] і до чинних у Європі міжнародних нормативних актів та і до європейського законодавства[44]. Більш детальні правила захисту даних регулюються на законодавчому рівні. У країнах, що входять до Європейського Союзу, ці нормативні акти були уніфіковані шляхом прийняття спільного правового акту для всього співтовариства – Регламенту (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних (далі – GDPR, польська версія – RODO), який набув чинності з 25 травня 2018 року і також застосовується до обробки персональних даних для цілей наукових досліджень та виконання науково-дослідних проєктів[45]. Слід підкреслити, що це стосується як даних осіб, які

[43] Стаття 51 Конституції Республіки Польща (Dz.U.1997.78.483):
1. Ніхто не може бути зобов'язаний інакше, як на підставі Закону розголошувати інформацію, що стосується його особи. 2. Органи державної влади не мають права отримувати, збирати та надавати інформацію про громадян, крім необхідної в демократичній правовій державі. 3. Кожен має право доступу до офіційних документів і наборів даних, що його стосуються. Обмеження цього права може бути визначено законом. 4. Кожен має право вимагати виправлення та видалення інформації, яка є неправдивою, неповною або зібраною у спосіб, що суперечить закону. 5. Правила та порядок збору та обміну інформацією конкретизуються в Законі.

[44] Двома ключовими актами тут є: Конвенція про захист прав людини і основоположних свобод (це право було витлумачено зі статті 8 Конвенції) та Хартія основних прав Європейського Союзу (де це прямо виражено в статті 8)

[45] 159 GDPR безпосередньо стосується питання наукових досліджень: *«Якщо персональні дані обробляються з метою наукових досліджень, цей Регламент також повинен застосовуватися до такої обробки. У цьому Положенні обробку персональних даних для цілей наукових досліджень слід тлумачити широко, включаючи, наприклад, технологічний розвиток та демонстрацію, фундаментальні дослідження, прикладні дослідження та дослідження, що фінансуються приватним капіталом. Крім того, слід враховувати мету Союзу, викладену у статті 179(1) ДФЕУ, яка полягає у створенні Європейського дослідницького простору. Вираз «для цілей наукових досліджень» повинен також включати дослідження, що проводяться в інтересах суспільства у сфері громадського здоров'я. З огляду на специфіку обробки персональних даних для дослідницьких цілей, повинні застосовуватися спеціальні умови, зокрема щодо публікації або*

працевлаштовані у певному проєкті, так і осіб, які є об'єктом дослідження, незалежно від того, чи поширюється інформація про них будь-яким чином, наприклад, у рамках наукової публікації. Колишня Робоча група ст. 29 вже вказувала, що термін «наукові дослідження» не може виходити за межі його загальноприйнятого значення, і вважає, що в цьому контексті «дослідження» означає «дослідницький проєкт, організований відповідно до методологічних та етичних стандартів відповідного сектора та відповідно до належної практики».[46] GDPR визначає, серед іншого, правові підстави допустимості обробки персональних даних, загальні принципи їх обробки, обов'язки, що покладаються на контролерів, а також права суб'єктів даних. Суб'єкти, які проводять наукові дослідження або здійснюють дослідницькі проекти, які обробляють персональні дані з цією метою, зобов'язані застосовувати загальні правила, що регулюють, зокрема, обов'язки, що покладаються на контролерів, спільних контролерів або обробників, залежно від ролі, покладеної на них у конкретному випадку. Для забезпечення законності всіх дій, пов'язаних з обробкою персональних даних, дуже важливо, щоб як суб'єкти, які проводять наукові дослідження, так і особи, які займаються їх виконанням, володіли необхідними знаннями в цій сфері. Зокрема, в аспекті міжнародної діяльності, у тому числі за участю суб'єктів з-поза меж Європейського Союзу, питання не є простим.

Метою нашої експертизи є представлення питання обробки персональних даних для цілей наукових досліджень, зокрема в міжнародному аспекті, у світлі вимог GDPR. Ключовими питаннями, які будуть розглянуті: сфера застосування GDPR у територіальному аспекті, правила обробки персональних даних, правові основи обробки даних, визначення ролі суб'єктів, що обробляють персональні дані

*іншого розкриття персональних даних у контексті дослідницьких цілей. Якщо результат наукових досліджень, зокрема в контексті охорони здоров'я, виправдовує подальші заходи в інтересах суб'єкта даних, до таких заходів повинні застосовуватися загальні положення цього Регламенту».*

[46] Wytyczne Europejskiej Rady Ochrony Danych 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 byłej Grupy Roboczej Art. 29 z dnia 10 kwietnia 2018 r., WP259 rev.01, 17PL, s. 27 (poparte przez EROD) // Керівництво Європейської ради з питань захисту даних 03/2020 щодо обробки даних про здоров'я для наукових досліджень у контексті пандемії COVID-19, Керівництво щодо згоди відповідно до Регламенту 2016/679 колишньої статті 29 Робочої групи від 10 квітня 2018 року, WP259 rev.01, 17PL, p. 27 (підтримується EDPB).



(контролер/адміністратор, співконтролер/співадміністратор, обробник), формальні зобов'язання, пов'язані з обробкою даних та застосуванням відповідних гарантій.

## 1. Територіальна сфера застосування GDPR

На початку слід зазначити, що GDPR застосовується до Європейського Союзу в широкому інституційному аспекті. Це пов'язано з тим, що правовим захистом цього акта користуються як громадяни держав-членів, так і громадяни так званих третіх країн, які проживають на території ЄС[47].

Стаття 3 GDPR визначає його територіальну сферу, тобто ситуації, у яких положення регламенту застосовуються, навіть якщо обробник даних не створений в Європейському Союзі. Це один з основоположних принципів, який надає GDPR екстериторіальність, що означає, що сфера його дії виходить за межі ЄС. У контексті спільних досліджень або реалізації дослідницьких проєктів, що виконуються спільно суб'єктом ЄС (наприклад, польським університетом) та суб'єктом, що не є членом ЄС (наприклад, українським університетом), застосування GDPR до того останнього випливає з кількох ключових критеріїв, викладених у вищезазначеному положенні:

3. Критерій «організаційна одиниця» (ч. 1 ст. 3 GDPR).

«Цей Регламент застосовується до обробки персональних даних у контексті діяльності, що здійснюється установою контролера або оператора в Європейському Союзі, незалежно від того, чи відбувається обробка в ЄС чи ні». Навіть якщо український університет не має офіційної філії в Польщі, але його наукова діяльність здійснюється в рамках «ефективного та результативного виконання діяльності – навіть мінімальної – через стабільні домовленості» в ЄС (наприклад, у постійній співпраці з польським університетом, який можна вважати

[47] Пункт 2 GDPR «Принципи та правила щодо захисту фізичних осіб у зв'язку з обробкою їх персональних даних не повинні, незалежно від їх громадянства або місця проживання, порушувати їх основні права і свободи, зокрема право на захист персональних даних».
14 GDPR: «Захист, що надається цим Регламентом, повинен застосовуватися до фізичних осіб, незалежно від їх громадянства або місця проживання, щодо обробки їх персональних даних».

його «організаційною одиницею» в ширшому сенсі, або через присутність його співробітників у Польщі з науковою метою), це може стати основою для застосування GDPR.

4. Критерій «керівництво діяльністю» та «моніторингова поведінка» (стаття 3(2)(a) та (b) GDPR).

«Цей Регламент застосовується до обробки персональних даних суб'єктів даних, які проживають на території ЄС, контролером або обробником, не створеним у ЄС, де діяльність з обробки передбачає:

c) пропонування товарів або послуг таким суб'єктам даних у Євросоюзі, незалежно від того, чи зобов'язані вони платити; або
d) моніторинг їх поведінки, тією мірою, якою така поведінка має місце в Союзі».

GDPR застосовується до обробки персональних даних фізичних осіб, які знаходяться в Євросоюзі, контролером або оператором, не зареєстрованим у Союзі, якщо діяльність з обробки передбачає пропозицію товарів або послуг таким особам у Союзі. Участь у дослідженнях, особливо за участю учасників ЄС (наприклад, з Польщі), може бути витлумачена як «пропозиція послуги» (участь у дослідженні) цим особам, навіть якщо це не передбачає оплати. Якщо український університет самостійно або у співпраці з польським університетом набирає учасників опитування з Польщі чи інших країн ЄС, він «спрямовує свою діяльність» на людей, які перебувають у ЄС, що автоматично включає його до сфери дії GDPR. Положення Регламенту також застосовуються у випадках, коли діяльність з обробки передбачає моніторинг поведінки фізичних осіб, якщо їхня поведінка відбувається на території Союзу. Багато наукових досліджень, особливо в таких галузях, як психологія, соціологія, медицина або поведінкові науки, покладаються на моніторинг поведінки, звичок, здоров'я або інших аспектів життя учасників. Якщо цей моніторинг стосується людей, які перебувають на території ЄС (наприклад, за допомогою онлайн-опитувань, збору даних з носимих пристроїв, аналізу онлайн-активності), то український університет, як суб'єкт, що бере участь у цьому моніторингу, підпадає під дію GDPR.



Також слід наголосити, що навіть якщо український університет напряму не набирає учасників з ЄС, а отримує персональні дані від польського університету (який, як суб'єкт ЄС, має відповідати GDPR), обробка цих даних українським університетом також підпадає під дію GDPR. Польський університет, як контролер даних, зобов'язаний забезпечити, щоб усі передачі даних за межі Європейського економічного простору відбувалися відповідно до Глави V GDPR, що вимагає використання відповідних гарантій (зазвичай це будуть Стандартні договірні положення – SCC). На практиці це означає, що одержувач даних з-поза меж ЄС (український університет) повинен взяти на себе зобов'язання дотримуватися європейських стандартів захисту даних, включаючи правила обробки персональних даних.

## II. Принципи обробки персональних даних

Основні принципи обробки персональних даних містяться у початковій частині GDPR – у статті 5 (глава II) і передують іншим основоположним нормам, таким як передумови законності обробки даних (статті 6 і 9 GDPR). Така структура статей є цілеспрямованою і чітко вказує на ключову важливість нормативного акта. Будь-який суб'єкт, що здійснює обробку даних з метою наукових досліджень та реалізації дослідницьких проектів, зобов'язаний їх дотримуватися. Хартія основних прав Європейського Союзу встановлює такі принципи, яким має відповідати обробка персональних даних: справедливість, визначеність мети та [48]законність. GDPR додає до цього каталогу ще сім: прозорість, мінімізація даних, точність, обмеження зберігання, цілісність і конфіденційність, а також підзвітність.

*Перший принцип – законність, надійність та прозорість*. Цей принцип є нічим іншим, як зобов'язанням обробляти персональні дані на підставі передумов законності, передбачених статтею 6 або статтею 9 GDPR (детально розглянуто у наступному розділі). Справедливість і прозорість вказані в пунктах 39, 58 і 60 преамбули GDPR. Ці принципи будуть виконуватися шляхом реалізації

[48] Стаття 8(2) Хартії основних прав Європейського Союзу.

