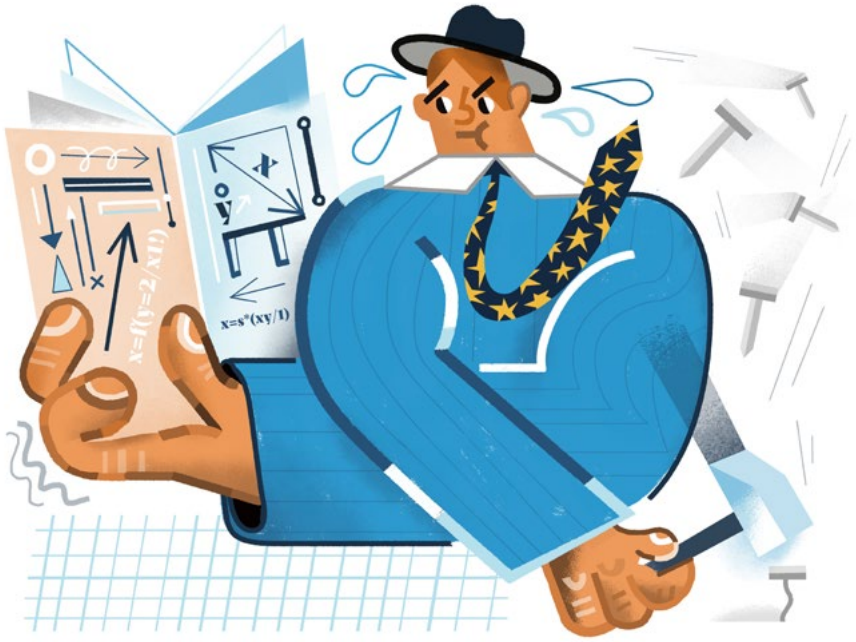
# Jak przetwarzać dane osobowe



RODO PORADNIK

Dla przedsiębiorców

## Patron poradnika

ODO 24 sp. z o.o. oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z dziedziny m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

## Autor poradnika

Leszek Kępa – ekspert bezpieczeństwa informacji, autor kilku książek i wielu publikacji na temat ochrony danych osobowych i bezpieczeństwa informacji. Posiada, uznane na całym świecie, certyfikaty CISA (Certified Information Security Auditor), CISM (Certified Information Security Manager) oraz CEH (Certified Ethical Hacker). Jest członkiem ISACA. Absolwent Szkoły Głównej Handlowej, Politechniki Częstochowskiej oraz Akademii Podlaskiej.

## Ilustracje

Karol Banach (karolbanach.com)

## Projekt i skład

Radosław Zbytniewski (zbytniewski.pl)

## Redakcja i korekta

Ewa Walewska

**ISBN: 978-83-943435-6-9**

**Wydanie I – Warszawa, maj 2019 r.**

# Wstęp

Dane osobowe są wszędzie, dlatego umiejętność ich przetwarzania stanowi w dużym stopniu o sukcesie firmy. Właściwie trudno sobie wyobrazić, aby firma, która się rozwija i dąży do osiągania wyników, nie przetwarzała danych osobowych.

Podczas przetwarzania danych osobowych należy stosować się do przepisów o ochronie danych osobowych. Może być to jednak sporym wyzwaniem dla przedsiębiorstwa, ponieważ nakładają one wiele ograniczeń i narzucają wiele obowiązków. Przepisy mają wpływ na prawie wszystkie procesy w firmie – to jeden z wielu powodów, dla których warto wiedzieć, jak praktycznie je stosować.

Wydawałoby się, że przepisy o ochronie danych osobowych są zawarte tylko w europejskim rozporządzeniu o ochronie danych osobowych oraz polskiej ustawie o ochronie danych osobowych. W praktyce okazuje się jednak, że zasady ochrony danych osobowych reguluje kilkaset rozmaitych aktów prawnych, m.in. Kodeks pracy, ustawa o świadczeniu usług drogą elektroniczną, a nawet przepisy Ordynacji podatkowej! Oprócz tego pod uwagę trzeba jeszcze brać umowy międzynarodowe [1]. Co więcej, przepisy te się zmieniają, a ostatnio nawet dość często. Naprawdę można się w tym wszystkim pogubić!

**Klienci preferują te firmy, które przetwarzają dane osobowe zgodnie z prawem.**

Przede wszystkim należy pamiętać, że zapewnienie zgodności z przepisami buduje wartość przedsiębiorstwa. Dane osobowe mają coraz wyższą wartość ekonomiczną. Dr Maciej Kawecki – koordynator krajowej reformy ochrony danych osobowych, kierujący Departamentem Zarządzania Danymi w Ministerstwie Cyfryzacji – podkreśla, że dane osobowe „stały się walutą XXI wieku. A jeżeli stały się tą walutą, to musimy traktować je jak walutę" [2]. Zaufanie jest jedną z najważniejszych wartości, jakie liczą się dla nas, gdy wybieramy bank, w którym chcemy ulokować swoje środki finansowe. Podobnie jest z danymi osobowymi – nie bez powodu klienci coraz częściej wybierają te organizacje, które dane o nich będą przetwarzać rzetelnie, uczciwie, bezpiecznie i zgodnie z prawem.

Warto zdać sobie sprawę z tego, że nieznajomość prawa utrudnia prowadzenie działalności gospodarczej. Przepisy ustalają m.in., jak odpowiednio sformułować treści zgód na przetwarzanie danych osobowych, a także jak wypełnić tzw. obowiązek informacyjny. Przykładowo art. 13 i 14 RODO określają obowiązki administratora danych wobec osoby, której dane dotyczą – należy do nich poinformowanie osoby o wejściu w posiadanie jej danych oraz o przysługujących jej w związku z tym prawach. Niedopełnienie tych obowiązków powoduje, że dane osobowe zebrane są nielegalnie, i może się okazać, że trzeba będzie je wszystkie usunąć (a przecież pozyskanie klientów i ich danych osobowych to największy koszt i wysiłek organizacji!). Co więcej, za takie postępowanie grozi kara, która może okazać się bardzo wysoka. *Ignorantia iuris nocet* – nieznajomość prawa szkodzi. Na nic zda się tłumaczenie, że nie znało się przepisów, każdy bowiem jest zobowiązany je znać.

**Przepisy zobowiązany jest znać i stosować każdy.**

Są jeszcze inne powody, dla których przepisy trzeba znać i stosować. Świadomość ochrony danych osobowych jest w Polsce wyjątkowo wysoka. Prawie każdy słyszał o RODO, a w związku z tym coraz więcej nieprawidłowości zgłasza się do Urzędu Ochrony Danych Osobowych (UODO). Efektem takich skarg są najczęściej kontrole, które w przypadku nieprawidłowości będą prowadzić do sankcji finansowych. Nakładane kary czy czasochłonne i kosztowne procesy sądowe zdecydowanie nie wpływają korzystnie na wizerunek organizacji.

W tym poradniku przedstawiłem podstawowe informacje o stosowaniu przepisów o ochronie danych: kiedy mamy do czynienia z danymi osobowymi, jak je zbierać, przetwarzać, zabezpieczać i kiedy usuwać, aby być w zgodzie z obowiązującym prawem. Jego celem jest pomóc czytelnikowi zrozumieć najważniejsze elementy tematyki ochrony danych osobowych. Tych z Państwa, których lektura niniejszego poradnika zachęci do dalszego zgłębiania tematu, odsyłam do książki „Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców", której jestem autorem.

**Leszek Kępa**

WIĘCEJ

[1] Przykładem umowy międzynarodowej, pozwalającej na zbieranie i przetwarzanie danych osobowych, jest umowa między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA – zob. http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20150001647 (dostęp: 17.04.2019 r.).
[2] M. Kawecki, Maciej Kawecki o RODO w NGO, rozm. przepr. R. Kowalski, 13.08.2018 r., https://publicystyka.ngo.pl/maciej-kawecki-o-rodo-w-ngo (dostęp: 17.04.2019 r.).

# Spis treści

# Akty prawne składające się na przepisy o ochronie danych osobowych

Na zestaw najważniejszych aktów prawnych dotyczących przetwarzania danych osobowych składają się:

- **rozporządzenie Parlamentu Europejskiego i Rady 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 Polsce akt ten w skrócie jest określany RODO, a w Europie – GDPR[3]. Rozporządzenie weszło w życie 25 maja 2016 r., a jego zapisy zaczęły obowiązywać od 2018 r.,**
- **ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,**
- **ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (przetwarzanie danych np. przez Policję czy Straż Leśną),**
- **ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (reguluje przetwarzanie danych w związku z zatrudnieniem, w tym monitoring pracowników),**
- **ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (publikowanie wizerunków osób),**
- **ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (reguluje m.in. przesyłanie informacji handlowych drogą elektroniczną),**
- **ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (reguluje m.in. marketing przez telefon).**

## OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH

Przepisy zarówno RODO, jak i ustawy o ochronie danych osobowych stanowią swojego rodzaju prawne ramy przetwarzania danych osobowych. Aby zrozumieć, jaki wpływ na obywateli mają zapisy RODO, warto zapoznać się z konstrukcją przepisów prawa Unii Europejskiej. Składają się na nie:

- **rozporządzenia,**
- **dyrektywy,**
- **decyzje,**
- **opinie,**
- **zalecenia.**

**Dyrektywy** europejskie mają moc wiążącą wyłącznie co do rezultatu, ich rolą jest harmonizacja prawa. Oznacza to, że państwa członkowskie mają obowiązek wdrożyć opisane w dyrektywie przepisy, ale mają przy tym swobodę sposobu ich implementacji. Przykładowo wymagania dyrektywy 95/46/WE weszły do polskiego porządku prawnego przez uchwalenie ustawy o ochronie danych osobowych w 1997 r.

**Rozporządzenia** europejskie z perspektywy prawa są podobne do polskich ustaw, mają charakter wiążący i – co najważniejsze – obowiązują bezpośrednio. Oznacza to, że do rozporządzenia unijnego w Polsce należy stosować się tak samo, jakby to była polska ustawa. Stosowanie przepisów przez kraje członkowskie UE reguluje art. 288 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), a nadrzędność przepisów unijnych Polska uznała 1 maja 2004 r. poprzez przystąpienie do UE.

**Do rozporządzenia unijnego trzeba stosować się tak samo, jakby to była polska ustawa.**

Niekiedy spotyka się jeszcze opinie. W zakresie ochrony danych osobowych opinie są przygotowywane przez Europejską Radę Ochrony Danych (dawniej Grupę Roboczą art. 29). Stanowią one jedynie – jak sama nazwa wskazuje – wytyczne, natomiast nie mają żadnej mocy wiążącej, chociaż organy nadzorcze biorą je pod uwagę.

Do niedawna kwestie przetwarzania danych osobowych w Europie regulowała dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Jak wiemy, państwa członkowskie muszą wprowadzić w życie przepisy opisane w danej dyrektywie, mają jednak przy tym swobodę wyboru metod i środków ich wdrożenia. Tłumacząc obrazowo: w przypadku dyrektywy 95/46/WE każdy miał wybudować most na rzece, ale jego ostateczny kształt i rodzaj użytych materiałów pozostawiono decyzji każdego z państw. Dyrektywa powstała w 1995 r., kiedy Internet zaledwie raczkował, a sposób prowadzenia biznesu znacząco różnił się od dzisiejszego. Przez ostatnie dwadzieścia lat gwałtowny rozwój technologii zmienił przetwarzanie danych tak bardzo, że przepisy wymagały gruntownych zmian.

Za bardzo pozytywną zmianę należy uznać to, że dyrektywę 95/46/WE zastąpiło unijne rozporządzenie, ponieważ ujednoliciło to przepisy dotyczące ochrony danych w krajach, które – wracając do wcześniejszej obrazowej metafory – w końcu mają identyczne mosty. W preambule RODO, w motywie 10, podkreślono:

**Aby zapewnić wysoki i spójny poziom ochrony osób fizycznych oraz usunąć przeszkody w przepływie**

WIĘCEJ

[3] RODO to skrótowiec oznaczający rozporządzenie o ochronie danych osobowych , a GDPR to unijny skrótowiec od General Data Protection Regulation.

**danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych.**

Zmiany przepisów są szczególnie korzystne dla wszystkich przedsiębiorców, którzy aktywnie działają na terenie całej Unii Europejskiej, tj. mają międzynarodowych partnerów, oddziały i sieć sprzedaży. Bez wątpienia bardzo korzystna dla nich jest także możliwość czerpania z dorobku innych krajów przez obserwowanie, jak dane zagadnienia są interpretowane w innych krajach unijnych.

**Największą zaletą RODO jest jeden zestaw przepisów dla obywateli i przedsiębiorstw w całej Unii Europejskiej.**

Trzeba pamiętać, że zasadnicze założenia się nie zmieniły – jeśli chodzi o ochronę danych osobowych, cele RODO są takie same jak cele dyrektywy 95/46/WE. W sprawozdaniu GIODO za 2017 r. wskazano:

**RODO nie powstało w próżni. Ponad 20 lat doświadczeń w stosowaniu dyrektywy 95/46/WE – zarówno przez administratorów danych, jak i podmioty danych, ale także niezależne organy nadzorcze, stało się podwalinami nowego prawa ochrony danych w Unii Europejskiej. Rozporządzenie opiera się na podstawowych wartościach tego istniejącego już systemu, utrzymując zasady ochrony danych oraz podstawy prawne przetwarzania danych, poddając je jedynie niezbędnym modyfikacjom [4].**

RODO to akt prawa napisany w miarę przystępnym językiem. Łacińska paremia *leges ab omnibus intellegi debant* stanowi o tym, że przepisy powinny być zrozumiałe przez wszystkich. Można uznać, że RODO spełnia ten warunek – przeciętny odbiorca powinien jasno zrozumieć, co z niego wynika, co można, co trzeba, a czego nie wolno. Może nie jest to idealny akt prawa, ale na pewno bardziej przystępny w odbiorze niż dawne polskie przepisy o ochronie danych.