інформаційного обов'язаку перед суб'єктами даних (статті 13 і 14 GDPR) у стислій, зрозумілій формі, сформульованій зрозумілою і простою мовою. Питання обов'язку інформування розглянуто у розділі «Формальні зобов'язання, пов'язані з обробкою даних» цього дослідження.

*Другий принцип полягає в обмеженні мети обробки даних*. Персональні дані повинні збиратися для конкретних, явних і законних цілей і не оброблятися в подальший спосіб, несумісний з цими цілями. Винятком є подальша обробка даних для цілей архівації в інтересах суспільства, для цілей наукових чи історичних досліджень або для статистичних цілей. Цей принцип призначений для забезпечення того, щоб суб'єкти даних усвідомлювали мету, з якою їхні дані збираються та використовуються. Це запобігає неконтрольованому та непередбачуваному використанню персональних даних для цілей, відмінних від тих, на які було надано початкову згоду або які були правовою основою для обробки. У випадку з науковими дослідженнями GDPR вводить значні спрощення та певну гнучкість у застосуванні цього принципу, що має вирішальне значення для динаміки та довгострокового характеру дослідницької діяльності. Стаття 5(1)(b) у поєднанні зі статтею 89(1) GDPR передбачає, що подальша обробка персональних даних для наукових, історичних або статистичних дослідницьких цілей не вважається несумісною з початковими цілями, для яких дані були зібрані. Це означає, що дані, спочатку зібрані для іншої мети (наприклад, медичні дані, зібрані для лікування, адміністративні дані), пізніше можуть бути використані для наукових досліджень без необхідності отримання нової згоди на кожну нову дослідницьку мету, за умови дотримання відповідних умов. Це фундаментальне полегшення, яке дозволяє повторно використовувати цінні набори даних, що має вирішальне значення для наукового прогресу. Гнучкість у принципі обмеження мети наукових досліджень пов'язана з абсолютною вимогою впровадження відповідних технічних та організаційних гарантій. Ці гарантії призначені для захисту прав і свобод суб'єктів даних. Далі ми розглянемо цю тему більш детально.

*Третім принципом* за статтею 5 GDPR, є *мінімізація даних*. Згідно з ним, обсяг оброблюваних даних повинен бути таким, який необхідний для досягнення конкретної мети обробки даних. При обробці даних з метою проведення наукових



досліджень і виконання науково-дослідних проектів необхідно відбирати дані і відбирати тільки ті, які адекватні досягненню поставленої мети.

*Четвертий – це принцип точності даних*, який вказує на те, що оброблювані персональні дані повинні бути точними і, при необхідності, оновлюватися. Необхідно розробити відповідні технічні та організаційні рішення для виправлення неправильних або застарілих даних. Цей принцип пов'язаний із правом особи, чиї дані ми обробляємо, виправляти свої дані[49].

*П'ятий принцип,* найбільш проблематичний для всіх суб'єктів, що обробляють персональні дані, - *це обмеження зберігання даних (принцип обмеженості часу)*. Цей принцип зводиться до того, що період обробки даних повинен бути обмежений часом, який необхідний для досягнення закладеної мети обробки даних. Після закінчення цього терміну дані мають бути видалені – оброблені як у паперовому, так і в електронному вигляді[50]. GDPR, а також національне законодавство Польщі вводять деякі специфічні правила щодо зберігання даних у контексті наукових досліджень, які враховують їх довгостроковий характер та цінність для суспільства. GDPR дозволяє зберігати персональні дані довше, ніж це необхідно для початкових цілей, за умови, що дані обробляються виключно для цілей архівації в інтересах суспільства, для цілей наукових або історичних

[49] Відповідно до статті 16 GDPR: «суб'єкт даних має право вимагати від контролера негайного виправлення неточних персональних даних, що стосуються його/її. Беручи до уваги цілі обробки, суб'єкт даних має право вимагати заповнення неповних персональних даних, у тому числі шляхом надання додаткової заяви». Можна виділити дві форми виправлення даних: ректифікацію, що розуміється як виправлення неправильних даних, і ректифікацію, що розуміється як доповнення неповних даних. При цьому він передбачає запит на виправлення та запит на доповнення – а не саме спростування та доповнення. Формулювання цього положення таким чином чітко вказує на те, що пов’язаний із цим обов'язок контролера не є абсолютним, і контролер може відмовитися враховувати запити суб'єкта даних у певних ситуаціях. M. Czerniawski, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, доступ: LEX. Порушення може полягати в невідповідності фактичному стану, застарілості, неправильному запису або інших дефектах, які роблять дані неправдивими. Це можуть бути як друкарські помилки, так і ситуації, коли дані вже не дійсні (наприклад, зміна місця проживання, зміна імені, зміна контактних даних). . Fajgielski, *Komentarz do rozporządzenia nr 2016/679 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)*, [w:] idem, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, доступ: LEX. Zob. więcej: A. Mrozowska, Dział XIVa *Przetwarzanie danych osobowych*, [w:] Woźnicki J. (red.), *Prawo o szkolnictwie wyższym i nauce. Komentarz*, Wolters Kluwer, Warszawa 2019.

[50] А. Мрозовська, *Захист персональних даних у вищій освіті* [у:] Ю. Возніцький (ред.), *Виявлення та обґрунтування напрямів регулювання ключового значення в Законі про вище соколине полювання та науку*, Варшава–Торунь 2020, с. 174-175.

досліджень або для статистичних цілей за умови впровадження відповідних технічних та організаційних [51]заходів. Це означає, що дані можуть зберігатися довше, якщо вони використовуються для продовження досліджень, перевірки результатів або формування основи для майбутніх аналізів за умови їх належного захисту. Польські нормативні акти в цьому відношенні більш точні. Відповідно до статті 469b(4) Закону «Про вищу освіту і науку», персональні дані, оброблені для цілей наукових досліджень або дослідно-конструкторських робіт, повинні бути анонімізовані негайно після досягнення мети наукового дослідження або дослідно-конструкторської роботи. Як вказують добрі практики, дослідницькі установи повинні розробити детальні плани управління даними (DMP), які чітко окреслюють політику зберігання та видалення даних для кожного дослідницького проекту. Принцип обмеженого зберігання тісно пов'язаний з правом на видалення даних («право на забуття»)[52]. Як правило, суб'єкт даних має право вимагати видалення своїх даних, коли вони більше не потрібні для цілей, для яких вони були зібрані, або коли він відкликав свою згоду і немає інших правових підстав. Однак GDPR передбачає виняток із права на забуття, якщо обробка необхідна для цілей архівування в інтересах суспільства, для наукових чи історичних досліджень або для статистичних цілей відповідно до статті 89(1) GDPR, якщо здійснення цього права може запобігти або серйозно ускладнити досягнення цілей такої обробки. Це означає, що за певних обставин, навіть якщо учасник дослідження подає запит на видалення своїх даних, контролер може мати право продовжувати їх зберігання, якщо це необхідно для цілісності та цілей наукового дослідження, за умови впровадження відповідних заходів безпеки даних.

Ще один принцип, який ми виділяємо в статті 5 GDPR – *це цілісність і конфіденційність* даних. Згідно з ним, персональні дані повинні оброблятися таким чином, щоб забезпечити їх відповідну безпеку, включаючи захист від несанкціонованої або незаконної обробки та випадкової втрати, знищення або пошкодження, за допомогою відповідних технічних або організаційних заходів. Тим не менш, на підставі рішення Голови Офісу із захисту персональних даних, передової практики та керівних принципів Європейської ради з питань захисту

[51] Стаття 5(1)(e) GDPR.
[52] Стаття 17(3)(d) GDPR



даних можна вказати на гарантії, які слід враховувати зокрема. Це буде розглянуто у підрозділі «Захист персональних даних при наукових дослідженнях і реалізації наукових проектів» нашої експертизи.

*Принцип підзвітності* є основою для всіх перерахованих вище принципів – у ньому зазначено, що контролер несе відповідальність за їх виконання і повинен бути в змозі продемонструвати їх дотримання. Кожен суб'єкт господарювання, який проводить наукові дослідження та проводить науково-дослідні проекти, повинен впроваджувати такі процедури та використовувати такі інструменти, які дозволять йому виконати цей обов'язок.

Крім основних, загальних принципів, що випливають зі статті 5 GDPR, діють два нових принципи, що породжують обов'язок контролерів враховувати захист даних на етапі проєктування/підготовки (*privacy by design*) і впроваджують засади конфіденційності за замовчуванням (*privacy by default*) – стаття 25 GDPR. Ці засади означають обов'язок враховувати захист персональних даних та конфіденційність суб'єктів даних на кожному етапі створення та існування системи (процедур, документації, програмного та апаратного забезпечення) для обробки персональних даних. Політика конфіденційності повинна бути частиною будь-якого проєкту, що передбачає обробку персональних даних таким чином, щоб конфіденційність, захист приватності була його частиною із самого початку. GDPR покладає на нас обов'язок запобігати, а не просто вживати коригувальних заходів[53].

## III. Правові засади обробки даних у наукових дослідженнях та реалізації наукових проектів

GDPR містить дві групи передумов, виконання яких є необхідною умовою реалізації проєкту/дослідження згідно з вимогами чинного законодавства в обробці персональних даних:

[53] Там же, с. 176.

a) перша стосується звичайних персональних даних (ст. 6),
b) друга – особливих категорій персональних даних (ст. 9).

Обробка персональних даних для цілей наукових досліджень та реалізації дослідницьких проектів може передбачати як обробку «звичайних даних», даних спеціальних категорій,[54] так і персональних даних, що стосуються кримінальних засуджень та кримінальних злочинів (ст. 10 GDPR). Загальний регламент не містить окремих положень щодо підстав для легалізації обробки даних у формі кримінальних засуджень та заборонених діянь, тому тут застосовуватиметься положення статті 6(1) Загального регламенту. Таким чином, при розгляді можливості застосування певних підстав для легалізації обробки даних слід враховувати як статтю 6(1), так і статтю 9(2) GDPR[55]. Обробка персональних даних підпадає під принцип загального дозволу на обробку звичайних даних, коли виконується хоча б одна з умов статті 6(1) GDPR, тоді як у випадку спеціальних категорій персональних даних застосовується принцип загальної заборони на обробку конфіденційних даних, якщо не застосовується будь-який із винятків, що дозволяють таку обробку відповідно до статті 9(2) GDPR. Перелік передумов для легалізації звичайних та спеціальних категорій персональних даних є вичерпним.

Передумовами для легалізації звичайної обробки даних є:

a) згода суб'єкта даних, що охоплює обробку для однієї або декількох цілей;
b) необхідність обробки для виконання договору, стороною якого є суб'єкт даних, або для вжиття заходів на вимогу цієї особи до укладення договору;
c) необхідність обробки для дотримання юридичного зобов'язання по стороні контролера;
d) необхідність обробки для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи;

[54] До особливих категорій персональних даних належать персональні дані, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство в профспілках, генетичні дані, біометричні дані (обробляються з метою однозначної ідентифікації фізичної особи), дані, що стосуються здоров'я, статевого життя або сексуальної орієнтації – стаття 9(1) GDPR. Цей перелік є закритим, решта даних вважається «звичайними даними».
[55] A. . Pyka, *Przetwarzanie danych osobowych do celów badań naukowych. Aspekty prawne*, [w:] Studnia Prawa Publicznego 2019 • NR 4 (28), c. 81-82.



e) необхідність обробки для виконання завдання, що виконується в інтересах суспільства або при здійсненні офіційних повноважень, покладених на контролера;
f) необхідність обробки для цілей законних інтересів контролера або третьої сторони, за винятком випадків, коли ці інтереси переважають інтереси або основні права та свободи суб'єкта даних, які вимагають захисту персональних даних, зокрема, якщо суб'єктом даних є дитина.

Особливу увагу слід приділити особливим категоріям даних, які часто називають чутливими даними. Відповідно до статті 9 GDPR, до цієї категорії належать дані, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство в профспілках, генетичні дані, біометричні дані, оброблені з метою однозначної ідентифікації фізичної особи, дані про здоров'я, дані, що стосуються статевого життя або сексуальної орієнтації. Ці дані вважаються «особливими» через їх надзвичайно конфіденційний характер та високий ризик дискримінації, стигматизації або порушень прав людини у разі їх неналежної обробки. До їх обробки висуваються більш суворі законодавчі вимоги.

Передумови легалізації обробки особливих категорій даних:

a) явна згода суб'єкта даних на обробку персональних даних для однієї або кількох конкретних цілей – Регламент 2016/679 передбачає, що законодавство ЄС або національне законодавство може виключати можливість відмови від заборони на обробку описаних даних самим суб'єктом даних;
b) необхідність обробки для виконання зобов'язань і здійснення конкретних прав контролером або суб'єктом даних у сфері зайнятості, соціального забезпечення та соціального захисту, якщо це дозволено законодавством Союзу або національним законодавством, або колективним договором згідно з національним законодавством, що передбачає належний захист основних прав та інтересів суб'єкта даних;
c) необхідність обробки для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи, а суб'єкт даних фізично або юридично не здатний дати згоду;

d) обробка даних фондом, неурядовою організацією або іншим некомерційним суб'єктом з політичними, ідеологічними, релігійними або профспілковими цілями в рамках дозволеної діяльності такого суб'єкта, що здійснюється з відповідними гарантіями та за умови, що обробка стосується лише членів або колишніх членів цього суб'єкта, або осіб, які підтримують з ним регулярні контакти у зв'язку з його цілями, і що дані не розголошуються за межами цього суб'єкта без згоди осіб, яких ці дані стосуються;
e) ситуація, коли дані були прямо оприлюднені самою особою, суб'єктом даних;
f) необхідність обробки судами з метою встановлення, слідства або захисту законних вимог або в рамках судових процедур;
g) необхідність обробки з міркувань важливого суспільного інтересу на основі законодавства ЄС або національного законодавства – ці причини повинні бути пропорційні закладеній меті, не повинні підривати суть права на захист даних, а також повинні існувати відповідні та конкретні заходи для захисту основних прав та інтересів суб'єкта даних;
h) необхідність обробки для цілей профілактичної охорони здоров'я або медицини праці, для оцінки працездатності працівника, для медичної діагностики, для надання медичної або соціальної допомоги, для лікування або для управління системами охорони здоров'я або соціальної допомоги та послугами на основі законодавства ЄС або національного законодавства, або відповідно до договору з медичним працівником;
i) необхідність обробки з міркувань суспільного інтересу в галузі громадського здоров'я, таких як захист від серйозних транскордонних загроз здоров'ю або забезпечення високих стандартів якості та безпеки медичних виробів та лікарських засобів, на основі законодавства ЄС або національного законодавства, що передбачає відповідні, конкретні заходи для захисту прав і свобод суб'єктів даних, зокрема професійну таємницю;
j) необхідність обробки для цілей архівування в інтересах суспільства, для цілей наукових та історичних досліджень або для статистичних цілей на основі законодавства ЄС або національного законодавства, яке є пропорційним закладеній меті, поважає суть права на захист даних і передбачає відповідні конкретні заходи для захисту основних прав та інтересів суб'єкта даних.



Правові передумови, зазначені як у статті 6(1) для звичайних персональних даних, так і в статті 9(2) для спеціальних категорій персональних даних, мають такий характер:

- автономний та
- рівний.

Автономність передумов для обробки є особливістю, яка робить достатнім базування обробки персональних даних виключно на одній з передумов. Рівність, у свою чергу, означає, що жодна з передумов не є переважною по відношенню до інших[56].

*Згода* є однією з найбільш часто використовуваних правових підстав у сфері наукових досліджень (стаття 6(1)(a) GDPR). Для того щоб бути дійсною, згода повинна відповідати кільком вимогам: бути добровільною, конкретною, свідомою та однозначною. Контролер повинен бути в змозі продемонструвати, що згода була надана. У наукових дослідженнях, де мета обробки даних може бути не до кінця визначена на момент збору даних, GDPR допускає можливість отримання так званої *широкої згоди* (*broad consent*). Це означає, що суб'єкти даних можуть дати згоду на обробку даних у межах певних сфер наукових досліджень або елементів дослідницьких проєктів, якщо ці дослідження відповідають визнаним етичним стандартам. Це забезпечує гнучкість у довгострокових дослідницьких проєктах[57]. Особа, якої стосуються ці дані, має право відкликати свою згоду в будь-який час, і цей процес відкликання згоди має бути таким же простим, як і її надання. Відкликання згоди не впливає на законність обробки на основі згоди до моменту відкликання. Після відкликання згоди контролер може більше не обробляти дані на

[56] D. Lubasz (red.), Meritum. Ochrona danych osobowych, Wolters Kluwer, Warszawa 2022 r., s. 120-121.Д. .
[57] 33 GDPR: «На момент збору даних часто неможливо повністю визначити мету обробки персональних даних для наукових цілей. Таким чином, суб'єкти даних повинні мати можливість дати згоду на певні галузі наукових досліджень, якщо дослідження відповідає визнаним етичним стандартам у наукових дослідженнях. Суб'єкти даних повинні мати можливість давати згоду лише на певні галузі досліджень або елементи дослідницьких проектів, якщо це дозволяє цільове призначення».

цій підставі та повинен видалити їх, якщо немає іншої правової підстави, яка дозволяє їх подальшу обробку (наприклад, юридичне зобов'язання). Відкликання згоди в наукових дослідженнях є особливо проблематичним, оскільки це може підірвати послідовність і надійність результатів. Дані в дослідженнях часто пов'язані одні з одними і є частиною більшого набору даних, що підлягають аналізу. Якщо учасник відкликає згоду, а його дані є невід'ємною частиною статистичної моделі або конкретного висновку, їх видалення може зробити недійсним або значно змінити результат дослідження. Це створює напругу між правами особи на дані та цілісністю і корисністю наукових досліджень. З цієї причини такі ситуації слід передбачати при розробці досліджень, наприклад, шляхом анонімізації даних якомога раніше або шляхом чіткого інформування учасників про вплив відмови від участі у використанні даних (наприклад, дані, які вже використовуються в агрегованій, знеособленій формі, не можна практично видалити з опублікованих результатів). Це також пояснює, чому «суспільний інтерес» часто є кращою правовою підставою для певних типів досліджень, оскільки він забезпечує більшу стабільність.

Обробка є законною, якщо вона необхідна для виконання завдання, що реалізується в інтересах суспільства (суспільний інтерес), або для здійснення повноважень публічного управління, покладених на контролера (стаття 6(1)(e) GDPR). Багато наукових досліджень, особливо тих, що проводяться державними установами, такими як університети, можуть ґрунтуватися на цій основі, якщо розглядати їх мету як служіння суспільному благу. У Польщі Закон «Про вищу освіту і науку» визнає проведення наукових досліджень закладами вищої освіти завданням, що служить суспільному благу. Вибір правової основи «суспільного інтересу» може значно спростити управління правами суб'єктів даних порівняно зі згодою. Коли згода є підставою для обробки персональних даних, суб'єкти даних мають сильне право відкликати згоду, що супроводжується зобов'язанням усунути дані. На противагу цьому, стаття 89(2) GDPR передбачає, що законодавство держав-членів може передбачати винятки з певних прав суб'єктів даних (права на доступ, виправлення, обмеження обробки, протесту) для дослідницьких цілей, якщо їх реалізація унеможливлює або серйозно перешкоджає досягненню цілей



дослідження. Це чітко пов'язано з обробкою в інтересах суспільства. Таким чином, підстава «суспільні інтереси» (також відповідно до національного законодавства, напр., стаття 469b Закону «Про вищу освіту та науку») забезпечує більш стабільну правову базу для довгострокових або великомасштабних дослідницьких проектів, де відкликання індивідуальної згоди може створювати великі проблеми. Це дещо зміщує баланс у бік мети дослідження за умови впровадження відповідних належних заходів.

Правовою основою для обробки персональних даних у рамках реалізації дослідницьких проєктів та наукових досліджень також може бути, відповідно до статті 6(1)(f) GDPR, «*законний інтерес контролера*». Ця правова база рідше використовується в наукових дослідженнях, а частіше використовується комерційними структурами. Він може використовуватися, коли дослідження служить приватним, а не суспільним інтересам, і не перевищують значущість прав та свобод суб'єкта даних. Така підстава вимагає проведення тесту на збалансованість між інтересами контролера та правами і свободами суб'єктів даних.