Trzeba pamiętać, że RODO jest tłumaczone z języka angielskiego, dlatego jego przepisów nie można interpretować literalnie (do czego jesteśmy przyzwyczajeni, zresztą w końcu nie bez powodu mówi się o „literze prawa"). Zawsze, gdy pojawią się wątpliwości, należy analizować cel, jaki przyświecał zapisom, warto także zajrzeć do wersji angielskiej

Ochrona danych osobowych w modelu europejskim została pomyślana jako ochrona publicznoprawna, czyli taka, w której prawo publiczne (a nie prywatne, cywilne) gwarantuje nam wszystkim ochronę naszych danych osobowych. Fundamentem tego modelu jest organ władzy publicznej, który ma naszym danym zapewnić ochronę. W Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO).

**Przepisy chronią osoby fizyczne w związku z przetwarzaniem ich danych osobowych.**

RODO ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych (art. 1 ust. 1). Jego celem jest chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. W motywie 4 RODO wybitnie podkreśla się, że przepisy o ochronie danych należy poukładać w taki sposób, aby służyły przede wszystkim ludziom. Widać wyraźnie, że osoby są w centrum uwagi RODO, zatem to ich interes i prawa należy brać pod uwagę w pierwszej kolejności. Można nawet pokusić się o stwierdzenie, że w razie konfliktu przepisów z interesem osób należałoby preferować prawa osób.

Przepisy posługują się pojęciem osoby fizycznej. Osoba fizyczna to określenie człowieka w prawie cywilnym – od

[4] Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2017, https://giodo.gov.pl/data/filemanager_pl/sprawozdaniaroczne/2017.pdf (dostęp: 17.04.2019 r.), s. 27.

chwili narodzenia do śmierci. W konsekwencji przepisy chronią dane osobowe jedynie osób żyjących. Warto podkreślić, że nie ma znaczenia narodowość osób, których dane są przetwarzane [5].

Podmiotami RODO, czyli tymi, którzy są zobowiązani stosować się do opisanych w nim zasad, są w zasadzie wszyscy w Unii Europejskiej, którzy przetwarzają dane osobowe. Zgodnie z art. 2 ust. 2 RODO wyjątkiem jest przetwarzanie danych osobowych:

- **przez osoby fizyczne w celach osobistych i domowych,**
- **w ramach działalności nieobjętej zakresem prawa UE,**
- **przez właściwe organy w związku z zapobieganiem przestępczości, wykrywania i ścigania czynów zabronionych itd. (bo to regulują odrębne przepisy),**
- **gdy dane osobowe nie są przetwarzanie w zbiorze (przetwarzanie nie ma charakteru usystematyzowanego, jest incydentalne).**

Przepisy RODO dotyczą organizacji, które przetwarzają dane osobowe w związku z jej działalnością prowadzoną w Unii Europejskiej, niezależnie od tego, czy samo przetwarzanie danych odbywa się na jej terenie. Nie ma znaczenia ani lokalizacja, ani narodowość osób, których dane osobowe są przetwarzane. W takim świetle RODO musi stosować się także podmiot mający siedzibę w Polsce, a świadczący usługi on-line wyłącznie dla obywateli spoza UE. Stosować RODO muszą też podmioty niemające jednostek organizacyjnych w UE, jeśli oferują towary i usługi osobom w UE lub jeśli monitorują osoby z jej terenu.

Rozporządzenie chroni prawa osób. Jednym z praw podstawowych, fundamentalnych, jest prawo do ochrony danych osobowych, opisane w art. 8 Karty praw podstawowych Unii Europejskiej.

**Ochrona danych osobowych jest fundamentalnym prawem człowieka.**

Odniesienie do podstawowych praw i wolności osób fizycznych znajdujemy w art. 1 ust. 2 RODO: „Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych". Bez wiedzy, o jakie prawa i wolności chodzi, trudno prawidłowo zaprojektować system przetwarzania danych osobowych. Zgodnie z RODO w wielu sytuacjach konieczna będzie ocena wpływu przetwarzania na prawa i wolności osób fizycznych lub ocena ryzyka ich naruszenia. Tych praw i wolności nie zdefiniowano w RODO, należy zatem uznać, że chodzi o te, które wymieniono w Karcie praw podstawowych Unii Europejskiej, mianowicie:

- **godność, w tym: poszanowanie godności ludzkiej, prawo do życia oraz do integralności fizycznej i psychicznej, zakaz tortur i poniżającego traktowania lub karania, zakaz niewolnictwa i pracy przymusowej,**
- **wolność, w tym m.in. prawo do ochrony danych osobowych, prawo do wolności i bezpieczeństwa osobistego, do poszanowania prywatności i życia rodzinnego, prawo zawarcia małżeństwa i założenia rodziny, wolność myśli, sumienia i religii, wolność zgromadzania się i stowarzyszania się, prawo do nauki, wolność wyboru zawodu i prawo podejmowana pracy w każdym państwie członkowskim,**
- **równość, w tym m.in. równość wobec prawa, zakaz wszelkiej dyskryminacji, prawa dziecka, prawa osób starszych, prawa osób niepełnosprawnych,**
- **solidarność, w tym m.in. prawo pracowników do informacji i konsultacji, do rokowań i działań zbiorowych, dostępu do pośrednictwa pracy, prawo do ochrony przed nieuzasadnionym zwolnieniem z pracy, prawo do godziwych warunków pracy, zakaz pracy dzieci i ochrona młodocianych w pracy, prawna, ekonomiczna i społeczna ochrona rodziny, prawo do zabezpieczenia społecznego i pomocy społecznej, do ochrony zdrowia,**
- **prawa obywatelskie, w tym m.in. prawo głosowania i kandydowania w wyborach do Parlamentu Europejskiego i w wyborach lokalnych, prawo do dobrej administracji, swoboda przemieszczania się i pobytu, wymiaru sprawiedliwości, w tym m.in. prawo dostępu do bezstronnego sądu i do skutecznego środka odwoławczego[6].**

W ramach ochrony danych osobowych RODO w rozdziale III przyznaje osobom określone prawa. Są to:

- **prawo do informacji o przetwarzaniu na etapie zbierania danych (art. 13 i 14 RODO),**
- **prawo dostępu do danych (art. 15 RODO),**
- **prawo do sprostowania danych (art. 16 RODO),**
- **prawo do żądania usunięcia danych (art. 17 RODO), nazywane też prawem do zapomnienia,**
- **prawo do ograniczenia przetwarzania (art. 18 i 19 RODO),**

[5] W sprawozdaniu za 2009 r. GIODO podkreśla, że narodowość użytkowników projektowanego portalu nie ma żadnego znaczenia z uwagi na fakt, że ustawa przyznaje ochronę danym osobowym każdej osoby (art. 1 ustawy o ochronie danych osobowych). Zob. Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2009, https://giodo.gov.pl/data/filemanager_pl/1953.pdf, (dostęp: 17.04.2019 r.), s. 91.
[6] Zob. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A12012P%2FTXT (dostęp: 17.04.2019 r.).

- **prawo do przenoszenia danych (art. 20 RODO),**
- **prawo do sprzeciwu (art. 21 RODO),**
- **prawo niepodlegania automatycznym decyzjom (art. 22 RODO).**

Trzeba podkreślić, że RODO nie narzuca żadnych rozwiązań technicznych i organizacyjnych – organizacje mogą dobierać środki we własnym zakresie. Jest to bardzo korzystne, doświadczenie już nas bowiem nauczyło, że przepisy, które określają, jakie techniki należy stosować, szybko się starzeją i po pewnym czasie blokują drogę lepszym rozwiązaniom.

## USTAWA O OCHRONIE DANYCH OSOBOWYCH

Przyjęcie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych uchyliło „dawną" ustawę o ochronie danych osobowych i akty wykonawcze, dla których była ona podstawą prawną. Akt ten stanowi jedynie uzupełnienie RODO, gdyż służy jego stosowaniu. Ustawa określa:

- **podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych (dzięki niej dowiadujemy się też, jakiego rodzaju podmioty należy uznawać za publiczne w rozumieniu RODO),**
- **zasady postępowania w przypadku naruszenia przepisów o ochronie danych osobowych,**
- **zasady kontroli przestrzegania przepisów o ochronie danych osobowych,**
- **odpowiedzialność cywilną za naruszenie przepisów,**
- **odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów.**

Ustawa ogranicza wysokość kar nakładanych na organy i podmioty publiczne do 100 tys. zł, z wyjątkiem państwowych i samorządowych instytucji kultury, dla których maksymalna kara może wynieść jedynie 10 tys. zł (art. 102 ust. 1 i 2).

WIĘCEJ

## POZOSTAŁE PRZEPISY

Ustawa o zmianie niektórych ustaw w związku z RODO[7] wprowadziła zmiany w wielu przepisach, mające na celu dostosowanie polskich regulacji do wymagań rozporządzenia.

Wszystkie te zmiany są uwzględnione w tym poradniku, niektóre jednak warto szczególnie odnotować, gdyż mogą być bardzo istotne dla niektórych przetwarzających.

W ustawie o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy uchylono art. 50, co oznacza, że dane osób z Centralnej Ewidencji i Informacji o Działalności Gospodarczej podlegają teraz ochronie wynikającej z RODO.

Art. 70a ust 1 i 2, art. 105 Prawa bankowego oraz art. 10 ust. 2 ustawy o kredycie konsumenckim wprowadzają konieczność wyjaśnienia wnioskującemu o kredyt lub pożyczkę, jakie czynniki miały wpływ na dokonaną ocenę jego zdolności kredytowej, o ile tego wnioskujący zażąda.

W ustawie o działalności ubezpieczeniowej i reasekuracyjnej wykreślono wymaganie pisemnej zgody, uznając, że wyraźna zgoda w jakiejkolwiek postaci będzie wystarczająca (art. 38 ust. 6 i 8, art. 39). Ustawodawca uzasadania to tym, że „w określonych sytuacjach fakt udzielenia zgody na podstawie art. 9 ust. 2 lit. a RODO może mieć bardziej praktyczne zastosowanie niż fakt udzielenia pisemnej zgody, która w określonych sytuacjach losowych może być pozbawiona elementu wyraźnej świadomości osoby, która tej zgody udziela". To korzystna zmiana, szczególnie że RODO nie wprowadza nigdzie obowiązku pisemnej zgody.

W Prawie oświatowym dodano (chociaż reguluje już to RODO), że dane osobowe trzeba zachować w poufności, ale można je ujawnić w przypadku np. zagrożenia zdrowia ucznia (art. 30a ust. 3). Można to uznać za odpowiedź na zdarzenie z czerwca 2018 r., kiedy to rodzice dzieci poszkodowanych w wypadki nie mogli dowiedzieć się, w jakim szpitalu one się znajdują[8]. To stanowi też wyraźne podkreślenie, że prawa osób są najważniejsze – w końcu chodzi o ochronę osób w związku z przetwarzaniem ich danych (a nie o samą ochronę danych jako taką).



[7] Zob. http://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=3050 (dostęp: 17.04.2019 r.).
[8] Zob. https://gazetakrakowska.pl/wypadek-w-tenczynie-absurd-z-rodo-nie-mogli-znalezc-dziecka/ar/13249142 (dostęp: 17.04.2019 r.).

# Wpływ przepisów na działalność podmiotów

Dane osobowe są w zasadzie wszędzie i znakomita większość podmiotów je przetwarza. Już samo zebranie danych pracownika w celu zatrudnienia wymaga stosowania się do przepisów o ochronie danych osobowych. RODO narzuca wiele obowiązków i ograniczeń, dlatego zapewnienie zgodności z jego przepisami stanowi niemałe wyzwanie. Przykładowo nie wystarczy tylko to, że osoby, których dane dotyczą, wyrażą zgodę na przetwarzanie ich danych, bo aby być w zgodzie z prawem, musimy dokładnie uzasadnić cel tego przetwarzania, a dane muszą być do tego celu potrzebne. Ograniczenia dotyczą również danych osobowych zebranych z publicznie dostępnych źródeł, takich jak strony internetowe czy katalogi adresowe. Aby móc z nich skorzystać, po zebraniu danych należy poinformować osoby, których dane dotyczą, o pozyskaniu ich danych i przysługujących im w związku z tym prawach. Warto pamiętać, że osoby te mają prawo sprzeciwić się przetwarzaniu swoich danych.

Niezależnie od oceny poszczególnych przepisów wszystkie podmioty przetwarzające dane osobowe są zobligowane do ich przestrzegania. Warto więc wiedzieć, jak stosować się do przepisów o ochronie danych osobowych, a jednocześnie efektywnie prowadzić swoją działalność biznesową.

## PODSTAWOWE ZASADY PRZETWARZANIA

Zasady przetwarzania danych osobowych są wymienione w art. 5 ust. 1 RODO. W ich świetle należy odczytywać przepisy dotyczące zadań i obowiązków podmiotów przetwarzających dane. Naruszenie tych zasad jest zagrożone najwyższymi sankcjami, jakie przewiduje RODO (art. 83 ust. 5 lit. a). Interesującą nowością jest zasada przejrzystości, która w tej formie nie była wcześniej wyrażona w polskich przepisach.