*Таблиця 1. Правові підстави для обробки персональних даних в рамках реалізації науково-дослідних проектів та проведення наукових досліджень*

| **Правові підстави** | **Стаття GDPR** | **Основні умови/вимоги до наукового дослідження** | **Наслідки для прав суб'єктів даних** | **Приклади використання в науці** |
|---|---|---|---|---|
| Згода | Стаття 6(1)(a) | Добровільна, конкретна, свідома й однозначна; можлива широка узгодженість напрямків досліджень; Обов'язок надати згоду. | Право відкликати згоду в будь-який час; необхідність видалення даних, якщо немає іншої правової підстави. | Опитування, інтерв'ю. |
| Суспільний інтерес[58] | Стаття 6(1)(e) | Обробка, необхідна для виконання завдання, що | Можливість обмеження прав | Епідеміологічні дослідження, |

[58] Стаття 469b Закону про наукові дослідження вказує на суб'єкти, які мають право обробляти дані з метою проведення наукових досліджень. Це: університети, наукові інститути Польської академії наук, науково-дослідні інститути, що діють відповідно до Закону від 30 квітня 2010 року про науково-дослідні інститути (Законодавчий вісник 2024 року, поз. 534), міжнародні наукові інститути, створені

| | | | | |
|---|---|---|---|---|
| | | виконується в інтересах суспільства; стосується, зокрема, державних установ (наприклад, університетів). | (доступ, виправлення, обмеження, протест) за національним законодавством (стаття 89(2)), якщо це перешкоджає дослідженню. | соціальні дослідження, що проводяться, наприклад, університетами, Польською академією наук. |
| Законний інтерес контролера | Стаття 6(1)(f) | Обробка необхідна для цілей законних інтересів контролера, за винятком випадків, коли інтереси або права фізичних осіб переважають. | Обов'язок проведення тесту на баланс; можливість заперечення з боку суб'єкта даних. | Дослідження ринку, внутрішнє дослідження в компаніях, приватне дослідження. |
| Подальша обробка в наукових цілях | Стаття 5(1)(b) у поєднанні зі Статтею 89(1) | Дані, спочатку зібрані з іншою метою; вважається таким, що відповідає початковим цілям; вимагає відповідних гарантій (псевдонімізація/ знеособлення). | Потрібна інформація про подальшу обробку (якщо це можливо); необхідність впровадження запобіжних заходів. | Повторне використання даних з медичних записів, адміністративних даних, архівів для нових наукових проектів. |

*Джерело: Власне дослідження*

Як правило, обробка даних спеціальних категорій заборонена через їхній конфіденційний характер і потенційний ризик дискримінації. Однак GDPR передбачає певні винятки з цієї заборони, які мають вирішальне значення для проведення наукових досліджень. Обробка чутливих персональних даних дозволяється, якщо це необхідно для цілей архівування в інтересах суспільства, для цілей наукових чи історичних досліджень або для статистичних цілей на основі законодавства ЄС або держави-члена. Це право має бути пропорційним закладеній меті, не порушувати суті права на захист даних та передбачати відповідні й конкретні заходи для захисту основних прав та інтересів суб'єкта даних. Крім того, обробка спеціальних категорій даних також дозволяється, якщо

на основі окремих актів, що діють на території Республіки Польща, Лукасевицький центр, інститути, що діють у межах Дослідницької мережі Лукасевич, Центр післядипломної медичної освіти, Польська академія мистецтв і наук.



суб'єкт даних дав свою явну згоду на обробку для однієї або кількох конкретних цілей.

Дані про стан здоров'я є однією з категорій чутливих даних, які найчастіше обробляються у наукових дослідженнях, особливо в клінічних дослідженнях. Обробка даних про здоров'я в наукових дослідженнях, хоча і має вирішальне значення для медичного прогресу, є сферою найвищого ризику в контексті GDPR, що вимагає багатовимірного юридичного та технічного підходу. Ці дані за своєю суттю є конфіденційними, чутливими і їх неправильне використання може призвести до серйозної дискримінації, стигматизації або іншої шкоди. Це робить обробку даних процесом із високим ризиком, який часто вимагає оцінки впливу на захист даних (DPIA). Рекомендації Європейської ради із захисту даних[59] уточнюють правила обробки даних про здоров'я для цілей наукових досліджень. Ці рекомендації вказують, що обробка даних про здоров'я в наукових дослідженнях може ґрунтуватися на згоді або національному законодавстві (стаття 9(2)(a) або (j)) з вимогою відповідних гарантій і професійної таємниці. Складність регулювання означає, що дослідники, які працюють з медичними даними, повинні дотримуватися не лише GDPR, але й конкретних національних нормативних актів (зокрема, статті 469b Закону про вищу освіту та науку) та відповідних галузевих норм. Вимога щодо «належних, конкретних заходів для захисту прав і свобод суб'єкта даних, зокрема професійної таємниці» (стаття 9(2)(i)) або «відповідних і конкретних заходів» (стаття 9(2)(j)) стосується не лише технічної безпеки, але й організаційних протоколів, етичної оцінки та чіткої комунікації, що робить дотримання досить складним викликом.

[59] Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19

## IV. Визначення ролі обробників персональних даних (контролер, співконтролер, інституція-обробник)

Однією з ключових проблем, з якою стикаються суб'єкти, що здійснюють обробку персональних даних у наукових дослідженнях та реалізації дослідницьких проєктів, є визначення їхньої ролі, оскільки кожна з них пов'язана з окремими зобов'язаннями, пов'язаними із GDPR. Більшість обов'язків, про які іде мова в цьому розділі, лежать на контролерах даних. Однак суб'єкт, який проводить дослідження або реалізує науковий проект, не завжди буде виступати в цій ролі.

Контролер (адміністратор) – це суб'єкт, який має право приймати рішення щодо персональних даних. Такий суб'єкт може набувати будь-якої організаційної форми – це може бути фізична особа, юридична особа, університет, фонд, неурядова організація, орган публічної влади чи будь-яка інша організація, якщо вона самостійно або спільно з іншими визначала цілі та способи обробки персональних даних[60].

Якщо хоча б два контролери спільно визначають цілі та методи обробки, ми маємо справу з відносинами спільного контролю (співадміністрування). Вони повинні визначити відповідні обов'язки та відносини між ними та суб'єктами даних за допомогою спільних домовленостей (стаття 26(1) та (2) GDPR). Положення GDPR не визначають форму, відповідну для домовленостей, укладених співконтролерами, зокрема, вони не вимагають письмової угоди. Співконтролери можуть вільно домовлятися про форму угоди, але вона повинна бути документально підтверджена, щоб відповідати принципу відповідальності, зазначеному в статті 5(2) GDPR[61].

[60] Стаття 4(7) GDPR: «контролер» означає фізичну або юридичну особу, державний орган, агентство або інший орган, який самостійно або спільно з іншими визначає цілі та засоби обробки персональних даних; якщо цілі та засоби такої обробки визначаються законодавством ЄС або держави-члена, контролер або конкретні критерії для його призначення також можуть бути визначені законодавством ЄС або держави-члена

[61] Див.: P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Legalis 2021, коментар до ст. 26 та література, зацитована в ній.



Стаття 26 GDPR передбачає мінімальні елементи угоди про спільне адміністрування даних (співконтроль), які водночас є обов'язковими. Це обов'язки сторін у сфері щодо:

- реалізації суб'єктом даних його прав та
- обов'язки співконтролерів щодо надання інформації, зазначеної у статтях 13 та 14 GDPR (інформаційні зобов'язання, див. наступний розділ).

У домовленостях може бути вказано контактна особа/пункт для суб'єктів даних. Основний зміст договору надається суб'єктам даних (стаття 26(2) GDPR). Європейська рада із захисту даних закликає до того, щоб угода також включала низку додаткових елементів. Пропозиції та рекомендації щодо переліку таких елементів випливає з Керівних принципів EDPB 7/2020[62]. Це положення, що стосуються: реалізації загальних принципів захисту даних (стаття 5 GDPR), правових підстав для обробки (стаття 6 GDPR), заходів безпеки (стаття 32 GDPR), повідомлення про витік персональних даних наглядовому органу та суб'єкту даних (стаття 33 та 34 GDPR), оцінка впливу на захист даних (статті 35 та 36 GDPR), оператора (стаття 28 GDPR), передача даних до третіх країн (глава V GDPR), організація контакту з суб'єктами даних та наглядовими органами, обмеження використання персональних даних з іншою метою одним із спільних контролерів[63].

Проводячи наукові дослідження самостійно, університет буде контролером даних. У разі проведення спільних досліджень ми, як правило, будемо мати справу з відносинами спільного адміністрування. Те ж саме стосується й організації наукової конференції декількома університетами/установами.

Від вищезазначених відносин слід відрізняти правову ситуацію інституції, яка обробляє персональні дані, тобто того суб'єкта, кому контролер доручає обробку персональних даних. Такий випадок виникне, коли контролер замість того, щоб самостійно виконати дію обробки, використовував для її виконання зовнішній суб'єкт. Саме такий зовнішній суб'єкт і буде називатися розпорядником

[62] Wytyczne 7/2020 EROD w sprawie koncepcji administratora i podmiotu przetwarzającego w RODO, przyjęte 7.07.2021 r.

[63] K. Palka-Bartoszek, *Współadministrowanie danymi osobowymi*, rozdział 8, M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2022 r., s.276-277. Там також більше інформації та шаблони угод про спільну обробку даними.

(процесором). Суб'єкт, який приймає такі функції, не набуває статусу контролера, оскільки він не має права приймати рішення щодо даних – він може робити з ними лише те, що контролер наказав йому зробити. Він також не отримає статусу співконтролера, оскільки не бере участі у визначенні цілей і методів обробки спільно з контролером. Навпаки, він буде зобов'язаний дотримуватися домовленостей, зроблених контролером у цьому відношенні, наприклад, щодо часу, місця та способу усунення даних. Те, що пов'язує контролера з розпорядником є договір або інший юридичний документ, на підставі якого контролер доручає розпоряднику виконувати завдання, пов'язані з обробкою персональних даних, що «належать» контролеру[64]. Це означає, що розпорядник оброблятиме такі дані, довірені йому контролером, з метою, встановленою контролером, і в порядку, визначеному контролером. Таким чином, розпорядник не є незалежним з точки зору діяльності, яку він здійснює – він діє від імені контролера[65].

Університет найчастіше виступатиме розпорядником у разі реалізації наукових проєктів, що фінансуються або співфінансуються із зовнішніх джерел. Це стосується, наприклад, Оперативної програми «Знання – освіта – розвиток» (POWER)[66] або у рамках Європейського фонду соціального розвитку (FERS).[67] У зв'язку з різноманіттям зовнішніх джерел фінансування наукових досліджень і науково-дослідних проектів завжди необхідно аналізувати документи, що визначають нормативно-правову базу того чи іншого проекту, зокрема нормативно-правові акти та керівні принципи. У них ми знайдемо відповідь на питання про те, як буде діяти бенефіціар/бенефіціари. Найчастіше договір доручення буде укладено з відповідною керівною інституцією або установою-посередником, у якому буде детально зазначено, які зобов'язання, пов'язані з обробкою та захистом персональних даних, будуть покладені на

[64] Найчастіше це буде договір про доручення обробки персональних даних.
[65] *Там же,* с. 27-28.
Стаття 4(8) GDPR: «обробник» означає фізичну або юридичну особу, державний орган, агентство або інший орган, який обробляє персональні дані від імені контролера;
[66] Детальніше: *Przewodnik po danych osobowych w projektach PO WER dla Wnioskodawców i Beneficjentów,* https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/przewodnik-po-danych-osobowych-w-projektach-po-wer-dla-wnioskodawcow-i-beneficjentow/ (доступ 29.06.2025)
[67] https://www.rozwojspoleczny.gov.pl/strony/zasady-przetwarzania-danych-osobowych-w-programie-fundusze-europejskie-dla-rozwoju-spolecznego/ (доступ 29.06.2025)



університет/університети. Доручення обробки даних також може відбуватися у разі передачі частини досліджень або аналітичної діяльності даних зовнішній організації (іншому університету, інституту).