**Zgodność z prawem, rzetelność i przejrzystość**
Dane osobowe muszą być „przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą" (art. 5 ust. 1 lit. a RODO). Rzetelność rozumiana jest jako uczciwe przetwarzanie. Gdy osoba, której dane dotyczą, zostanie należycie poinformowana o wszystkich istotnych dla niej aspektach tego przetwarzania (np. w jakim celu, jakie dane, jak długo itd.), będziemy mówić o przejrzystości, gdyż dla tej osoby wszystkie kwestie związane z przetwarzaniem będą jasne. Zgodność z prawem oznacza, że do przetwarzania danych istnieją podstawy prawne wynikające z RODO (art. 6).

**Ograniczenie celu przetwarzania**
Dane mają być zbierane w konkretnych, wyraźnych i uzasadnionych celach. Cel przetwarzania musi być jasno sprecyzowany, nie można zmieniać go bez uzasadnionej przyczyny (art. 5 ust. 1 lit. b RODO).

**Minimalizacja danych**
Dane osobowe mają być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane" (art. 5 ust. 1 lit. c RODO). Nie można zbierać danych, które nie są związane z celem przetwarzania czy które do tego przetwarzania nie są potrzebne. RODO posługuje się określeniem „niezbędne", ale należy je rozumieć jako „potrzebne". Przykładowo wiek kierowcy nie jest niezbędny do ubezpieczenia samochodu, ale bez wątpienia jest potrzebny do oceny ryzyka.

**Prawidłowość**
Dane osobowe muszą być „prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane" (art. 5 ust. 1 lit. d RODO). Prawidłowość danych zapewnia się najczęściej na etapie zbierania danych, np. porównując podane informacje z danymi z dokumentu tożsamości. W systemach on-line stosuje się tzw. słowniki danych, które pozwalają uniknąć pomyłek. Przykładowo gdy osoba poda kod pocztowy, system wyświetli jej do wyboru miejscowości lub ulice objęte tym kodem pocztowym. Z tą zasadą koresponduje prawo osoby do sprostowania tych danych, które są nieprawidłowe (art. 16 RODO). Nieaktualne lub nieprawidłowe dane mogą powodować trudności w realizowaniu podstawowych praw, np. mogą utrudnić uzyskanie pracy.

**Ograniczenie przechowywania**
Zasada ograniczenia przechowywania zabezpiecza przez przetwarzaniem danych o osobie w nieskończoność. Zgodnie z nią dane muszą być „przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane" (art. 5 ust. 1 lit. e RODO).

**Integralność i poufność danych**
RODO nakazuje, aby zapewnić „odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych" (art. 5 ust. 1 lit. f RODO). Zabezpieczenia muszą być dopasowane do poziomu ryzyka dla praw lub wolności osób, których dane dotyczą (art. 32 ust. 1 RODO). Zauważmy, że należy szacować ryzyko z perspektywy osób, których dane dotyczą – oceniając zabezpieczenia, należy kierować się oceną tego, jakie skutki dla osób może nieść za sobą naruszenie poufności lub integralności ich danych.

**Rozliczalność**
Administrator jest w całości odpowiedzialny za przestrzeganie wszystkich wymienionych zasad i musi być w stanie wykazać, że są stosowane (art. 5 ust. 2 RODO). Jest to oczywiste, ale wydaje się, że w RODO chciano podkreślić, że nie można przenieść tej odpowiedzialności na pracownika czy też na podwykonawcę lub zleceniobiorcę.

## ZADANIA W ZWIĄZKU Z RODO

Kiedy przetwarzamy dane osobowe, jesteśmy zobowiązani do stosowania całego spektrum wymagań zawartych w RODO. Są one następujące:

- **określenie, jakie rodzaje (kategorie) danych będą przetwarzane,**
- **ustalenie, jakie będzie źródło danych (od osób, których dane dotyczą, lub z innych źródeł),**
- **ustalenie celu przetwarzania,**
- **obliczenie, jak długo dane będą przechowywane, i przygotowanie procesu usuwania danych,**
- **ocena ryzyka dla praw i wolności,**
- **przygotowanie oceny skutków dla ochrony danych,**
- **prowadzenie rejestrów czynności przetwarzania i rejestru kategorii czynności przetwarzania,**
- **przygotowanie treści informacji dla osób, których dane będą zbierane (włączając w to zgody),**
- **wydawanie i odbieranie upoważnień do przetwarzania danych czy uprawnień dostępu do danych lub systemów,**
- **zapoznawanie pracowników z przepisami,**
- **zabezpieczenie danych,**
- **nadzór nad zgodnością z przepisami o ochronie danych osobowych,**
- **usuwanie danych osobowych,**
- **monitorowanie zmian w przepisach,**
- **zbieranie, aktualizowanie, prostowanie i usuwanie danych osobowych,**
- **spełnianie obowiązku informacyjnego „na żądanie" (prawo do informacji),**
- **przyjmowanie sprzeciwów i odwoływanie zgód,**
- **rozpatrywanie skarg na przetwarzanie danych,**
- **realizowanie praw osób,**
- **zawieranie umów powierzenia przetwarzania danych osobowych,**
- **sprawdzanie kontrahenta przed powierzeniem mu przetwarzania danych,**
- **poddawanie się kontroli zleceniodawcy,**
- **przenoszenie danych w ramach prawa do przeniesienia danych,**
- **informowanie Prezesa UODO o zgłoszeniu, aktualizacji, odwołaniu inspektora ochrony danych,**
- **publikowanie imienia, nazwiska oraz telefonu bądź adresu poczty elektronicznej inspektora ochrony danych na stronie internetowej,**
- **uprzednie konsultacje związane z oceną skutków dla ochrony danych,**
- **poddawanie się kontroli Prezesa UODO.**

WIĘCEJ

# Podmioty prywatne i publiczne

Przepisy o ochronie danych osobowych dotyczą zarówno podmiotów prywatnych, jak i podmiotów publicznych. Warto jednak zauważyć, że w praktycznym stosowaniu istnieje pewna subtelna różnica. Podmioty publiczne, w myśl zasady praworządności wyrażonej w art. 7 Konstytucji Rzeczypospolitej Polskiej, działają wyłącznie na podstawie i w granicach prawa. Oznacza to, że mogą one przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu określonych prawem zadań, obowiązków i upoważnień. Zasadę tę podkreśla wyraźnie art. 51 Konstytucji:

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.**

Wynika z tego, że podmioty publiczne nie powinny zbierać danych osobowych jedynie na podstawie zgody i że powinien istnieć przepis prawa, który zezwala im na zbieranie i przetwarzanie danych osobowych. Podmioty prywatne mogą natomiast zbierać w zasadzie dowolne dane, o ile będą mieć np. zgodę osób, których dane dotyczą, i dane będą odpowiednie do celu, w jakim mają być przetwarzane.

Z art. 9 ustawy o ochronie danych osobowych dowiadujemy się, jakie organizacje należy uważać za organy i podmioty publiczne. Są to:

- **jednostki sektora finansów publicznych,**
- **instytuty badawcze,**
- **Narodowy Bank Polski.**

Natomiast w art. 9 ustawy o finansach publicznych znajdujemy opis tego, jakie podmioty są zaliczane do jednostek sektora finansów publicznych. Ich lista jest następująca:

- **organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały,**
- **jednostki samorządu terytorialnego oraz ich związki,**
- **związki metropolitalne,**
- **jednostki budżetowe,**
- **samorządowe zakłady budżetowe,**
- **agencje wykonawcze,**
- **instytucje gospodarki budżetowej,**
- **państwowe fundusze celowe,**
- **Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego,**
- **Narodowy Fundusz Zdrowia,**
- **samodzielne publiczne zakłady opieki zdrowotnej,**
- **uczelnie publiczne,**
- **Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne,**
- **państwowe i samorządowe instytucje kultury,**
- **inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.**

# Urząd Ochrony Danych Osobowych

W Polsce organem nadzoru jest Prezes UODO (zwany też „Prezesem Urzędu"), który zgodnie z art. 52 RODO:

- **działa w sposób w pełni niezależny,**
- **nie zwraca się do nikogo o instrukcje i od nikogo ich nie przyjmuje,**
- **nie podejmuje zajęć (zarobkowych, niezarobkowych) sprzecznych ze swoimi obowiązkami,**
- **dysponuje zasobami, które pozwalają mu skutecznie wypełniać swoje zadania.**

W polskich przepisach (art. 34 ustawy o ochronie danych osobowych) doprecyzowano, że Prezes UODO:

- **jest obywatelem polskim,**
- **posiada wyższe wykształcenie,**
- **wyróżnia się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych,**
- **korzysta w pełni z praw publicznych,**
- **nie był skazany prawomocnym wyrokiem za umyślne przestępstwo,**
- **posiada nieposzlakowaną opinię.**

Zadania organu nadzorczego określa art. 57 RODO. Najważniejszym z nich jest monitorowanie i egzekwowanie przepisów RODO na terytorium organu. Natomiast art. 58 RODO szczegółowo opisuje jego uprawnienia, m.in:

- **nakazywanie dostarczania i uzyskiwanie wszelkich informacji potrzebnych organowi do realizacji swoich zadań,**
- **prowadzenie postępowań w formie audytów ochrony danych,**
- **zawiadamianie (administratora lub podmiotu przetwarzającego) o podejrzeniu naruszenia RODO,**
- **uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego,**
- **wydawanie ostrzeżeń,**
- **udzielanie upomnień,**
- **nakazywanie spełniania żądań osób, których dane dotyczą,**
- **nakazywanie dostosowania przetwarzania do wymagań RODO,**
- **wprowadzenie ograniczenia przetwarzania,**
- **nakazywanie usunięcia danych,**
- **stosowanie administracyjnej kary pieniężnej (na mocy art. 83 RODO) zależnie od okoliczności sprawy.**

Z UODO warto skontaktować się po to, aby uzyskać praktyczną pomoc w sprawach związanych ze stosowaniem przepisów. Informacje o sposobach kontaktu znajdują się na jego stronie internetowej pod adresem: www.uodo.gov.pl.

# Dane osobowe

W RODO przyjęto definicję danych osobowych w zasadzie niezmienioną w porównaniu do dawnej ustawy o ochronie danych osobowych. Obecnie – zgodnie z art. 4 pkt 1 RODO – brzmi ona następująco:

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

Definicje danych osobowych z dyrektywy 95/46/WE, wcześniejszej polskiej ustawy o ochronie danych osobowych (która stanowiła implementację dyrektywy) oraz z RODO – obecnie obowiązująca – są ze sobą zgodne. Oznacza to, że wszystkie informacje, które były danymi osobowymi w poprzednim stanie prawnym, pozostają nimi także i teraz.

**Dowolna informacja dotycząca osoby fizycznej może stanowić dane osobowe.**

Nie wszystkie informacje o osobie to dane osobowe. Dawniej w polskich przepisach było doprecyzowane, że „informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań" (art. 6 ust. 1 dawnej ustawy o ochronie danych osobowych). RODO podchodzi do tej kwestii bardzo podobnie w motywie 26 preambuły:

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

Zatem aby mówić o danych osobowych, spełnione muszą być jednocześnie następujące warunki:

- **musimy mieć do czynienia z informacjami,**
- **informacje te muszą dotyczyć osoby,**
- **osoba musi być fizyczna (ang. *natural person*), a nie prawna – oznacza to, że musi być człowiekiem oraz musi być żyjąca,**
- **osoba ta musi być już zidentyfikowana bądź możliwa do zidentyfikowania,**
- **zidentyfikowanie nie może wymagać nadmiernych środków.**

W odniesieniu do osób zmarłych w motywie 27 RODO podkreślono, że nie ma ono zastosowania do przetwarzania ich danych osobowych. W konsekwencji można wnioskować, że tego rodzaju informacje to także dane osobowe, tyle że nie przysługuje im ochrona wynikająca z RODO.

## KATEGORIE DANYCH OSOBOWYCH

W RODO wyróżnia się dwie kategorie danych osobowych – dane osobowe szczególnych kategorii (w tym m.in. dane biometryczne) oraz pozostałe dane osobowe, które można określić jako dane zwykłe. Najczęściej przetwarzane są dane zwykłe.

### Dane wrażliwe

RODO wyróżnia pewne rodzaje danych osobowych, którym należy się szczególna ochrona, „gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności" (motyw 51). Takie dane określa się mianem „danych szczególnych kategorii" (ang. *special categories of personal data*). W motywie 10 RODO nazywa się je także „danymi wrażliwymi", w praktyce mówi się jeszcze o „danych sensytywnych".

Wszystkie rodzaje szczególnych kategorii danych osobowych wymieniono w art. 9 RODO. Są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne (ale przetwarzanie w celu identyfikacji), dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej osoby. W katalogu tych danych w ogóle nie pojawiają się dane, które dotyczą skazań, orzeczeń o ukaraniu i mandatów karnych. Reguluje je odrębnie art. 10 RODO:

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

Dane wrażliwe same w sobie zazwyczaj nie są danymi osobowymi. Muszą występować w połączeniu z danymi pozwalającymi zidentyfikować osobę, aby można było uznać je za dane osobowe. Za dane wrażliwe należy uznawać też „zwykłe" informacje, które ze sobą zestawione mogą pozwolić na wywnioskowanie danych wrażliwych.