Чітке визначення ролей (контролер, співконтролер, розпорядник/обробник) у дослідницьких проектах, особливо в складних, часто міжнародних партнерствах, має вирішальне значення для уникнення прогалин у відповідальності та забезпечення повної відповідності GDPR. У дослідницьких проектах часто беруть участь багато суб'єктів (наприклад, університети, лікарні, зовнішні лабораторії, окремі дослідники, спонсори). GDPR визначає різні ролі: контролер (визначає цілі та засоби), обробник/розпорядник (обробляє дані від імені контролера) та співконтролери (спільно визначають цілі та засоби). Відсутність ясності щодо ролей призводить до нечіткого поділу обов'язків. У разі витоку даних або невиконання прав суб'єкта даних важко визначити, хто несе відповідальність, що може призвести до перекладання відповідальності та недотримання правил. Тому, перш ніж розпочати обробку даних у рамках наукової співпраці, слід провести глибокий юридичний аналіз, щоб точно визначити роль кожної зі сторін (що відповідає реалізації *принципу privacy by design* – стаття 25 GDPR). Ця ясність має вирішальне значення для розробки юридично обов'язкових угод про обробку даних (для відносин між контролером і розпорядником) або договорів про спільне адміністрування (співконтроль). Цей проактивний крок мінімізує юридичні ризики, забезпечує підзвітність та оптимізує зусилля щодо дотримання вимог усіма залученими суб'єктами

## V. Офіційні зобов'язання, пов'язані з обробкою даних

Як зазначено, GDPR визначає принципи та правові основи для обробки персональних даних, а також формує конкретні правові рішення (формальні зобов'язання), яких зобов'язані дотримуватися всі суб'єкти, що здійснюють обробку персональних даних у своїй діяльності. Суб'єкти, що провадять наукову та дослідницьку діяльність, повинні дотримуватися їх, як і всім інші інституції,

адаптуючи засади їх виконання до специфіки своєї діяльності. Формальні зобов'язання можна поділити на загальні, що стосуються суб'єкта/установи, та конкретні, пов'язані з проведенням конкретного дослідження або реалізації проекту.

На рівні установи, що здійснює науково-дослідницьку діяльність (контролер даних, наприклад, університет), можна виділити такі зобов'язання, які є постійними і повинні виконуватися на постійній основі[68]:

1. розробка процедур оцінки ризиків та впливу на захист персональних даних (стаття 24(1), стаття 32(1) та стаття 35 GDPR);
2. розробка документації із захисту персональних даних, зокрема реєстру дій з обробки та шаблонів інших необхідних документів (стаття 5(2) та стаття 30 GDPR);
3. розробка правил поведінки у разі витоку персональних даних (ст. 33 GDPR);
4. створення інфраструктури, що відповідає вимогам безпеки персональних даних (ст. 32 GDPR);
5. укладення договорів доручення із зовнішніми суб'єктами, які обслуговують контролера (ст. 28 GDPR);
6. дотримання інформаційних зобов'язань (ст. 13 і 14 GDPR);
7. призначення спеціаліста (уповноваженого) з питань захисту даних (далі: DPO) (стаття 37 GDPR);
8. видача співробітникам дозволів на обробку даних, відповідне навчання працівників (ст. 29, ст. 4 п. 2 і ст. 25 GDPR).[69]

Другий тип вимог – це ті, які спрямовані на конкретну діяльність, пов'язану з обробкою даних, тобто в контексті дослідницької діяльності – ті, які стосуються конкретних досліджень/наукових проектів. Вони повинні бути реалізовані по кожному окремому проекту:

[68] M. Jagielski, *Ochrona danych osobowych jako element oceny etycznej badań naukowych z udziałem ludzi*, [w:] *Diametros - An Online Journal of Philosophy*, 2023, t.76, c. 5.
[69] Щодо необхідної документації див.: M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*



1. визначення правових підстав для обробки окремих категорій даних, у тому числі визначення того, чи буде необхідним отримання згоди на обробку даних та чи є плани щодо повторного використання раніше зібраних даних (так зване *вторинне використання*) (статті 6-7 GDPR);
2. визначення особливих категорій даних (так званих чутливих конфіденційних даних), які будуть оброблятися в рамках проекту (ст. 9);
3. визначення відносин окремих суб'єктів, які співпрацюють у рамках наукового проекту (контролери/співконтролери/розпорядники (обробники) та укладання відповідних договорів/домовленостей (статті 26 та 28 GDPR);
4. легалізація можливої передачі даних за межі Європейського економічного простору (ст. 44-49 GDPR)
5. підготовка інформаційних зобов'язань (ст. 13 і 14 GDPR);
6. проведення оцінки ризиків та, можливо, оцінки впливу на проект (так званий DPIA) або з використанням процедури попередніх консультацій (стаття 24(1), стаття 32(1) та статті 35-36 GDPR);
7. визначення методів забезпечення безпеки окремих процесів обробки, включаючи використання таких прийомів, як псевдонімізація та знеособлення (ст. 34 GDPR).[70]

У цій експертизі розглянемо дві основні формальні вимоги, про які слід подбати при реалізації конкретних дослідницьких проектів, а саме: легалізація можливої передачі за межі Європейського економічного простору та дотримання інформаційних зобов'язань.

[70] M. Jagielski, *Ochrona danych osobowych* ... c. 5-6.

## VI. Передача даних за межі Європейського економічного простору в рамках наукових досліджень та реалізації дослідницьких проектів

Сучасні наукові дослідження, особливо ті, що проводяться у великих масштабах і в рамках міжнародних консорціумів, у все більшому ступені базуються на зборі, обробці та обміні величезними масивами даних. Значна частина цих даних мають характер персональний, що створює складні проблеми для дослідників та наукових установ з точки зору дотримання правил захисту даних, зокрема GDPR. Операції з обробки персональних даних, що здійснюються в Європейському Союзі та, ширше, в Європейському економічному просторі, не вимагають впровадження додаткових вимог, крім тих, з якими ми маємо справу щодо процедур, що здійснюються на території однієї держави-члена (наприклад, на території Польщі). Це цілком зрозуміло в рамках GDPR, який уніфікує правила обробки даних в рамках ЄС (ЄЕП), забезпечуючи свободу передачі персональних даних всередині ЄС. Положення GDPR передбачають загальну заборону на передачу персональних даних третім країнам[71] та міжнародним організаціям. Звільнення від цієї заборони вимагає виконання однієї з таких умов:

- посилання на рішення Комісії про ствердження наявності у третій країні або міжнародній організації відповідного рівня системи захисту персональних даних (так зване рішення про адекватність) – стаття 45 GDPR;[72]
- використання відповідних гарантій, зокрема стандартних положень про захист даних або обов'язкових корпоративних норм – статті 46 та 47 GDPR;

[71] GDPR не містить визначення третьої країни, але слід враховувати, що будь-яка країна, яка не входить до складу ЄЕП, повинна розглядатися як така. Для отримання додаткової інформації дивіться *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe*. Komentarz, red. P. Litwiński, Warszawa 2021, s. 422; та P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2022, c. 523.

[72] Наразі до переліку увійшли: Швейцарія, Аргентина, Гернсі, острів Мен, Джерсі, Андорра, Ізраїль, Уругвай, Нова Зеландія, Канада (для операцій з обробки підпадає під дію Канадського закону про захист персональної інформації та електронних документів (PIPEDA), Фарерські острови, Японія, Сполучене Королівство Великої Британії та Північної Ірландії та Південна Корея. Список третіх країн і територій, які, на думку Комісії, відповідають відповідним вимогам, можна знайти за посиланням: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (доступ: 29.06.2025)



- використання будь-яких винятків (винятків від заборони передачі), передбачених статтею 49 GDPR, наприклад, експортер даних покладається на явну згоду суб'єкта даних, чиї дані мають бути передані до третьої країни[73].

Відповідно до статті 45(1) GDPR, передача персональних даних до третьої країни (міжнародної організації) може відбуватися, коли Комісія встановить, що конкретна третя країна (або конкретна міжнародна організація) забезпечує належний рівень захисту персональних даних. Прийняття Комісією позитивних *висновків* (*positive findings)* щодо певної третьої країни визначає, що ця країна забезпечує належний рівень захисту персональних даних у розумінні GDPR на своїй території. На практиці це означає, що коли дані мають бути передані до країни, на яку поширюється рішення Комісії про адекватність, немає необхідності використовувати інші механізми передачі, такі як угода про передачу[74].

За відсутності рішення про адекватність для відповідної третьої країни, передача персональних даних можлива за умови застосування «відповідних гарантій», які забезпечують забезпечені законом права та ефективні засоби правового захисту для суб'єктів даних (статті 46 і 47 GDPR) або використання винятку, зазначеного в статті 49 GDPR. На практиці найбільш часто використовуваним і найбільш адекватним механізмом у випадку наукового дослідження є стандартні договірні положення (SCC). Це модельні договірні положення, прийняті Європейською комісією, які сторони угоди про передачу даних повинні включити до своїх договорів, що забезпечить законність передачі за межі ЄЕП. Положення, що застосовуються, повинні бути прийняті та застосовані в повному обсязі. Неможливо виділити окремі положення або змішати положення з різних наборів пунктів. У разі необхідності можуть бути вжиті додаткові заходи для забезпечення належного рівня захисту даних під час передачі до третіх країн. З 27 червня 2021 року набуло чинності останнє імплементаційне рішення Комісії (ЄС) 2021/914[75] щодо стандартних договірних положень, відповідно до рішення Суду ЄС у справі

[73] D. Lubasz (red.), *Meritum* (...), там же, с. 369.

[74] *Там же*, с. 374.

[75] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32021D0914&from=EN

Schrems II (C-311/18). Договірні положення охоплюють різні сценарії передачі даних, а саме:

- передача даних між контролерами,
- передача даних контролером обробнику в третій країні,
- передача даних між розпордядниками,
- передача даних обробником контролеру в третю країну[76].

Однак після рішення у справі Schrems II простого застосування SCC вже недостатньо. Експортер даних повинен провести оцінку впливу на передачу даних TIA (TIA - Transfer Impact Assessment). TIA – це юридичний та фактичний аналіз правової системи третьої країни, спрямований на оцінку того, чи будуть договірні положення ефективними на практиці, особливо в контексті можливості доступу до даних державних органів. Європейська рада із захисту даних визначила шестиетапний процес TIA, що включає, зокрема й інші, розуміння передачі, визначення інструменту передачі, оцінку його ефективності, прийняття додаткових заходів, вжиття необхідних процедурних кроків та повторну оцінку. Це свідчить про те, що дотримання GDPR для передачі даних вимагає не лише формального використання інструментів, а й постійної, проактивної оцінки ризиків[77].