### Dane biometryczne

Definicja danych biometrycznych jest zawarta w art. 4 pkt 14 RODO. Wskazuje ona elementy, które powinny być spełnione łącznie, czyli:

- **są to dane o osobie,**
- **wynikają ze specjalnego przetwarzania technicznego, przy wykorzystaniu środków technicznych, pozwalających na zebranie takich danych i przetworzenie ich za pomocą algorytmu w matematyczną reprezentację takiej cechy,**
- **dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej,**
- **umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby (dane osobowe takie jak wizerunek twarzy lub dane daktyloskopijne).**

W świetle tej definicji zdjęcie, nawet twarzy, nie będzie stanowić danych biometrycznych, co znajduje zresztą potwierdzenie w motywie 51 RODO:

**Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi,**

**umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.**

**Dane spseudonimizowane**

W RODO pojawiają się także dane spseudonimizowane. Używa się jeszcze określenia „pseudonimowe", ale raczej nie jest to prawidłowe, mimo że termin pochodzi od wyrazu „pseudonim", oznaczającego „imię, nazwisko lub inną nazwę, których ktoś używa, aby ukryć swoje prawdziwe imię lub nazwisko"[9]. Przykładowo na uczelniach publikuje się oceny studentów, ale zamiast imienia i nazwiska podaje się jedynie numer albumu. Takie dane to wciąż dane osobowe, ale tylko dla tych osób, które wiedzą, kto się kryje za pseudonimem lub jak zamienić go na dane identyfikujące osobę.

Pseudonimizacja pomaga w ochronie danych, gdyż w razie utraty spseudonimizowanych informacji potencjalna szkoda będzie mniejsza. Ten, kto uzyska takie dane, nie będzie mógł ich wykorzystać, gdyż nie będzie wiedział, kogo dotyczą.

WIĘCEJ

## PRZETWARZANIE DANYCH OSOBOWYCH

Zawarta w RODO definicja pojęcia przetwarzania danych wskazuje na przykładowy zestaw operacji, które są uważane za przetwarzanie danych. Katalog ten nie jest w żaden sposób wyczerpujący, a jedynie wylicza czynności, które niewątpliwie należy uznać za przetwarzanie danych. Zgodnie z art. 4 pkt 2 RODO:

**„przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.**

W tłumaczeniu RODO na język polski zaginęło określenie „wszelkie" czy „dowolne" (ang. *any*) operacje, i nie pojawiło się w sprostowaniu do niego. Jednak bez wątpienia chodzi o jakiekolwiek operacje na danych, jakiekolwiek czynności dotyczące danych osobowych podczas całego cyklu ich życia – aż do momentu ich usunięcia.

Szczególną uwagę należy zwrócić na wyraz „operacje" oraz sformułowanie „na danych osobowych" – jeśli operacje nie są wykonywane bezpośrednio na danych osobowych, nie występuje przetwarzanie. Przykładowo kurier transportujący zamkniętą paczkę dokumentów nie będzie przetwarzał danych osobowych zawartych w tych dokumentach, ale firma prowadząca archiwum i sortująca dokumenty w formie papierowej – już tak.



## ADMINISTRATOR DANYCH OSOBOWYCH

RODO posługuje się terminem „administrator", jednak w praktyce używamy określenia „administrator danych osobowych" (ADO). W bardzo dużym skrócie można określić go jako właściciela zebranych danych, który decyduje o tym, co się z nimi dzieje – po co je zbiera, co z nimi robi, komu je przekazuje itp. Pojęcie administratora zdefiniowano w 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.**

Jest to jedno z najważniejszych dla organizacji pojęć, dlatego że to ona będzie administratorem danych.

## UDOSTĘPNIANIE DANYCH OSOBOWYCH

„Udostępnianie" w języku potocznym oznacza pożyczanie, umożliwianie korzystania z czegoś, np. można komuś udostępnić samochód albo książkę. Przez odbiorcę (ang. *recipient*) zgodnie z art. 4 pkt 9 RODO należy rozumieć:

**osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego**

[9] Hasło: pseudonim, Słownik języka polskiego PWN, https://sjp.pwn.pl/szukaj/pseudonim.html (dostęp: 17.04.2019 r.).

**postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.**

Różnica między odbiorcą danych a stroną trzecią jest bardzo istotna, chodzi bowiem o przesłanki legalności przetwarzania danych. Przykładowo pracownik administratora lub procesora może być odbiorcą danych, ale nie musi spełniać dodatkowych warunków prawnych, jeśli jest przez pracodawcę upoważniony do przetwarzania danych. Natomiast strona trzecia nie jest upoważniona czy umocowana. Wynika z tego, że odbiorca w rozumieniu RODO jest pojęciem całkowicie odmiennym od odbiorcy, który był zdefiniowany w dawnej ustawie o ochronie danych osobowych – tamten po uzyskaniu danych stawał się ich administratorem. W takim świetle odbiorcę należy rozumieć jako swojego rodzaju adresata danych, kogoś, komu dane się ujawnia, ale nie ma znaczenia, czy ten adresat jest uprawniony do przetwarzania, czy nie jest.

## PRZEKAZYWANIE DANYCH DO PAŃSTWA TRZECIEGO

Przekazywanie danych poza terytorium Polski należy podzielić na dwa rodzaje:

- **przekazywanie danych do państw Unii Europejskiej czy szerzej – na teren Europejskiego Obszaru Gospodarczego (EOG),**
- **przekazywanie danych do pozostałych państw (tzw. państw trzecich).**

Celem dyrektywy 95/46/WE było m.in. zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi. Ten cel jest wciąż ważny – RODO kontynuuje założenia dyrektywy. Znalazło to swoje odzwierciedlenie w art. 1 ust. 1 RODO, a także w samej nazwie tego aktu. Z tego powodu przekazywanie danych do państw z terenu Europejskiego Obszaru Gospodarczego w zasadzie nie różni się niczym od przekazywania danych na terytorium Polski.

**Przekazywanie danych w Unii Europejskiej nie różni się niczym od przekazywania danych na terytorium Polski.**

Sytuacja nieco się komplikuje w przypadku pozostałych państw. Przede wszystkim należy określić, co rozumie się przez przekazywanie danych poza kraj. Po pierwsze dane muszą znaleźć się pod władzą innego państwa – bezpośrednio lub pośrednio, tj. wtedy, gdy podmiot, który ma je przetwarzać, np. zagraniczny przedsiębiorca, będzie podlegał władzy innego państwa. Po drugie musi istnieć także zamiar przekazywania tych danych. Dane osobowe udostępnione na polskiej stronie internetowej, bez intencji przetwarzania ich poza krajem, pomimo możliwości dostępu do nich z całego świata nie będą przekazywane do innego państwa[10]. Podobnie jest w przypadku zabrania laptopa z danymi osobowymi w podróż zagraniczną – dane znajdą się co prawda na terytorium innego państwa, ale ani laptop, ani dane nie wejdą w jego władanie. Nie jest to więc przekazywanie danych poza kraj w rozumieniu przepisów RODO.

Aby móc przekazywać dane poza terytorium Europejskiego Obszaru Gospodarczego, należy spełnić określone warunki:

- **decyzja Komisji Europejskiej musi stwierdzać odpowiednią ochronę w państwie trzecim, zgodnie z art. 45 RODO,**
- **jeśli nie ma takiej decyzji, muszą zostać zastosowane odpowiednie zabezpieczenia danych, opisane w art. 46 i 47 RODO,**
- **jeśli nie ma decyzji i nie zastosowano zabezpieczeń z art. 46–47 RODO, należy spełnić warunek opisany w art. 49 RODO.**

Gwarancje ochrony mogą dotyczyć nie tylko państw, lecz także organizacji. Przykładowo program Tarcza Prywatności jest mechanizmem samocertyfikowania dla przedsiębiorstw mających swoją siedzibę w Stanach Zjednoczonych. Mechanizm ten został uznany decyzją Komisji Europejskiej, przyjętą 12 lipca 2016 r., za zapewniający odpowiedni poziom ochrony danych osobowych przekazywanych do tak certyfikowanych przedsiębiorstw z USA. Zanim nastąpi więc przekazywanie danych, należy upewnić się, że przedsiębiorca z siedzibą w USA posiada ważną certyfikację[11].

Jeśli gwarancje ochrony nie są „odpowiednie", ale administrator zapewnia właściwe zabezpieczenia, korzystając ze specjalnych wzorców umów lub klauzul (w RODO opisywane jako „standardowe klauzule umowne" oraz „wiążące reguły korporacyjne"), to dane także można przekazać do państwa trzeciego.

[10] Por. wyrok Europejskiego Trybunału Sprawiedliwości z 6 listopada 2003 r., sygn. C-101/01, Bodil Lindqvist v. Aklagarkammaren I Jönköping.
[11] Można to sprawdzić na stronie: www.privacyshield.gov/list (dostęp: 17.04.2019 r.).

# Kiedy dane są „osobowe”, a kiedy nie są

Na pytanie, czy określone dane są danymi osobowymi, bardzo często nie da się odpowiedzieć, jeśli nie weźmie się pod uwagę kontekstu, w którym występują. Informacja: „zarabia 6 tys. zł miesięcznie” albo „Prezes Zarządu” nic nie mówi o osobie, ale nabierze charakteru danych osobowych, gdy zostanie połączona z:

- **danymi dotyczącymi konkretnej, zidentyfikowanej osoby (np. dane o wynagrodzeniu połączone z informacją: „Jan Kowalski mieszkający na ul. Stawki 7 w Radomiu” staną się danymi osobowymi – wynagrodzenie jest informacją o tej osobie),**
- **danymi, które umożliwią przy niewielkim nakładzie pracy zidentyfikowanie osoby (np. „Prezes Zarządu ODO 24 sp. z o.o.”),**
- **kontekstem, który pozwoli łatwo ustalić tożsamość (informacja: „właściciel czarnego porsche” połączona z: „mieszka we wsi Całowanie” pozwoli ustalić tożsamość osoby, gdyż wieś Całowanie jest jedna, a zamieszkuje ją niewiele ponad 600 osób – obie informacje w takim kontekście staną się danymi osobowymi).**

**Jeżeli dane nie pozwalają jednoznacznie zidentyfikować osoby, to takie dane nie są osobowe.**

W zasadzie każdy zestaw informacji o osobie może stanowić dane osobowe. Wszystko zależy od tego, czy ten, kto jest w ich posiadaniu, będzie mógł ustalić tożsamość osoby, której dane dotyczą, i od tego, jak szybko albo przy jakim nakładzie pracy będzie w stanie to zrobić.

## IMIĘ I NAZWISKO ORAZ ADRES

Imiona powstały na skutek potrzeby identyfikowania osób w niewielkich społecznościach. Tam, gdzie te społeczności były większe, wykształciły się przydomki, a nawet nazwiska. Współcześnie imię i nazwisko jest podstawą identyfikowania osoby w społeczeństwie. Tak jak wizerunek w bezpośrednim kontakcie identyfikuje osobę, imię i nazwisko pomagają identyfikować ją we wszelkiego rodzaju dokumentach, wykazach, spisach, ewidencjach. W działalności gospodarczej trudno sobie wyobrazić identyfikowanie osoby bez tak zasadniczych danych jak imię i nazwisko.

Pięć najczęściej spotykanych w Polsce nazwisk nosi ok. 700 tysięcy osób. Samo imię i nazwisko nie stanowią danych osobowych, dopóki nie zostaną one powiązane z informacją dodatkową, pozwalającą na identyfikację osoby. Czasami wystarczy nazwa miejscowości (np. „Stefan Żeromski ze Strawczyna") albo inna informacja uzupełniająca („Andrzej Duda – Prezydent"). Samo imię i pierwsza litera nazwiska (np. „Janusz Z.") nie stanowią danych osobowych, chociaż już informacja „Mariusz O. z Woli Gułowskiej" może identyfikować osobę.

Sam adres także nie identyfikuje konkretnej osoby, a jedynie określone miejsce. Pod jednym adresem może bowiem przebywać czy mieszkać wiele osób. Jednak w połączeniu z dodatkową informacją adres mógłby już zidentyfikować konkretną osobę. Taką dodatkową informacją jest z pewnością imię i nazwisko. W takim połączeniu dane te stają się danymi osobowymi – znajdziemy je np. w dowodzie osobistym, prawie jazdy, dowodzie rejestracyjnym itp.

W niektórych sklepach sprzedawcy proszą klientów dokonujących zakupów o podanie kodu pocztowego. Pozwala im to na określenie miejscowości albo regionu, a w dużych miastach – nawet nazwy ulicy, przy której mieszka klient. Dzięki powiązaniu kodów pocztowych ze sprzedażą można określić, w jakich regionach kraju, jakie towary sprzedają się najlepiej. Sam kod pocztowy nie stanowi danych osobowych[12].

## NUMER IP

Numer IP identyfikuje urządzenia w sieci Internet. Organ nadzorczy na swojej stronie internetowej w sekcji poświęconej odpowiedziom na najczęściej zadawane pytania podkreśla, że adres IP może być w pewnych przypadkach uznany za dane osobowe[13]. Jest to oczywiście w zgodzie z generalną zasadą, że za dane osobowe może zostać uznana dowolna informacja dotycząca osoby fizycznej.

Sam numer IP stanowi dane osobowe głównie dla operatorów telekomunikacyjnych, którzy są w stanie powiązać ten numer z danymi konkretnego użytkownika sieci. Numer IP powiązany z innymi danymi osobowymi stanie się automatycznie danymi osobowymi.