## VII. Інформаційні зобов'язання

Окремим питанням є дотримання контролером інформаційних зобов'язань, які є ключовими для забезпечення прозорості та поваги до прав суб'єктів даних. Це зобов'язання застосовується незалежно від правових підстав для обробки, охоплюючи всі передумови відповідно до статті 6 і статті 9 GDPR. Важливо, що це також стосується даних, отриманих пасивним способом, таких як файли cookie або інші технології відстеження, які можуть бути використані в наукових дослідженнях

[76] https://uodo.gov.pl/pl/535/2506 (доступ 29.05.2025)
[77] Див. Рекомендація EDPB 01/2020 щодо заходів щодо доповнення інструментів передачі для забезпечення відповідності рівню захисту персональних даних ЄС, прийнята 18 червня 2021 року, доступна за адресою: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_pl



(наприклад, аналіз поведінки користувачів на дослідницьких платформах). GDPR розрізняє дві основні ситуації, у яких виникає зобов'язання щодо надання інформації: коли дані збираються безпосередньо від суб'єкта даних (стаття 13 GDPR) і коли дані отримані іншими способами, наприклад, від третьої сторони або із загальнодоступних джерел (стаття 14 GDPR). Якщо персональні дані для цілей наукового дослідження збираються безпосередньо від учасників, контролер (суб'єкт, який проводить дослідження, наприклад, університет, інститут) зобов'язаний надати їм низку інформації на момент збору даних:

- Ідентифікаційні дані та контактні дані контролера (і, якщо застосовно, його представника).
- Контактні дані інспектора із захисту даних (DPO), якщо його призначено.
- Цілі обробки персональних даних – має бути чітко зазначено, з якою метою дані будуть використовуватися в науковому дослідженні. У випадку з науковими дослідженнями GDPR (пункт 33) допускає певну гнучкість у визначенні мети, оскільки він часто не повністю ідентифікується на етапі збору даних. У таких випадках суб'єкти повинні мати можливість дати згоду на «певні галузі наукових досліджень» за умови, що дослідження відповідає визнаним етичним стандартам.
- Правові підстави для обробки – наприклад, зверніть увагу, що згода на обробку персональних даних для дослідницьких цілей повинна бути чітко відокремлена від згоди на участь у самому дослідженні.
- Права людини – суб’єкта (власника):
    - Право на доступ (ст. 15 GDPR).
    - Право на виправлення (ст. 16 GDPR).
    - Право на видалення («право на забуття») (стаття 17 GDPR) – включаючи винятки для дослідницьких цілей (стаття 17(3)(d) GDPR).
    - Право на обмеження обробки (ст. 18 GDPR).
    - Право на заперечення проти обробки (стаття 21 GDPR – якщо обробка ґрунтується на суспільних інтересах або законних інтересах контролера – стаття 6(1)(e) або (f)) – у випадку наукового дослідження

важливо мати на увазі специфіку, оскільки ці дані часто необхідні для цілісності дослідження.
    - Право на перенесення даних (ст. 20 GDPR) – досить рідко застосовується в наукових дослідженнях.
    - Право відкликати згоду в будь-який час (якщо обробка ґрунтується на згоді), не впливаючи на законність обробки на основі згоди до її відкликання.
    - Право на подання скарги до наглядового органу (голови Управління з питань захисту персональних даних).
- Період, протягом якого будуть зберігатися персональні дані, а якщо це неможливо, критерії визначення цього періоду (наприклад, 5 років після завершення дослідницького проекту).
- Інформація про те, чи є надання даних законодавчою або договірною вимогою, а також про наслідки його ненадання.
- Інформація про одержувачів персональних даних (наприклад, фінансові установи, розпорядники контролера).
- Інформація про намір передати дані третій країні (за межами Європейського економічного простору) або міжнародній організації. Ви також повинні повідомити про визначення або невизначення Європейською комісією належного рівня захисту даних у вашій країні або про використані гарантії (наприклад, стандартні договірні положення)
- Інформація про автоматизоване прийняття рішень, включаючи профілювання (як зазначено в статті 22(1) та (4) GDPR), і, принаймні в цих випадках, відповідну інформацію про принципи прийняття рішень, а також про значимість і передбачувані наслідки такої обробки для суб'єкта даних.

Стаття 13(4) GDPR передбачає важливий виняток із зобов'язання щодо інформації: виняток застосовується, якщо суб'єкт даних уже має всю необхідну інформацію. Контролер повинен бути в змозі продемонструвати, що особа дійсно володіє всією необхідною інформацією; простого припущення або презумпції того, що особа може володіти інформацією, недостатньо. Цей виняток може застосовуватися до всіх або частини зобов'язань щодо інформації. Тягар доведення лежить на



адміністраторі/контролері, а це означає, що покладатися на цей виняток ризиковано, якщо немає незаперечних доказів попереднього повного розкриття інформації.

Приклад інформаційного повідомлення:

*Ми хотіли б повідомити Вам, що у зв'язку з Вашою участю у науковому дослідженні під назвою «Освіта в Польщі: аналіз рівня освіти мешканців сільської та міської місцевості», Ваші персональні дані будуть оброблятися відповідно до положень Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (загальний вигляд Регламент про захист даних, далі: GDPR). Адміністратором Ваших персональних даних, що обробляються в рамках цього наукового дослідження, є Університет, Krakowskie Przedmieście 26/28, 00-927 Warsaw. Ви можете зв'язатися з нами по електронній пошті за адресою badania@uw.edu.pl. Ваші персональні дані будуть оброблятися з метою участі в науковому дослідженні «Освіта в Польщі: аналіз рівня освіти жителів сільської та міської місцевості» та анонімної публікації результатів дослідження. Правовою основою для обробки ваших персональних даних є стаття 6(1)(e) GDPR у зв'язку зі статтею 469b Закону про вищу освіту і науку, тобто обробка необхідна для виконання завдання, що виконується в інтересах суспільства (проведення наукових досліджень державним університетом). Одержувачами даних будуть Варшавський технологічний університет із зареєстрованим офісом на площі Політехніка 1 у Варшаві (аналіз даних) та Google LLC із зареєстрованим офісом у Маунтін-В'ю. Дослідження проводиться з використанням форм та дисків, наданих компанією Google (сервіс Google G-Suite для освіти), з якою Варшавський університет підписав угоду про доручення обробки персональних даних. Як наслідок, ваші персональні дані можуть оброблятися в дата-центрах Google, які можуть бути розташовані за межами Європейського економічного простору – у США. У цьому випадку передача ґрунтується на стандартних*

*договірних положеннях, затверджених Європейською комісією, що забезпечують належний рівень захисту даних. Ваші персональні дані у зв'язку з участю в дослідженні будуть оброблятися протягом усього періоду дослідження – 12 місяців. Після закінчення дослідження Ваші персональні дані будуть видалені або анонімізовані таким чином, що Вас неможливо буде ідентифікувати. Результати дослідження будуть оприлюднені лише в анонімній формі. Адміністратор призначив Інспектора (спеціаліста) з питань захисту даних, з яким ви можете зв'язатися електронною поштою за адресою: iod@adm.uw.edu.pl. Ви можете звертатися до DPO з усіх питань, пов'язаних з обробкою ваших персональних даних Варшавським університетом та реалізацією ваших прав, пов'язаних з обробкою персональних даних. При цьому завдання ОПО не полягає в наданні інформації про сам аудит.*

*Ви маєте такі права:*

- *Право на доступ (стаття 15 GDPR) – ви маєте право отримати підтвердження того, чи обробляємо ми ваші персональні дані, і якщо так, то отримати доступ до них та інформацію про їх обробку.*
- *Право на виправлення (ст. 16 GDPR) – ви маєте право вимагати виправлення неправильних персональних даних без невиправданої затримки або заповнення неповних даних.*
- *Право на видалення («право на забуття») (ст. 17 GDPR) – ви маєте право вимагати видалення ваших персональних даних у певних ситуаціях. Однак ми повідомляємо вам, що це право не застосовується, якщо обробка необхідна для цілей наукового дослідження, оскільки існує ймовірність того, що здійснення цього права завадить або серйозно ускладнить досягнення цілей такої обробки.*
- *Право на обмеження обробки (ст. 18 GDPR) – ви маєте право вимагати обмеження обробки даних у певних ситуаціях (наприклад, коли ви оскаржуєте точність даних).*
- *Право на заперечення проти обробки (стаття 21 GDPR) – ви маєте право заперечувати проти обробки ваших персональних даних, якщо підставою для обробки є суспільний інтерес або законний інтерес контролера. У цьому випадку контролер може продовжити обробку, якщо він продемонструє переконливі законні підстави, які переважають ваші інтереси, права та свободи.*
- *Ви також маєте право подати скаргу до Голови Управління з питань захисту персональних даних, якщо вважаєте, що обробка ваших персональних даних порушує положення GDPR.*

*Надання персональних даних у формі є добровільним, проте необхідним є участь у науковому дослідженні. Відмова від надання даних завадить вам взяти участь у проєкті. Ваші персональні дані не будуть підлягати автоматизованому прийняттю рішень, включаючи профілювання.*

Стаття 14 GDPR регулює інформаційні зобов'язання, коли персональні дані були отримані не безпосередньо від суб'єкта даних, а з інших джерел. Це може мати місце в наукових дослідженнях, коли дані отримуються з загальнодоступних баз даних та реєстрів (наприклад, CEIDG), від інших адміністраторів (наприклад, з медичних реєстрів, архівних даних) або від іншої особи. Окрім інформації, що вимагається статтею 13 GDPR, контролер повинен надати суб'єкту даних таку додаткову інформацію:

- Категорії відповідних персональних даних (наприклад, демографічні дані, дані про здоров'я, дані про поведінку, генетичні дані). Необхідно вказати, який тип даних був отриманий.
- Джерело персональних даних і, де це застосовно, чи надходять вони із загальнодоступних джерел. Це ключова інформація, яка відрізняє статтю 14 від статті 13 і має важливе значення для повної прозорості.

Ефективність інформаційного обов'язку значною мірою залежить від способу його виконання, який регулюється статтею 12 GDPR. Це положення встановлює загальні правила надання інформації, які застосовуються як до даних, зібраних безпосередньо (ст. 13), так і опосередковано (ст. 14). Інформація повинна бути подана в стислій, прозорій, зрозумілій і легкодоступній формі, з використанням

зрозумілої і простої мови. Це особливо важливо в наукових дослідженнях, де часто зустрічаються складні медичні, психологічні або технічні терміни. Мова повинна бути адаптована до потреб і можливостей реципієнтів, щоб кожен учасник дослідження, незалежно від його освіти або знання спеціалізованої термінології, міг повністю розуміти, на що він дає згоду і які наслідки обробки його даних.

Зобов'язання щодо розкриття інформації відповідно до статей 13 і 14 GDPR є фундаментальним елементом захисту персональних даних і є ключовими для забезпечення прозорості та контролю за даними в наукових дослідженнях. Їх правильне виконання є не лише юридичною вимогою, а й етичною, що вибудовує довіру між дослідниками та учасниками. Порушення нормативно-правових актів у цій сфері може спричинити за собою накладення високих фінансових санкцій з боку контролюючих органів. Управління з питань захисту персональних даних у Польщі вже наклало значний штраф (943 470,00 злотих) за порушення статті 14(1) та (2) GDPR[78]. Крім фінансових санкцій, недотримання їх може призвести до серйозної репутаційної шкоди науковим установам та окремим дослідникам. Втрата довіри громадськості може перешкоджати набору учасників для майбутніх досліджень і негативно впливати на можливості співпраці.