## NUMER PESEL

Numer PESEL nadaje się głównie obywatelom polskim, chociaż mogą go otrzymać także cudzoziemcy, zameldowani w Polsce na dłuższy pobyt. Jest on swojego rodzaju identyfikatorem osoby. Zakłada się, że nie ma dwóch takich samych numerów PESEL, więc jest to identyfikator unikalny, co w ustawie o ewidencji ludności zostało podkreślone słowem „jednoznacznie"– art. 15 ust. 2:

**Numer PESEL jest to jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną, przy czym:**

[12] Warto odnotować, że ta zasada nie musi obowiązywać we wszystkich krajach. Przykładowo w Wielkiej Brytanii kod pocztowy jednoznacznie może identyfikować określony adres. Bywa nawet, że Brytyjczycy zamiast adresu podają sam kod pocztowy.
[13] Zob. https://www.giodo.gov.pl/pl/319/2258 (dostęp: 17.04.2019 r.).

**1) data urodzenia zawarta jest w pierwszych sześciu cyfrach w następującej kolejności: dwie ostatnie cyfry roku urodzenia, miesiąc urodzenia wraz z zakodowanym stuleciem urodzenia oraz dzień urodzenia;**

**2) stulecie urodzenia kodowane jest poprzez dodanie do liczby oznaczającej miesiąc urodzenia:**

**a) liczby 80 – w przypadku osób urodzonych w latach 1800–1899,**

**b) liczby 0 – w przypadku osób urodzonych w latach 1900–1999,**

**c) liczby 20 – w przypadku osób urodzonych w latach 2000–2099;**

**3) liczby oznaczające rok, miesiąc lub dzień, będące liczbami jednocyfrowymi, poprzedza się cyfrą „0", z zastrzeżeniem zasady określonej w pkt 2;**

**4) numer porządkowy osoby zawarty jest w cyfrach od siódmej do dziesiątej, przy czym ostatnia cyfra numeru porządkowego zawiera oznaczenie płci: cyfrę parzystą (w tym „0") dla kobiet, a cyfrę nieparzystą dla mężczyzn;**

**5) jedenasta cyfra numeru PESEL jest liczbą kontrolną umożliwiającą elektroniczną kontrolę poprawności nadanego numeru identyfikacyjnego.**

W społeczeństwie zwykło się przykładać dużą uwagę do zachowywania numeru PESEL w tajemnicy, podczas gdy w gruncie rzeczy jest on niczym innym jak tylko identyfikatorem. Upraszczając, można powiedzieć, że poszczególni mieszkańcy naszego kraju są ponumerowani, a PESEL jest po prostu numerem danej osoby. Numer PESEL stanowi dane osobowe – takie jest stanowisko organu nadzorczego, który zauważa, że „sam numer PESEL stanowi dane osobowe w rozumieniu ustawy o ochronie danych osobowych"[14].

## NUMER TELEFONU

Jeszcze nie tak dawno jeden telefon służył całej rodzinie. Telefonia komórkowa szybko zmieniła ten stan rzeczy, dzisiaj numer telefonu jest związany raczej z konkretną osobą, a nie z miejscem. Mimo że sam numer telefonu (jako ciąg cyfr) nie stanowi danych osobowych, to jednak jest wyjątkową informacją, umożliwiającą bezpośredni kontakt z konkretną osobą. RODO, skupiając się na ochronie danych, silnie podkreśla konieczność lub możliwość ustalenia tożsamości osoby. Dane kontaktowe nieco wymykają się takiemu ujęciu, gdyż sama możliwość skontaktowania się z daną osobą nie musi (chociaż oczywiście może!) prowadzić do ustalenia jej tożsamości. Chociaż numer telefonu nie jest samodzielnie danymi osobowymi, stanowi jednak informację, która umożliwia naruszenie podstawowych praw lub wolności.

Jeżeli korzysta się z numerów telefonów w celu kontaktu z osobami, należy pamiętać o art. 172 ust. 1 Prawa telekomunikacyjnego, z którego wynika, że dzwonienie jest możliwe tylko wtedy, gdy uzyska się na to zgodę. Wykonywanie połączeń pod wygenerowane czy losowe numery telefonów jest zabronione, gdyż nie ma na to uprzedniej zgody użytkownika:

**Zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę.**

Dla operatora świadczącego usługi telekomunikacyjne sam numer telefonu będzie danymi osobowymi. Ma on bowiem w swojej bazie klientów dane pozwalające powiązać numer z danymi osoby i w ten sposób ją zidentyfikować.

Numer telefonu w połączeniu z imieniem albo nazwiskiem należy uznawać za dane osobowe. Jeśli jest on zestawiony z innymi informacjami o osobie, mimo że nie zawsze będą to dane osobowe, również należy traktować go bardzo ostrożnie (podobnie np. wysokość wynagrodzenia).

Informacji, które samodzielnie nie będą danymi osobowymi w rozumieniu przepisów, bo nie pozwalają na ustalenie tożsamości, ale umożliwiają kontakt z konkretną osobą, jest więcej. Będą to np. numery Gadu-Gadu, identyfikatory Skype oraz prywatne adresy poczty elektronicznej.

## ADRES E-MAIL

Adres poczty elektronicznej pozwala na kontakt z konkretną osobą – podobnie jak numer telefonu. Różni się jednak nieco większą zawartością informacji, może bowiem ujawniać np. miejsce zatrudnienia, przynależność do określonej organizacji lub pewne cechy danej osoby. Firmowe adresy poczty elektronicznej zawierają w sobie najczęściej imię i nazwisko oraz nazwę firmy. Możliwość kontaktu połączona z identyfikacją osoby z imienia i nazwiska oraz miejscem jej pracy pozwala na ustalenie tożsamości użytkownika danego adresu. To powoduje, że firmowy adres e-mail uznawany jest za dane osobowe. Nie ma przy tym znaczenia, czy taki adres jest powszechnie dostępny, czy też nie.

Prywatnych, najczęściej darmowych, adresów poczty elektronicznej nie zwykło się uważać za dane osobowe – nawet jeżeli zawierają imię i nazwisko. Każdy może założyć konto pocztowe o dowolnej nazwie, oczywiście o ile nie jest ona już zajęta. To sprawia, że prywatny adres

[14] http://www.giodo.gov.pl/317/id_art/973/j/pl/ (dostęp: 17.04.2019 r.).

e-mail nie identyfikuje jednoznacznie konkretnej osoby. Należy jednak pamiętać, że e-mail wciąż pozwala na kontakt z jego właścicielem, a więc nieuprawnione wykorzystanie adresu poczty elektronicznej może spowodować naruszenie sfery prywatności danej osoby.

Warto wiedzieć, że gdy pracownik odchodzi z pracy, należy usunąć, a przynajmniej zablokować jego adres poczty elektronicznej. Podkreślił to GIODO w sprawozdaniu za 2011 r.:

**Przetwarzanie imienia i nazwiska w ramach służbowego adresu e-mail osoby, która już nie pracuje jest niezgodne z celem, dla którego dane te były zbierane. (…) ciągła aktywność przedmiotowego adresu poczty elektronicznej, a zarazem możliwość przesyłania wiadomości na ten adres, pośrednio jednak nadal wpływało na utożsamianie osoby (…) ze spółką, co w obecnej sytuacji dawało fałszywy obraz jej aktywności zawodowej. Ponadto osoba, do której, zgodnie z jej identyfikatorem zawartym w adresie, kierowana była korespondencja, nie miała możliwości zapoznania się z nią, co z kolei stanowiło przejaw naruszenia wolności tej osoby do prawa komunikowania się oraz ochrony jej korespondencji[15].**

### NUMER RACHUNKU BANKOWEGO

Numer rachunku bankowego (NRB) składa się z 26 cyfr. W numerze rachunku, w cyfrach od 3 do 10, zaszyta jest informacja o banku. Jest to tzw. numer rozliczeniowy jednostki organizacyjnej banku. Sam numer rachunku w zasadzie nie prowadzi do identyfikacji konkretnej osoby, dla przeciętnej osoby nie stanowi więc danych osobowych, podobnie jak kwoty i daty przelewów. Jednak dla banków, a w szczególności macierzystego banku posiadacza rachunku, taka identyfikacja jest możliwa poprzez wprowadzenie numeru rachunku do systemu komputerowego.

Podobnie zatem jak w innych przypadkach numer rachunku bankowego staje się danymi osobowymi dopiero wówczas, gdy zostanie połączony z innymi danymi osobowymi, identyfikującymi osobę. W podobny sposób można traktować także numer dowodu osobistego, legitymacji czy nawet numer rejestracyjny samochodu.



## Projektowanie systemu przetwarzania danych

Gdy chce się zbudować dom, trzeba zamówić jego projekt wykonany przez specjalistę, następnie trzeba urządzić wnętrze, zapewnić bieżącą wodę, elektryczność i instalacje. Nie inaczej jest z przetwarzaniem danych osobowych – zanim zacznie się je zbierać, należy się do tego przygotować.

RODO wprowadziło nowe rozwiązanie, którym jest obowiązek projektowania każdego nowego procesu (systemu przetwarzania) danych osobowych. Nakazuje ono wkomponować bezpieczeństwo i prywatność w proces przetwarzania już na etapie projektowania przetwarzania danych osobowych. Jest to bardzo praktyczne podejście, bo łatwiej (i taniej!) dobrze zaprojektować dom niż wprowadzać rozmaite poprawki do złej konstrukcji.

Niektóre wymagania trzeba spełnić jeszcze przed rozpoczęciem zbierania danych. Przykładowo należy zastanowić się, jak długo dane osobowe będą przechowywanie, gdyż o tym trzeba informować na etapie ich zbierania (zgodnie z art. 13 i 14 RODO). Nieprzekazanie takiej informacji lub podanie fałszywych terminów skutkuje tym, że osoba podaje swoje dane w nie do końca dla niej jasnych okolicznościach. Może to powodować, że tak zebrane dane zostaną uznane za zebrane nielegalnie, i może się okazać, że trzeba będzie je usunąć…

Do etapów projektowania nowego procesu przetwarzania należy zaliczyć:

- **ustalenie sposobu udokumentowania projektu nowego procesu (aby zapewnić rozliczalność),**
- **określenie celu przetwarzania i opisanie cyklu życia danych osobowych,**
- **identyfikacja podstaw prawnych przetwarzania,**

[15] Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2011, https://giodo.gov.pl/data/filemanager_pl/sprawozdania-roczne/2011.pdf (dostęp: 17.04.2019 r.), s. 75–76.

- **obliczenie okresów przechowywania danych,**
- **wskazanie potencjalnych partnerów w przetwarzaniu (podmiotów przetwarzających),**
- **określenie odbiorców danych,**
- **ustalenie transferów do państw trzecich,**
- **ocenienie ryzyka dla praw i wolności osób,**
- **wskazanie środków zmniejszających ryzyko lub po prostu zabezpieczeń danych (pseudonimizacja, szyfrowanie, minimalizacja, *data protection by design and by default*, anonimizacja),**
- **ustalenie sposobów realizacji wybranych praw (prawo do przenoszenia danych),**
- **zatwierdzenie nowego procesu.**

Na samym wstępie projektowania procesów przetwarzania danych niezbędnie jest określenie, czy przetwarzanie będzie miało „wrażliwy" charakter, czy też nie. Procesy przetwarzania danych osobowych można podzielić na dwie kategorie:

- **przetwarzanie „normalne" – gdy prawa osób fizycznych w związku z przetwarzaniem nie są zagrożone lub są, ale w niewielkim stopniu (ryzyko niskie),**
- **przetwarzanie „wrażliwe" – gdy jest wysokie ryzyko dla praw i wolności.**

## OCENA SKUTKÓW DLA OCHRONY DANYCH

W przypadku przetwarzania wrażliwego konieczne będzie wykonanie oceny skutków dla ochrony danych (art. 35 ust. 3 RODO). Dotyczy to następujących przypadków:

- **zautomatyzowane podejmowanie decyzji lub profilowanie na podstawie oceny czynników osobowych,**
- **przetwarzanie na dużą skalę danych wrażliwych,**
- **systematyczne monitorowanie na dużą skalę miejsc publicznych,**
- **wykonywanie operacji przetwarzania znajdujących się w wykazie operacji wymagających przeprowadzenia takiej oceny, przygotowanym przez organ nadzorczy (art. 35 ust. 4 RODO).**

Ocena skutków dla ochrony danych jest nowym instrumentem prawnym wprowadzonym przez RODO. Jest też uzupełnieniem procesu zarządzania ryzykiem dla praw i wolności osób, których dane mają być przetwarzane. W dokumencie Grupy Roboczej art. 29 czytamy:

**Ocena skutków dla ochrony danych jest procesem pozwalającym opisać przetwarzanie oraz ocenić jego konieczność i proporcjonalność, a także mającym wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych poprzez ocenę ryzyka i określenie środków pozwalającym zaradzić tym czynnikom ryzyka[16].**

– co wybitnie podkreśla specjalną rolę oceny skutków. Moim zdaniem należałoby pójść dalej – ocenę skutków dla ochrony danych powinno wykonywać się (i regularnie powtarzać) dla wszystkich operacji przetwarzania danych osobowych, gdyż jak twierdzi Grupa Robocza art. 29:

**Oceny skutków dla ochrony danych są ważnym narzędziem rozliczalności, ponieważ ułatwiają administratorom nie tylko przestrzeganie wymogów określonych w RODO, ale także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO (…) Innymi słowy ocena skutków dla ochrony danych jest procesem budowania i wykazywania zgodności[17].**

Przy podejściu, że ocena skutków dla ochrony danych jest wykonywana dla każdego procesu przetwarzania danych, te oceny byłyby głównym narzędziem do wykazywania zgodności i stanowiłyby serce systemu przetwarzania danych osobowych.

W normie ISO 29134, stanowiącej wytyczne do oceny skutków, czytamy, że ocena ta często jest uznawana za „system wczesnego ostrzegania", gdyż pozwala wykryć potencjalne ryzyka dla prywatności i inwestować w środki im przeciwdziałające przed ich wystąpieniem, a nie później, kiedy koszty są znacznie wyższe. Ocena skutków pozwala budować zaufanie klientów i pracowników do organizacji.

WIĘCEJ

**Sercem całego systemu ochrony danych osobowych jest zarządzanie ryzykiem dla praw i wolności osób.**

## OCENA RYZYKA

Zarządzanie ryzykiem jest częścią naszego życia, chociaż zapewne mało kto zdaje sobie z tego sprawę. Nawet zwierzęta oceniają ryzyko! Zanim lew podejmie walkę z innym samcem, analizuje przede wszystkim korzyści, jakie odniesie z potencjalnej wygranej, a następnie ocenia, jakie ma szanse na wygraną – czy jego przeciwnik jest silny, młody, czy też już stary i nieco zmęczony. Oce-

[16] Grupa Robocza art. 29, Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679, WP 248 rev.01, przyjęte 4.4.2017 r., ostatnio zmienione i przyjęte 4.10.2017 r., s. 4.
[17] Ibidem.

ny ryzyka nie należy się bać, bo ciągle je oceniamy, nawet o tym nie wiedząc.

Unijne rozporządzenie ocenę ryzyka stawia w samym centrum – cały system ochrony danych osobowych zgodny z RODO opiera się na ocenie ryzyka.

**Wyraz „ryzyko" pojawia się w treści RODO prawie osiemdziesiąt razy.**

Na etapy zarządzania ryzykiem składają się:

- **identyfikacja ryzyka (określenie, co złego może się stać i spowodować stratę, jak, gdzie i dlaczego strata może się zdarzyć),**
- **analiza ryzyka (określenie, jaka jest szansa na złe zjawisko i jakie będą jego konsekwencje, wyliczenie poziomu ryzyka),**
- **ocena ryzyka (określenie, czy ryzyko nie jest zbyt duże, porównanie ryzyka do poziomu, który jest akceptowalny),**
- **ustanowienie priorytetów postępowania (należy zacząć od rzeczy właściwych, tj. od największego ryzyka),**
- **sterowanie ryzykiem (ustalenie, co robić z ryzykiem),**
- **kontrola, monitorowanie i ocena podjętych działań (kontrolowanie, czy trzymamy się planu).**

Pierwsze trzy etapy – identyfikację, analizę i ocenę ryzyka – określa się jako szacowanie ryzyka.

Jeśli ryzyko dla praw i wolności wydaje się wysokie, należy wykonać ocenę skutków dla ochrony danych. Jeśli wynika z niej, że uda się zmniejszyć ryzyko dla praw i wolności, to dane będzie można zacząć przetwarzać, a jeśli nie – należy skontaktować się z organem nadzorczym w celu uzyskania porady. Proces ten określa się mianem „uprzednich konsultacji".

Administrator powinien planować przetwarzanie danych z dość dużym wyprzedzeniem, co najmniej trzymiesięcznym, ponieważ może się okazać, że konsultacje będą trwać 14 tygodni, a dodatkowo mogą zostać przedłużone o czas żądania i uzyskiwania informacji przez organ nadzorczy.

Ocena ryzyka musi być dokonywana regularnie, gdyż jego zmiana może powodować konieczność aktualizacji oceny skutków dla ochrony danych. Zgodne z art. 35 ust. 11 RODO:

**W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.**

WIĘCEJ

## OCHRONA DANYCH NA ETAPIE PROJEKTOWANIA

W RODO nie pojawia się ani razu termin „prywatność" (ang. *privacy*) – jest wyłącznie mowa o ochronie danych osobowych. *Privacy* jest znacznie szerszym pojęciem niż *data protection*. To istotna różnica, której – jak się wydaje – wiele osób nie zauważa, naprzemiennie używając określenia „ochrona prywatności" i „ochrona danych osobowych".

Koncepcja uwzględniania ochrony na etapie projektowania (mylnie określana *privacy by design*) nakazuje zaplanować operacje przetwarzania oraz środki ochrony, jeszcze zanim zacznie się przetwarzać dane osobowe. Planowanie nowego procesu przetwarzania danych porównuję do budowy domu – zawsze trzeba zaczynać od planu. Przepis art. 25 ust. 2 RODO odnosi się do „domyślnej" (ang. *default*) konfiguracji przetwarzania, określanej jako domyślna ochrona. Ustawienia prywatności w urządzeniach, produktach lub usługach mają być nakierowane na maksymalną ochronę użytkownika. Do niego ma należeć decyzja, czy i jakie dane chce udostępnić. Doskonałym przykładem mogą być samochodowe kamerki – domyślnie (tj. po wyjęciu z opakowania i uruchomieniu) powinny nagrywać tylko obraz, bez dźwięku. Nagrywanie dźwięku powinno zostać pozostawione decyzji użytkownika.

WIĘCEJ

## MINIMALIZACJA DANYCH

Co za dużo, to niezdrowo – tak można by powiedzieć o koncepcji minimalizacji danych. Przez minimalizację danych należy rozumieć nie tylko ograniczenie zbierania danych do tego, co potrzebne do osiągnięcia celu przetwarzania, lecz także ograniczenie ilości i rodzaju danych w stosunku do określonych operacji przetwarzania. Przykładowo w bankowości elektronicznej pełna historia rachunku może być ograniczona do kilku ostatnich miesięcy, a gdy klientowi będzie potrzebna dłuższa lista – wystarczy, że złoży wniosek.

Dobrze zaprojektowana i użyta minimalizacja danych będzie korzystna dla przedsiębiorcy. Systemy komputerowe przetwarzające tylko tyle danych, ile potrzeba, będą pracować szybciej. W razie wycieku danych ryzyko dla osób nie będzie tak duże jak przy pełnych danych, a co za tym idzie – potencjalne konsekwencje dla przedsiębiorcy też będą mniej dotkliwe.

## PSEUDONIMIZACJA

Gdy w pociągu usłyszymy, że „Ryba przekazał Siarze, że widział się z Bąblem, który był na ślubie Rudego", niewiele się dowiemy, gdyż niewtajemniczeni nie wiedzą, kim są Ryba, Siara, Bąbel i Rudy – prawdziwe dane osobowe zostały zastąpione pseudonimami. Takie działanie nazy-

wa się pseudonimizacją. Warto przemyśleć stosowanie pseudonimizacji na etapie projektowania przetwarzania. Przykładowo może się okazać, że w wielu przypadkach wystarczy posługiwanie się numerem klienta zamiast jego kompletnymi danymi. Pseudonimizacja stanowi jednocześnie swojego rodzaju minimalizację ilości danych w określonych operacjach przetwarzania. Nie zmniejszy ona zakresu przetwarzania danych jako takich, bo zakres zbieranych danych pozostaje bez zmian, lecz zmniejszy ryzyko dla ochrony danych w pewnych miejscach czy procesach.

## Inspektor Ochrony Danych (IOD)

Każdy przedsiębiorca musi znać wymagania stawiane przez przepisy o ochronie danych osobowych, stosować je i monitorować ich stosowanie. W niektórych przypadkach przedsiębiorca będzie zobowiązany korzystać z pomocy eksperta posiadającego odpowiednią wiedzę i doświadczenie. Stosownie do motywu 97 RODO:

**jeżeli w sektorze prywatnym przetwarzania dokonuje administrator, którego główna działalność polega na operacjach (...), to w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych.**

Nie ma znaczenia, czy w przetwarzaniu przedsiębiorca będzie administratorem, czy procesorem – jeśli spełni określone warunki, musi korzystać z pomocy fachowca, którego RODO określa mianem „inspektora ochrony danych" (ang. *data protection officer*). Jego obowiązki opisuje art. 39 RODO. Są to:

- **informowanie zainteresowanych stron o obowiązkach wynikających z przepisów i doradzanie w sprawach ochrony danych osobowych,**
- **monitorowanie przestrzegania RODO,**
- **udzielanie zaleceń co do oceny skutków dla ochrony danych i monitorowanie jej wykonania,**
- **pełnienie funkcji punktu kontaktowego dla organu nadzorczego i dla osób w związku z przetwarzaniem ich danych osobowych.**

**Inspektor ochrony danych ma pełnić funkcję pojedynczego punktu, w którym każdy może uzyskać wyczerpujące informacje na temat zgodności przetwarzania z przepisami o ochronie danych.**

Trzeba pamiętać, że jeśli organizacja nie wyznaczyła inspektora, gdyż nie miała takiego obowiązku, realizacja zadań opisanych w art. 39 RODO musi być zapewniona przez inną osobę.

Inspektora trzeba wyznaczyć zawsze, gdy:

- **dane przetwarzane są przez organ lub podmiot publiczny,**
- **główna działalność ma związek z systematycznym monitorowaniem osób na dużą skalę,**
- **główna działalność wymaga przetwarzania danych wrażliwych lub danych dotyczących wyroków skazujących i czynów zabronionych na dużą skalę.**

Inspektora można też wyznaczyć dobrowolnie.

RODO nie stawia żadnych wymagań odnośnie do wykształcenia czy też niekaralności inspektora ochrony danych. Wyznacza się go, biorąc pod uwagę przede wszystkim jego kwalifikacje zawodowe i umiejętność poradzenia sobie z obowiązkami (art. 37 ust. 5 RODO). Inspektorem musi być osoba fizyczna, nie może nim być przykładowo osoba prawna (np. spółka z o.o. czy spółka akcyjna). Inspektorem może być nawet pracownik innej firmy – ważne, aby była to osoba wskazana z imienia i nazwiska.

Z treści art. 39 RODO wynika, że inspektor ochrony danych musi:

- **znać przepisy o ochronie danych osobowych, by móc informować administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach na nich spoczywających,**
- **posiadać pewne umiejętności audytorskie, by monitorować zgodność z przepisami o ochronie danych osobowych,**
- **wiedzieć, jak wykonać ocenę skutków dla ochrony danych, co jest niezbędne do udzielania zaleceń w sprawie jej wykonania,**
- **rozumieć, jak szacować ryzyko i jak ustalać priorytety na jego bazie,**
- **umieć współpracować z organem nadzorczym.**

Inspektor ochrony danych musi być też osobą godną zaufania (art. 38 ust. 5 RODO).

W motywie 97 RODO podkreśla się, że niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający. To może prowadzić do wniosku, że inspektor powinien być trochę szyty na miarę.

Zgodnie z art. 37 ust. 2 RODO grupa przedsiębiorstw może powołać jednego inspektora ochrony danych. Podobnie jest w przypadku podmiotów publicznych – one także mogą powoływać wspólnego inspektora ochrony danych (art. 37 ust. 3 RODO). W Polsce inspektorów ochrony danych trzeba zgłaszać do organu nadzorczego. W przypadku wyznaczenia jednego inspektora dla kilku podmiotów każdy z tych podmiotów będzie zobowiązany odrębnie zgłosić go do rejestracji (art. 10 ust. 5 ustawy o ochronie danych osobowych) – nie wystarczy, że zawiadomienia dokona jeden z nich.

Można powołać zastępcę inspektora ochrony danych, który może wykonywać jego zadania w czasie jego nieobecności (art. 11a ustawy o ochronie danych osobowych). Do zastępcy stosuje się te same kryteria co do samego inspektora, w tym także zawiadamia się Prezesa UODO o jego wyznaczeniu (art. 11a ust. 3).

Jak wiemy, dane kontaktowe inspektora należy podawać podczas zbierania danych oraz w wielu innych sytuacjach. Podawanie danych związanych z konkretną osobą wiąże się z tym, że przy każdej zmianie na stanowisku inspektora trzeba będzie zmodyfikować wszystkie formularze papierowe i on-line, a to będzie kosztowne. Rozumiał to prawodawca unijny, dlatego nakazał podawać – gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych, tj. dane, które umożliwiają z nim kontakt, a nie jego dane. Polski ustawodawca nie był już tak elastyczny – zgodnie z art. 10 ust. 1 ustawy o ochronie danych osobowych imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora trzeba publikować na stronie internetowej i aktualizować przy każdej zmianie na stanowisku inspektora.

WIĘCEJ

## USŁUGOWY INSPEKTOR OCHRONY DANYCH

Dzisiaj nikogo już nie dziwi usługowe prowadzenie ksiąg finansowych. W usługowym inspektorze ochrony danych także nie ma nic złego. Gdyby nie chciano, aby funkcja inspektora ochrony danych była pełniona usługowo, to w RODO nie pojawiłby się art. 37 ust. 6, w którym określono, że „inspektor ochrony danych może (…) wykonywać zadania na podstawie umowy o świadczenie usług".

Umowa o świadczenie usługi inspektora ochrony danych może zostać zawarta z firmą zewnętrzną, przy czym inspektor musi zostać wskazany z imienia i nazwiska. W przypadku takiego inspektora podmiot świadczący usługę nie musi unikać wewnętrznego konfliktu interesów, gdyż w art. 38 ust. 6 RODO chodzi o konflikt interesów pomiędzy administratorem a wyznaczonym u niego inspektorem, a nie konflikt interesów między pracodawcą a pracownikiem. Podobnie rzecz ma się z odwoływaniem lub karaniem pracownika podmiotu świadczącego usługę inspektora – nie znajduje tu zastosowania ograniczenie wynikające z art. 38 ust. 3 RODO.