У контексті виконання формальних зобов'язань слід пам'ятати, що GDPR містить спеціальний регламент, що стосується обробки даних з метою проведення наукових досліджень, так звані наукові винятки. Їх суть полягає в тому, що в обмін на впровадження відповідних гарантій прав і свобод суб'єктів даних, суб'єкти, які використовують дані в дослідницьких цілях, звільняються від обов'язку дотримуватися певних зобов'язань і відповідати певним вимогам[79]. При цьому як необхідні гарантії, так і обсяг винятків регулюються одночасно GDPR та положеннями національного законодавства Польщі: Закону про вищу освіту та науку. Найважливішими привілеями, зазначеними в цьому рішенні, є:

[78] Decyzja PUODO ZSPR.421.3.2018 z dnia 15 marca 2019 r. (Рішення Голови Управління з питань захисту персональних даних ЗСПР.421.3.2018 від 15 березня 2019 року)
[79] Стаття 89(1) GDPR



1. можливість використання раніше зібраних даних для інших цілей для дослідницьких цілей (так зване *вторинне використання)* (стаття 5(1)(b) GDPR);
2. можливість продовження терміну зберігання даних (ст. 5(1)(e) GDPR);
3. можливість отримання згоди суб'єкта даних на використання даних, незважаючи на неможливість точно визначити мету їх використання (так звана територіальна згода) (стаття 4(11) та стаття 7 GDPR, у зв'язку з пунктом 33 GDPR);
4. можливість використання спеціальної правової норми для обробки особливих категорій даних (стаття 9(2)(j) GDPR та стаття 469b(2) Закону «Про вищу освіту і науку»);
5. можливість уникнення необхідності дотримання зобов'язання щодо надання інформації (стаття 14(5)(b) GDPR);
6. можливість відмови у видаленні даних (стаття 17(3)(d) GDPR); можливість уникнення необхідності дотримання зобов'язань, що випливають з наступних прав суб'єктів даних: право на доступ до даних (стаття 15), право на виправлення (стаття 16), право на обмеження обробки (стаття 18) та право на протесту (стаття 21) (стаття 89(2) GDPR та стаття 469b(1) Закону про вищу освіту та науку).[80]

Представлені винятки створюють особливий режим обробки персональних даних для дослідницьких цілей, що підтверджує привілейований статус положень GDPR. Його ідея полягає в тому, щоб сприяти науковим дослідженням, забезпечуючи при цьому захист прав і свобод суб'єктів даних. Саме тому можливість використання зазначених винятків завжди обтяжена необхідністю виконання вимог, що захищають права і свободи учасників дослідження. Вони конкретизуються у вищезазначених положеннях. Для кращого захисту суб'єктів даних ці положення повинні строго тлумачитися і не повинні зловживатися. Їх застосування не може позбавити ці суб'єкти захисту, на який вони мають право.

Підсумовуючи, варто зазначити, що структура нормативного регулювання наукової діяльності у розрізі GDPR є дворівневою. Суб'єкти наукової дільності повинні

[80] M. Jagielski, Ochrona danych osobowych(...) ibidem, c. 5.

спочатку відповідати загальним вимогам GDPR щодо обробки персональних даних (перший рівень). Це вимоги, які мають інституційний характер, тобто стосуються способу функціонування наукової установи, та вимоги, присвячені конкретним починанням, таким як дослідницькі проекти або здійснення наукових досліджень. Незважаючи на те, що імплементація цих вимог має бути адаптована до типу веденої діяльності, ці вимоги мають загальний характер, тобто суб'єкти, які проводять дослідження, розглядаються як усі інші суб'єкти, зобов'язані застосовувати GDPR для їх реалізації. Нормативні акти ЄС та національне законодавство також містять спеціальні рішення, розроблені спеціально для цілей обробки персональних даних у дослідницьких цілях – так звані винятки з досліджень (другий рівень). Їх метою є полегшення наукової діяльності, а тому вони призначені для використання при дотриманні вимог щодо проведення такої діяльності[81].

## VIII. Захист персональних даних у наукових дослідженнях та реалізації дослідницьких проектів

GDPR змінив підхід до захисту персональних даних на проактивний, що базується на оцінці ризиків. Не існує універсальних рішень, які можна використовувати – кожен контролер даних, тобто наразі кожен університет, повинен індивідуально розробити свою систему обробки персональних даних, щоб належним чином адаптувати гарантії, процедури та документацію до регулювання ЄС. Певні вказівки щодо наукових досліджень можна знайти у статті 469b Закону «Про вищу освіту та науку», яка вказує, що контролер даних впроваджує відповідні технічні та організаційні гарантії для прав і свобод фізичних осіб. Зокрема, це включає псевдонімізацію або шифрування даних, надання дозволу на обробку даних мінімально необхідній кількості осіб, контроль доступу до приміщень, де зберігаються документи, що містять персональні дані, та розробку процедури для визначення способів захисту даних. Крім того, персональні дані анонімізуються

[81] *Там же*, с. 7.



відразу після досягнення мети наукових досліджень або дослідно-конструкторських робіт. До цього часу дані, за якими можна ідентифікувати особу, записуються окремо та об'єднуються з детальною інформацією лише у випадку, якщо цього вимагає мета дослідження.

*Аналіз конкретних рішень Голови Офісу із захисту персональних даних (PUODO)* дає практичні поради щодо очікуваних гарантій та сфер, у яких університети найчастіше припускаються помилок. Нижче наведено вибрані реальні випадки, які ілюструють типові проблеми у сфері вищої освіти.

*Рішення Голови Офісу із захисту персональних даних (PUODO) щодо Варшавської школи економіки (SGH) – справа No. ДКН.5131.26.2023 (від 30.11.2023)*[82]

*Рішення стосувалося ненавмисної публікації та несанкціонованого доступу до персональних даних близько 1000 осіб, опрацьованих в додатку набору для студентських обмінів. Витік тривав 27 днів. Причиною стала помилка програміста при перенесенні системи на новий сервер, що призвело до випадкового включення можливості несанкціонованої появи підсторінок панелі адміністратора і її включення на робочому сервері. URL з даними був проіндексований пошуковою системою, яка зробила дані загальнодоступними. З точки зору голови Офісу із захисту персональних даних, ключові причини витоку вказали на більш глибокі, системні проблеми. В університеті визнали, що аналіз ризиків для операцій з обробки даних, у яких стався витік, проводився лише після того, як стався інцидент, а до цього «формалізовано не проводився». Крім того, процедури тестування та впровадження були недостатніми. Тестування змін на сервері розробки виконував «сам програміст», а після розміщення їх в репозиторії «друга людина з команди (...) перевірила, чи коректно працює додаток», але без прив'язки до формальних процедур. Університет лише після порушення підготував процедури для виконання тестів, сценаріїв тестування та перевірки коду іншим програмістом перед тим, як передати їх у реалізацію. Цей інцидент підкреслив, що проблема полягала не в одній людській помилці, а в принципових недоліках в управлінні даними. Відсутність формалізованого аналізу ризиків перед інцидентом, недостатні процедури тестування, відсутність перегляду коду іншими розробниками свідчать про системні недоліки в управлінні IT-*

[82] https://uodo.gov.pl/pl/138/3483

*процесами та в безпеці даних. У своїх рішеннях Голова Офісу з питань захисту персональних даних часто аналізує не лише безпосередню причину порушення, а й ширший організаційний та процедурний контекст, який до нього призвів. Це означає, що від університетів очікують впровадження комплексних, задокументованих систем управління захистом даних, які регулярно перевіряються, а не лише реагування на інциденти, які виникають. Голова Управління із захисту персональних даних наклав на SGH штраф у розмірі 35 тисяч злотих. Воєводський адміністративний суд у Варшаві відхилив скаргу Варшавської школи економіки, підтвердивши, що до витоку даних призвела не лише людська помилка, а перш за все обробка даних, яка не відповідає GDPR. Голова Офісу захисту персональних даних встановив, що університет порушив статтю 5(1)(f) GDPR (принцип цілісності та конфіденційності) та статтю 32 GDPR (обов'язок впроваджувати відповідні заходи безпеки обробки). Суд наголосив, що стаття 32(1) GDPR вимагає впровадження адекватних заходів, а не будь-яких заходів.*

*Рішення Голови Офісу із захисту персональних даних (PUODO) щодо Варшавського університету природничих наук (SGGW) – Справа No. ZSOŚS.421.25.2019 (від 21 серпня 2020 року)*[83]

*У 2019 році було викрадено приватний ноутбук співробітника SGGW, у якому містилися персональні дані абітурієнтів (орієнтовно до 100 тисяч осіб). Працівник скопіював ці дані на мобільний пристрій, діючи всупереч процедурам, чинним в університеті. Голова Офісу із захисту персональних даних наклав фінансовий штраф у розмірі 50 тисяч злотих на SGGW. Університет подав апеляцію на це рішення, стверджуючи, що не несе відповідальності за дії працівника, який перевищів свої повноваження. Воєводський адміністративний суд та Вищий адміністративний суд (7 лютого 2025 року) відхилили скарги університету. Вищий адміністративний суд не погодився з позицією SGGW, визнавши університет контролером даних та заявивши, що він не виконав своїх зобов'язань у сфері перевірки поведінки працівників з точки зору дотримання принципів захисту персональних даних. У цьому рішенні чітко зазначено, що університет як контролер даних несе повну відповідальність за захист даних, навіть коли дії працівника порушують внутрішні процедури. Простого*

[83] https://uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019



*існування процедур недостатньо; Університет повинен активно перевіряти їх дотримання працівниками, що може вимагати впровадження додаткових технічних заходів контролю (наприклад, блокування копіювання даних на неавторизовані пристрої), а також регулярних тренінгів і аудитів. Адміністратор несе відповідальність за ефективність впроваджених організаційних заходів, а не тільки за їх формальне існування.*

*Рішення Голови Офісу захисту персональних даних щодо Університету Лазарського – справа DKN.5110.14.2022 від 2 квітня 2025 року*[84]

*Президент Офісу захисту персональних даних виніс попередження Університету Лазарського за затримку введення внутрішніх правил, що стосуються правил співпраці між адміністратором та інспектором із захисту даних (DPO). Спочатку університет не впровадив заходів для забезпечення того, щоб DPO був належним чином та оперативно залучений до всіх питань, пов'язаних із захистом персональних даних, мав достатні ресурси для підтримки рівня професійної експертизи, не отримував інструкцій щодо виконання своїх завдань, не потрапляв у конфлікт інтересів через інші завдання та обов'язки, а також щоб його чи її робота контролювалася (жодних положень про план роботи DPO чи план аудиту). Незважаючи на те, що порушення були усунені (університет вніс зміни до політики захисту даних та ухвалив додаткові нормативні акти), затримка з їх впровадженням призвела до винесення попередження. У цьому рішенні наголошується, що Голова Офісу захисту персональних даних надає великого значення належному статусу та функціонуванню інспектора із захисту даних, вважаючи його ключовим елементом системи захисту даних. Цей приклад яскраво показує, що Голова Офісу захисту персональних даних сприймає належне функціонування інспектора із захисту даних (його незалежність, доступ до ресурсів, включеність у процеси прийняття рішень, відсутність конфлікту інтересів та нагляд за його роботою) як основу дотримання GDPR. Запізніле або неадекватне виконання цих аспектів безпосередньо призводить до регуляторних дій. Це означає, що DPO – це не просто формальність, а ключовий елемент ефективної системи захисту даних. Заклади вищої освіти, які маргіналізують роль DPO або не надають належної підтримки, збільшують ризик недотримання вимог, оскільки роль DPO полягає в консультуванні та контролі за дотриманням правил захисту даних.*