WIĘCEJ

# Zbieranie danych

Nie można przetwarzać danych na zasadzie „to może teraz zbierajmy dane i zobaczymy, jak nam to wyjdzie – jakoś to będzie". Trzeba ustalić, w jakim celu dane są zbierane (dane muszą przecież być „zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach" – zgodnie z art. 5 ust. 1 lit. b RODO), a później – jakie dane będą potrzebne do zrealizowania tego celu przetwarzania (a muszą być one „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów" – w myśl art. 5 ust. 1 lit. c RODO). Przedsiębiorca musi umieć uzasadnić, dlaczego te dane są mu potrzebne, jaką podstawę prawną znalazł do ich zbierania oraz dlaczego właśnie takie dane zbiera. Pamiętajmy, że to on jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych i musi umieć wykazać ich przestrzeganie (art. 5 ust. 2 RODO). Cel przetwarzania będzie komunikowany osobom, których dane dotyczą, więc niezbędne jest określenie go wcześniej, zanim dane zacznie się zbierać.

Warto zastanowić się nad celem w szerszym kontekście, np. określić, co administrator chce osiągnąć dzięki przetwarzaniu danych (kontekst biznesowy) i czy dane są mu potrzebne:

- **bezpośrednio (np. do marketingu bezpośredniego, telemarketingu),**
- **pośrednio (tj. firma chce sprzedawać produkty lub świadczyć usługi; danych nie potrzebuje jako takich, ale dane są potrzebne np. w celu zawarcia umowy, zapłaty rachunku itp.).**

Każde pozyskiwanie nowych danych z perspektywy administratora uznaje się za zbieranie danych. Dane mogą być zbierane na dwa sposoby:

- **bezpośrednio od osób – podczas kontaktu lub interakcji z osobą,**
- **w inny sposób – gdy dane podawane są przez inne osoby, gdy administrator kupił marketingową bazę danych lub gdy zebrał dane z Internetu.**



Mimo że RODO takiego obowiązku nie nakłada wprost, należy odnotowywać datę zebrania danych. Informacja o tym, kiedy dane zebrano, będzie potrzebna do ustalenia, jak długo dane można przechowywać. Oprócz tego należy zbierać informacje o okolicznościach zebrania danych, tj. czy dane zebrano bezpośrednio od osoby, której dotyczą, czy nie, a jeśli nie – odnotować informację o źródle pochodzenia, w szczególności gdy są to źródła powszechnie dostępne.

**Nie można zbierać większej ilości danych, niż jest to niezbędne do realizacji określonego celu przetwarzania.**

## OBOWIĄZEK INFORMACYJNY

Podczas zbierania danych osobowych – niezależnie od tego, czy dane zbiera się bezpośrednio od osób, czy nie – należy przekazać następujące informacje (art. 13 i 14 RODO):

- **tożsamość i dane kontaktowe administratora („właściciela") danych,**
- **dane kontaktowe inspektora ochrony danych (o ile został wyznaczony),**
- **cel przetwarzania danych,**
- **podstawa prawna przetwarzania,**
- **odbiorcy danych – wskazanie, komu dane udostępnia się teraz lub w przyszłości,**
- **zamiar przekazywania danych do państwa trzeciego,**
- **okres przechowywania danych,**

- **informacja o prawach przysługujące osobie, której dane dotyczą, w tym prawie do cofnięcia zgody,**
- **informacja o prawie wniesienia skargi do organu nadzorczego,**
- **jeśli dane przetwarza się na podstawie uzasadnionego interesu – określenie, jakie to są interesy,**
- **informacje o zautomatyzowanym podejmowaniu decyzji.**

Gdy dane zbiera się bezpośrednio od osoby, należy dodatkowo poinformować ją o tym, czy podanie danych jest dobrowolne, czy obowiązkowe. Jeśli podanie danych jest obowiązkowe, należy to uzasadnić; najczęściej podanie danych będzie konieczne do zawarcia umowy lub będzie wynikać z przepisów prawa. W takiej sytuacji należy wskazać możliwe konsekwencje niepodania danych.

Jeśli dane zbiera się z innych źródeł, należy przekazać jeszcze informację o źródle pochodzenia danych. Przy tego rodzaju pozyskiwaniu danych osobowych obowiązek informacyjny spełnia się zgodnie z art. 14 ust. 3 RODO:

- **w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca,**
- **jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą (np. podczas kontaktu telefonicznego czy e-mailowego),**
- **jeżeli planuje się udostępnić dane innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.**

Dawniej przepisy nakazywały przekazywać informacje osobom bezpośrednio po utrwaleniu danych, niezależnie od tego, czy dane były kompletne, czy też nie, czy ich użyto itp. Postępowanie, które wskazuje RODO, jest znacznie bardziej praktyczne.

Na szczęście stosownie do art. 13 ust. 4 i art. 14 ust. 5 lit. a RODO nie trzeba przekazywać tych informacji, które osoba już ma (które już zna). Tak będzie najczęściej w sytuacji, gdy osoba przekazuje określone dane jednostce organizacyjnej bez ich żądania, z własnej woli i chęci.

Prócz udzielenia informacji na etapie pozyskiwania danych trzeba pamiętać, że osoby mają prawo uzyskać rozmaite informacje w trakcie przetwarzania. Zgodnie z art. 15 RODO każda osoba ma prawo zapytać o to, czy jej dane są przetwarzane, a jeśli są – ma prawo wglądu w dane jej dotyczące. Ma również prawo uzyskać następujące informacje:

- **cele przetwarzania,**
- **kategorie danych osobowych,**
- **komu dane są lub mogą być przekazywane,**
- **planowany okres przechowywania lub, gdy nie jest możliwe jego wskazanie, kryteria ustalania tego okresu,**
- **informacje o przysługujących prawach,**
- **wszelkie dostępne informacje o źródle danych.**

Wgląd w dane nie zawsze będzie możliwy. Wówczas racjonalne będzie przygotowanie kopii danych. Jeśli osoba zwróci się z wnioskiem o udzielenie informacji drogą elektroniczną i nie zaznaczy inaczej, odpowiedzi należy udzielić elektronicznie. Realizacja prawa dostępu może być i kosztowna, i czasochłonna, dlatego pierwszy raz informacji należy udzielić bezpłatnie, a za kolejne kopie przepisy pozwalają pobierać „rozsądną" opłatę (art. 15 ust. 3 RODO).

## PRZESŁANKI LEGALNOŚCI, UPOWAŻNIENIA I POWIERZENIA

Przepis art. 6 ust. 1 RODO przewiduje sześć przesłanek pozwalających na przetwarzanie danych osobowych. Są to:

- **osoba, której dane dotyczą, wyraziła zgodę na przetwarzane jej danych,**
- **osoba, której dane dotyczą, dąży do zawarcia i realizacji umowy,**
- **przetwarzanie jest niezbędne do spełnienia obowiązku wynikającego z przepisów prawa,**
- **przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (np. sytuacje ratowania życia),**
- **przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,**
- **przetwarzanie jest niezbędne do celów wynikających z uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (tej przesłanki nie może wykorzystać organ publiczny w ramach realizacji swoich zadań).**

## ZGODA NA PRZETWARZANIE DANYCH

Jerzy Bralczyk o zgodzie pisał tak:

**Jedno z piękniejszych słów! Cieszymy się, gdy je słyszymy, z satysfakcją je także wypowiadamy. To nie tylko rzeczownik, to także formuła przez wieki wypracowana, słowo-zaklęcie, które, gdy wypowiedzia-**

WIĘCEJ

**ne, ustala, niemal magicznie, pożądany stan. „Zgoda?" pytamy, a gdy usłyszymy „zgoda!" – już zgoda jest. Czasem ludzie tę zgodę zawierają, czasem ją wyrażają: zgoda, która jest zawarta, likwiduje konflikty i ich skutki, zgoda, która jest wyrażona, umożliwia zamierzone przedsięwzięcia[18].**

Jedną ze szczególnych przesłanek legalności przetwarzania danych osobowych jest właśnie zgoda (art. 6 ust. 1 lit. a RODO). Mimo że wszystkie przesłanki są równe, to zgodę należy stosować wtedy, gdy nie znajdzie zastosowania żadna inna przesłanka legalności. Nie można jednak wykorzystywać zgody jako podstawy do każdego przetwarzania. Przykładowo w celu zawarcia umowy przesłanką przetwarzania danych osobowych będzie art. 6 ust. 1 lit. b RODO: „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy". Na wykorzystywanie danych w celu zawarcia lub wykonania umowy zgoda nie jest potrzebna, a nawet może wprowadzać w błąd, gdyż osoba, która zgodę wyraziła, ma prawo w dowolnym momencie ją wycofać (art. 7 ust. 3 RODO).

Jeśli dane przetwarza się na podstawie udzielonej zgody, ciężar udowodnienia zgody na przetwarzanie danych osobowych spoczywa na administratorze (art. 7 ust. 1 RODO). W przypadku gdy zgoda udzielana jest za pomocą systemu komputerowego (np. on-line), warto odnotować dokładną datę, godzinę i miejsce jej udzielenia. Trzeba pamiętać, że wyrażenie zgody wymaga aktywnej akcji – kliknięcia kwadracika ze zgodą, przesunięcia suwaka, złożenia podpisu. Zgodnie z RODO milczenia lub braku akcji nie można uznać za wyrażenie zgody.

Definicja zgody jest zawarta w art. 4 pkt 11 RODO:

**„zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.**

Przepisy RODO zliberalizowały, w odniesieniu do wcześniej obowiązujących przepisów, regulacje dotyczące formy zgody. Zgoda na przetwarzanie danych wrażliwych nie musi być już pisemna (chociaż musi być wyraźna), zezwala się też na zgodę wynikającą z działania, określaną jako „wyraźne działanie przyzwalające" (ang. *clear affirmative action*).

Zgoda będzie potrzebna najczęściej w takich przykładowych sytuacjach:

- **gromadzenie informacji o lokalizacji użytkowników aplikacji on-line w celach marketingowych,**
- **proszenie zidentyfikowanych klientów o podanie kodu pocztowego albo określenie, do jakiego przedziału wiekowego należą (o ile te dane nie są potrzebne do zrealizowania celu przetwarzania, lecz są pomocne)[19],**
- **dzielenie się danymi osobowymi z innymi podmiotami (handel danymi).**

Zgoda na przetwarzanie danych osobowych może być także „zapłatą" za usługę lub towar. Doskonałym tego przykładem są serwisy oferujące darmowe konta poczty elektronicznej w zamian za zgodę na przetwarzanie danych osobowych. Należy przy tym pamiętać, że taka zgoda musi być dobrowolna i nie można w żaden sposób przymuszać osób do jej wyrażenia. W przypadku serwisów internetowych rekomenduje się, aby pole do wyrażenia zgody, np. checkbox, domyślnie nie było zaznaczone. Dopiero samodzielne jego zaznaczenie ma oznaczać dobrowolne i świadome wyrażenie zgody.

**Współcześnie dane osobowe stały się rodzajem cyfrowej waluty, którą użytkownicy Internetu muszą płacić za korzystanie z różnego rodzaju – w teorii darmowych – usług[20].**

Innym przykładem korzyści w zamian za zgodę są rabaty, np. tańszy abonament telefoniczny. Wraz z odwołaniem zgody można zabrać taki przywilej – wówczas cena usługi lub towaru będzie wyższa – ale nie można żądać zwrotu wcześniej uzyskanych korzyści (wcześniej naliczonych rabatów).

Jeśli zgodę wyrażano elektronicznie, to wycofanie jej powinno być możliwe za pośrednictwem podobnego kanału komunikacji, gdyż zgodnie z art. 7 ust. 3 RODO „wycofanie zgody musi być równie łatwe jak jej wyrażenie". Niezgodne z przepisami jest nakazywanie odwoływania zgody wyłącznie drogą pocztową lub osobiście, jeżeli zgodę osoby wyrażają podczas rozmowy telefonicznej z call center lub on-line.

[18] J. Bralczyk, 1000 słów, Warszawa 2017, s. 52.
[19] Pytanie niezidentyfikowanych klientów, np. przy kasie w hipermarkecie, o takie same informacje nie wymaga zgody, gdyż same te informacje nie będą danymi osobowymi, a zatem nie występuje przetwarzanie danych osobowych. Jednak w połączeniu z danymi osobowymi nabiorą one cech danych osobowych.
[20] Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2015, https://giodo.gov.pl/data/filemanager_pl/sprawozdania-roczne/2015.pdf (dostęp: 17.04.2019 r.), s. 296.

# Przetwarzanie danych w zatrudnieniu

Dane o pracownikach i osobach wykonujących pracę to zapewne najczęściej pojawiające się dane osobowe w przedsiębiorstwie. Podlegają one szczególnej ochronie, ponieważ ich ujawnienie mogłoby istotnie wpłynąć na prawa i wolności osób. Do tego typu danych można zaliczyć:

- **dane o zdrowiu (orzeczenie lekarskie o braku przeciwwskazań do pracy na określonym stanowisku, dokumentacja dotycząca chorób zawodowych, dokumentacja związana z wypadkami w pracy),**
- **informacja o przynależności związkowej,**
- **informacja o skazaniach (potwierdzenie, czy osoba nie była karana, niezbędne do zatrudnienia np. ochroniarza, niektórych nauczycieli lub kierowców w transporcie drogowym),**
- **akta pracownicze (życiorys, przebieg kariery zawodowej, oceny pracownicze),**
- **informacja o wynagrodzeniu i korzystaniu z rozmaitych innych świadczeń, w tym także pozafinansowych,**
- **historia nieobecności i ich powody (chorobowe, urlopy planowanie i na żądanie),**
- **dane z monitoringu.**

Kwestie zatrudnienia uznano za wyjątkowo istotne – RODO w art. 88 ust. 1 pozwoliło państwom członkowskim wprowadzić bardziej szczegółowe przepisy w związku z zatrudnieniem. W Polsce zagadnienia te uregulowano przez wprowadzenie zmian do Kodeksu pracy.