Інші важливі рішення Голови Офісу захисту персональних даних щодо безпеки даних у державному секторі/університетах

Голова Офісу із захисту персональних даних регулярно накладає фінансові штрафи на контролерів (у тому числі з державного сектора) за неповідомлення про витік

[84] https://orzeczenia.uodo.gov.pl/document/urn:ndoc:gov:pl:uodo:2022:dkn_5110_14/content



даних наглядовому органу протягом 72 годин та за неповідомлення терміново суб'єктів даних про витік. Це повторювана проблема, яка вказує на недоліки в процедурах управління інцидентами. Рішення Голови Офісу захисту персональних даних (часто попередження, але також і штрафи) виносяться проти суб'єктів, які не надають Голові Офісу доступ до персональних даних та інформації, необхідної для виконання його завдань у провадженні. Це є порушенням основних обов'язків контролера у співпраці з наглядовим органом. Як приклад можна навести штраф, накладений на міського голову за відсутність належних організаційних заходів, які б унеможливили копіювання персональних даних працівником міської ради. Голова Офісу захисту персональних даних наголошує, що державні установи зобов'язані застосовувати вищі стандарти щодо безпеки оброблюваних даних. Цей випадок, хоч і не має прямого відношення до університетів, вказує на загальну тенденцію у вимогах щодо дотримання законодавства з боку Офісу із захисту персональних даних: до суб'єктів державного сектору, включаючи університети, ставлення більш суворе з точки зору безпеки даних. Це пов'язано з їхньою роллю в суспільстві та довірою суспільства, яку вони отримують. Це означає, що університети не можуть зупинятися на мінімальних вимогах GDPR, а повинні прагнути до зразкових практик у сфері захисту даних, оскільки будь-який збій може бути оцінений більш суворо, ніж у приватному секторі.

На підставі аналізу положень GDPR, Закону «Про вищу освіту і науку» та ключових рішень Голови Офісу із захисту персональних даних можна виділити низку запобіжників, які університети та інші наукові установи повинні впроваджувати або посилювати для забезпечення дотримання нормативно-правових актів про захист персональних даних.

1. Псевдонімізація та знеособлення:
    - Псевдонімізація: це важливий захід безпеки. Вона передбачає обробку персональних даних таким чином, що вони не можуть бути призначені конкретній особі без використання додаткової інформації (ключа), яка зберігається окремо та захищена. Псевдонімізовані дані все одно залишаються персональними даними, але ризик їх витоку набагато

нижчий. Часто це золота середина в дослідженнях, коли повна анонімізація унеможливила б аналіз.

- Анонімізація: означає незворотну трансформацію персональних даних таким чином, що унеможливлює ідентифікацію фізичної особи. Знеособлені дані перестають бути персональними даними і не підпадають під дію GDPR. Якщо мета дослідження це дозволяє, це найкраще рішення.

2. Контроль доступу:
   - Принцип мінімального дозволу: Доступ до персональних даних надається тільки тим особам, для яких абсолютно необхідно виконати завдання в рамках проекту.
   - Ролі та дозволи: визначте конкретні ролі з призначеними дозволами на доступ (наприклад, дослідник, статистик, менеджер даних).
   - Надійна автентифікація: вимога до надійних паролів, двофакторна автентифікація (2FA) скрізь, де це можливо.
   - Моніторинг доступу: систематично записуйте та переглядайте журнали доступу до даних.
3. Шифрування:
   - Шифрування даних у стані спокою: шифрування дисків (цілих, частин), папок, файлів, а також баз даних, де зберігаються дані досліджень.
   - Шифрування даних при передачі: Використання безпечних протоколів (SSL/TLS, HTTPS, VPN) для передачі даних, особливо за межами внутрішньої мережі установи.
4. IT-безпека:
   - Мережева безпека: брандмауер, системи виявлення та запобігання вторгнень (IDS/IPS).



   - Регулярні оновлення: операційні системи, програмне забезпечення, бази даних і дослідницькі програми для захисту від відомих вразливостей безпеки.
   - Антивіруси та антивірусні програми: постійний захист робочих станцій і серверів.
   - Резервне копіювання та відновлення: регулярно створюйте зашифровані резервні копії та тестуйте процедури відновлення даних.
5. Процедури та політики:
   - Політика захисту даних: внутрішня документація, яка встановлює правила обробки та захисту даних.
   - Правила чистоти робочого столу/екрана: обмежте видимість даних на екранах і в паперовій формі.
   - Процедури управління інцидентами: план боротьби з витоком даних (звітування, реагування, документування, інформування суб'єктів даних).
   - Угоди про обробку: коли дані обробляються зовнішніми сторонами (наприклад, статистичними компаніями, постачальниками програмного забезпечення), необхідні угоди про обробку даних, що відповідають GDPR.
6. Навчання та обізнаність:
   - Обов'язкове навчання: Регулярне навчання для всього дослідницького та допоміжного персоналу щодо принципів захисту та безпеки даних.
   - Підвищення обізнаності: Сприяння культурі безпеки даних у дослідницькій команді.
7. Фізична охорона:
   - Захист приміщень, де зберігаються дані (сервери, паперові архіви), від несанкціонованого доступу (наприклад, контроль доступу, моніторинг).

Ефективний захист персональних даних у наукових дослідженнях є безперервним процесом і потребує комплексного підходу, що поєднує надійний аналіз ризиків та DPIA з впровадженням адекватних технічних та організаційних заходів. Рішення Офісу із захисту персональних даних, хоча часто і загальні, чітко вказують на те, що основними причинами інцидентів є недостатній аналіз ризиків та відсутність елементарних заходів безпеки. Порушення також часто є наслідком людської помилки. Офіс із захисту персональних даних послідовно наголошує на важливості регулярного навчання для всіх осіб, які мають доступ до даних, включаючи науковий та технічний персонал.

## ВИСНОВКИ

У наш час захист персональних даних є одним з ключових питань проведення наукових досліджень. Це пов'язано зі зростанням важливості обробки цих даних в рамках сучасних наукових досліджень, а отже, і поглибленням взаємодії між питаннями використання персональних даних та провадження наукової діяльності. Дуже важливо забезпечити, щоб цілі досліджень реалізувалися таким чином, щоб одночасно захищати права та свободи осіб, яких торкнулися дані, та зміцнювати довіру громадськості до науки. Для цього потрібне чітке розуміння та застосування відповідної законодавчої бази. Виклики, пов'язані з GDPR у наукових дослідженнях, часто виходять за рамки простої відповідності до чинного законодавства. Неодноразово наголошується на адміністративному навантаженні та відсутності чітких орієнтирів. Таке повторення цих спостережень свідчить про системну проблему. Йдеться не лише про складність самого нормативно-правового акта, а й про труднощі його практичного тлумачення та реалізації, особливо в конкретному контексті наукового дослідження.

Для того, щоб спростити формальні зобов'язання, пов'язані з обробкою персональних даних, слід розробити стандартизовані інструменти та шаблони, які дослідники будуть використовувати, без необхідності постійно створювати документацію з нуля. Необхідно розробити модульні шаблони для форм згоди та інформаційних зобов'язань, які можна адаптувати до різних типів досліджень (наприклад, опитування, клінічні випробування, обсерваційні дослідження), шаблони договорів про доручення, контрольні списки, які дозволять провести початковий аналіз ризиків і визначити, чи буде потрібна оцінка впливу на захист даних (DPIA). Створення шаблонів дозволить дослідникам швидко створювати сумісні документи, адаптовані до їхніх конкретних потреб проєкту, зменшуючи кількість помилок і адміністративного часу, забезпечуючи при цьому узгодженість основного повідомлення GDPR у всій установі. Для того, щоб це стало можливим, необхідне і навчання персоналу, на якому так часто наголошує Голова Офісу з питань захисту персональних даних. Навчання має бути спрямоване на впровадження проактивної культури захисту даних, де дотримання вимог розглядається як невід'ємна частина етичного проведення досліджень, а не лише як регуляторна перешкода. Прихильність керівництва та підтримка спеціалістів із захисту персональних даних DPO є ключовими для формування цієї культури.

## БІБЛІОГРАФІЯ


**Монографії та дослідження**

- Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018
- Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022
- Jagielski M. (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2022 r.,
- Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Legalis 2021
- Litwiński P. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz,* Warszawa 2021
- Lubasz D. (red.), *Meritum. Ochrona danych osobowych*, Wolters Kluwer, Warszawa 2022 r.

- Woźnicki J. (red.), *Prawo o szkolnictwie wyższym i nauce. Komentarz*, Wolters Kluwer, Warszawa 2019.
- Woźnicki J. (red), *Identyfikacja i uzasadnienie kierunków regulacji o kluczowym znaczeniu w ustawie prawo o sokolnictwie wyższym i nauce*, Warszawa–Toruń 2020.

**Статті в журналах, неперіодичних виданнях**

- Jagielski M., *Ochrona danych osobowych jako element oceny etycznej badań naukowych z udziałem ludzi*, [w:] Diametros - An Online Journal of Philosophy, 2023, t.76.
- Pyka A., *Przetwarzanie danych osobowych do celów badań naukowych. Aspekty prawne*, [w:] Studnia Prawa Publicznego 2019 • NR 4 (28).

**Веб-джерела**

- https://www.rozwojspoleczny.gov.pl/strony/zasady-przetwarzania-danych-osobowych-w-programie-fundusze-europejskie-dla-rozwoju-spolecznego/ (дата звернення 29.06.2025)
- https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/przewodnik-po-danych-osobowych-w-projektach-po-wer-dla-wnioskodawcow-i-beneficjentow/ (дата звернення 29.06.2025)
- https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (дата звернення: 29.06.2025)
- https://uodo.gov.pl/pl/535/2506 (дата звернення 29.05.2025)
- https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_pl (дата звернення 29.05.2025)

**Рішення Голови Офісу з питань захисту персональних даних**

- ZSPR.421.3.2018 від 15 березня 2019 року ZSOŚS.421.25.2019 (від 21 серпня 2020 року)
- ДКН.5131.26.2023 від 30 листопада 2023

**Керівні принципи та висновки Європейської ради із захисту даних**

- Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19
- Wytyczne 7/2020 EROD w sprawie koncepcji administratora i podmiotu przetwarzającego w RODO, przyjęte 7.07.2021 r.,
- Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, przyjęte 18.06.2021 r.

**Керівні принципи та висновки Робочої групи за статтею 29**

- Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 z dnia 10 kwietnia 2018 r., WP259 rev.01, 17PL

**Законодавство**

- Karta Praw Podstawowych Unii Europejskiej, Dz.Urz.UE 2016 C 202
- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 nr 78 poz. 483
- Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1, ze sprost.) – GDPR/RODO
- Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce, Dz.U. 2018 poz. 1668