## REKRUTACJA

W procesie rekrutacji zbiera się aplikacje kandydatów, m.in. życiorysy, listy motywacyjne, dokumenty potwierdzające wykształcenie i odbyte szkolenia. Są one źródłem cennych informacji ze sfery prywatnej kandydata. W tym procesie można zbierać w zasadzie dowolne dane, dlatego że na ich przetwarzanie osoba aplikująca na dane stanowisko powinna wyrazić zgodę (co też zresztą chętnie czyni, bo w jej interesie jest przedstawienie pracodawcy interesujących go informacji). Już samo wysłanie życiorysu i/lub listu motywacyjnego na adres określonej firmy może stanowić skuteczne wyrażenie zgody. Stosownie do motywu 32 RODO może ono „polegać na (…) innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych".

Wysłanie aplikacji pocztą elektroniczną powinno być zatem wystarczającym przyzwoleniem na przetwarzanie danych. Jednak w razie kontroli lub ewentualnych problemów łatwiej będzie to udokumentować, gdy zgody będą zbierane. Warto wiedzieć, że zgody nie są konieczne, ale tylko wówczas, gdy zakres podawanych danych nie wykracza poza ten zdefiniowany w przepisach prawa.

Trzeba pamiętać, że zgoda na etapie rekrutacji nie może obejmować informacji o nałogach, stanie zdrowia, życiu seksualnym lub orientacji seksualnej czy danych biometrycznych. Informacje o niekaralności kandydata mogą zbierać tylko ci pracodawcy, wobec których z przepisów wynika obowiązek zatrudniania osób, które nie były karane. Dodatkowo osoby mające pracować z nieletnimi powinny zostać sprawdzone w Rejestrze Sprawców Przestępstw na Tle Seksualnym (art. 12 pkt 6 ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym).

Zgoda może stanowić podstawę do przetwarzania innych danych osobowych kandydata (lub pracownika), przy czym nie mogą to być dane dotyczące wyroków skazujących i czynów zabronionych i pod warunkiem, że brak zgody bądź jej wycofanie nie będzie podstawą do niekorzystnego traktowania kandydata czy też pracownika. Dane wrażliwe, a także te dotyczące skazań i wyroków można gromadzić, o ile poda je kandydat z własnej woli. Wyjątkiem będą sytuacje, gdy przepisy prawa zezwalają lub nakazują (np. ustawa o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego). Oznacza to, że żądać takich danych nie można, ale jeśli kandydat poda je z własnej woli, to wówczas można je przetwarzać. Rekrutacja może zostać zlecona agencji pośrednictwa pracy. W większości przypadków zgoda kandydata na przetwarzanie danych wyrażana jest agencji – i to ona jest administratorem danych osobowych. Dane wybranych kandydatów są później przekazywane pracodawcy przez agencję.

Portale pośredniczące w tego typu rekrutacjach nie są administratorami danych osobowych. Udostępniają one jedynie narzędzia do publikowania ogłoszeń na portalach internetowych, zatem są co najwyżej procesorem, czyli mogą przetwarzać dane osobowe na zlecenie administratora. Obowiązek informacyjny spoczywa więc na pracodawcy.

WIĘCEJ

## MONITORING

Pracodawca udostępnia pracownikowi rozmaite narzędzia, takie jak samochód, laptop, tablet, dostęp do Internetu, telefon komórkowy itp. Korzystanie z nich w celach prywatnych generuje koszty, nie powinno więc dziwić, że pracodawca chce kontrolować, w jaki sposób te narzędzia są wykorzystywane.


Kodeks pracy zezwala na:

- **monitoring wizyjny (art. $22^2$ § 1),**
- **monitoring poczty elektronicznej (art. $22^3$ § 1),**
- **inne formy monitoringu (art. $22^3$ § 4).**

Monitoring można wprowadzić tylko wtedy, gdy jest niezbędny:

- **zapewnienia bezpieczeństwa pracowników,**
- **ochrony mienia,**
- **kontroli produkcji,**
- **zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.**

Celów monitoringu określonych przez przepisy nie można poszerzać o własne cele, np. monitorować, czy pracownik pracuje wydajnie, czy też może się leni. Kodeks pracy zobowiązuje do poszanowania godności i innych dóbr osobistych pracownika (art. $22^2$ § 2 i art. $22^3$ § 2). Decydując się na jakąkolwiek formę monitorowania, należy zadbać o to, aby nie zostały one naruszone.

Zauważmy, że w przypadku monitoringu wizyjnego ustawodawca wyraźnie mówi o tym, że chodzi o rejestrację obrazu. Należy więc wnioskować, że nie można nagrywać dźwięku. Kamery nie mogą swoim zasięgiem obejmować toalet, pryszniców i innych pomieszczeń sanitarnych, szatni, stołówek i palarni, nie można też monitorować pomieszczeń udostępnianych zakładowej organizacji związkowej.

Niezbędność monitoringu trzeba będzie umieć wykazać, więc warto ją udokumentować.

## UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Osoby mające dostęp do danych osobowych powinny zostać upoważnione do ich przetwarzania (art. 29 RODO). Upoważnienie może zostać wydane w dowolnej formie, ale w niektórych przypadkach musi być pisemne. Przykładowo zgodnie z art. $22^{1b}$ Kodeksu pracy pisemne upoważnienie należy wydać osobom mającym przetwarzać wrażliwe dane osobowe pracowników (dane szczególnych kategorii, wymienione w art. 9 ust. 1 RODO, oraz dane dotyczące wyroków skazujących i czynów zabronionych). W Kodeksie pracy podkreśla się także, że osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

Pisemne upoważnienie, a także oświadczenie o zachowaniu danych w tajemnicy i oświadczenia o zapoznaniu się z regulacjami stanowią jeden z organizacyjnych elementów ochrony danych osobowych. Można je przechowywać w aktach pracowniczych albo razem z kopiami wydanych upoważnień do przetwarzania danych osobowych.

### SZKOLENIA

Każda osoba upoważniona do przetwarzania danych osobowych musi zostać zapoznana z przepisami o ochronie danych osobowych. RODO nie nakazuje takich zadań wprost, ale można je wywnioskować z art. 39 ust. 1. Stosownie do jego zapisów do zadań inspektora ochrony danych należą m.in.:

- **działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania,**
- **informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO.**

Jeśli organizacja nie powoła inspektora, to automatycznie jego zadania przechodzą na administratora danych. O szkoleniach jest mowa także w art. 47 ust. 2 RODO.

**Człowiek może być najmocniejszym ogniwem bezpieczeństwa, tylko musi być odpowiednio przygotowany.**

Szkolenia stanowią niezwykle istotny element ochrony danych osobowych. Pełnią głównie funkcję zapobiegawczą, bo ataki takie jak phishing czy wyłudzanie haseł bądź danych odnoszą sukces głównie dlatego, że użytkownikom brakuje wiedzy o podstawowych zasadach bezpieczeństwa. Przed zagrożeniami można się bronić dzięki przeprowadzaniu odpowiednich szkoleń i pokazywaniu użytkownikom, co wolno robić, jak przetwarzać dane, jakie działania są dozwolone, a co jest absolutnie niedopuszczalne.

Istotne jest to, aby przeszkolenie odbyło się przed rozpoczęciem przetwarzania danych osobowych przez pracownika. W niedużej organizacji może to być szkolenie tradycyjne. Natomiast w dużych firmach lub tam, gdzie jest znaczna rotacja pracowników (np. centra telefoniczne), z powodzeniem można skorzystać z oferty szkoleń elektronicznych, tzw. e-learningu.

W razie naruszenia przepisów, kiedy firma zechce pociągnąć pracownika do odpowiedzialności, może on po prostu bronić się niewiedzą. Jeśli faktycznie nie został odpowiednio przeszkolony, może to prowadzić do wyłączenia jego odpowiedzialności. Dlatego też warto szkolić pracowników z zasad bezpiecznego przetwarzania danych osobowych i każdorazowo dokumentować ten fakt stosownym zaświadczeniem.

WIĘCEJ

### WYMIANA INFORMACJI MIĘDZY PRACOWNIKAMI

Jeżeli pracodawca zbiera dane osobowe zgodnie z prawem, a wymieniają się nimi osoby, które są przez niego umocowane do ich przetwarzania (upoważnione), to nie może być mowy o naruszeniu przepisów o ochronie danych osobowych, nawet jeśli inni pracownicy kwestionują dostęp do danych osobowych[21].

## Powierzenie przetwarzania danych

Adwokat (a od niedawna także radca prawny) jest przykładem zawodu, który pozwala na uzyskanie upoważnienia do reprezentowania określonej osoby przed sądem w procesie karnym – udziela mu ona pełnomocnictwa do działania w jej imieniu i na jej rzecz. Podobnie przedsiębiorca w ramach swojej działalności będzie czasami zlecał firmom zewnętrznym zadania do zrealizowania na jego rzecz. Może być także odwrotnie – to właśnie on będzie przyjmował zlecenia od innych podmiotów.

RODO zezwala na przetwarzanie danych osobowych przez firmy zewnętrzne w imieniu administratora (wynika to z treści art. 28 ust. 1). Przykładami takiego przetwarzania są następujące usługi:

- **księgowość zlecana firmie zewnętrznej,**
- **kopertowanie i wysyłka korespondencji,**
- **mailing elektroniczny,**
- **obsługa call center,**
- **przechowywanie w archiwum dokumentów firmowych,**
- **niszczenie dokumentów.**

Jeżeli korzysta się z tego typu usług, należy zawrzeć odpowiednią umowę, zgodnie z art. 28 ust. 3 RODO.

[21] Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2017, https://giodo.gov.pl/data/filemanager_pl/sprawozdania-roczne/2017.pdf (dostęp: 17.04.2019 r.), s. 38.

Taka umowa nazywa się „umową powierzenia", a podmiot, który przyjmuje dane do przetwarzania – „podmiotem przetwarzającym" lub „procesorem". Przepis art. 28 ust. 9 RODO wymaga, aby umowa powierzenia została zawarta w formie pisemnej, dopuszczalna jest forma elektroniczna.

Nie można zlecić przetwarzania jakiemukolwiek podmiotowi, gdyż zgodnie z art. 28 ust. 1 RODO można korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Przez zapewnienie tych gwarancji należy rozumieć, że podmiot:

- **będzie miał wolę podpisania umowy w formie pisemnej (co nakazuje art. 28 ust. 9 RODO), która zawiera wszystkie elementy wymagane prawem, opisane w art. 28 RODO, a szczególnie w jego ust. 3,**
- **dostarczy administratorowi dodatkowych informacji, które pozwolą mu się upewnić, że przetwarzanie przez niego danych będzie spełniało wymagania RODO, a tym samym chroniło prawa osób, a co najmniej ich nie naruszało,**
- **w sposób wiarygodny wykaże, że będzie stosował się do zasad opisanych w umowie.**

Podmiot przetwarzający może przetwarzać dane tylko w takim zakresie, na jaki pozwala mu na to umowa z administratorem danych. Nie staje się on właścicielem danych, które mu powierzono – przetwarza je wyłącznie w imieniu (i za zgodą) zleceniodawcy (art. 28 ust. 1 RODO). Dopuszczalne jest także dalsze powierzanie przetwarzania przez procesora, przy czym umowa powierzenia musi dopuszczać taką możliwość (art. 28 ust. 2 RODO). Umowę powierzenia może podpisać tylko administrator (przedsiębiorca), a właściwie osoba lub osoby, które go reprezentują. Nie może jej podpisać dyrektor określonego działu czy pracownik, chyba że posiada pełnomocnictwo do takiego działania w imieniu przedsiębiorcy.

Nie ma ograniczeń co do powierzania danych – jeśli tylko administrator ma prawo je przetwarzać, to może także powierzyć ich przetwarzanie innemu podmiotowi. Wyjątkiem jest detektyw, który nie może powierzać przetwarzania danych osobowych, gdyż zabrania mu tego art. 8 ust. 2 ustawy o usługach detektywistycznych.

Skorzystanie z usług podmiotu zewnętrznego może spowodować potencjalny wzrost ryzyka dla praw i wolności, a co za tym idzie – konieczne może okazać się wykonanie oceny skutków dla ochrony danych. Im większe ryzyko związane z powierzeniem przetwarzania, tym bardziej szczegółowo należy sprawdzić, czy podmiot zapewni wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Brak umowy powierzenia będzie powodować trudności w ustaleniu, na jakiej podstawie udostępniono innemu podmiotowi dane osobowe. Powierzenie jest w pewnym sensie uzupełnieniem podstaw prawnych do przetwarzania, gdyż każdy, kto przetwarza dane osobowe, musi mieć do tego podstawę.

Warto prowadzić rejestr umów powierzenia przetwarzania danych osobowych. Pozwoli to panować nad tym, kto przetwarza dane osobowe w imieniu przedsiębiorcy, a także zweryfikować, czy dokonano sprawdzenia wiarygodności podmiotu, w jakim zakresie i kiedy zaplanowano kolejne sprawdzenie itp. W rejestrze dobrze też przechowywać informacje o podmiotach, którym przetwarzanie powierzył podmiot przetwarzający. Taki rejestr co prawda nie jest obowiązkowy, a przynajmniej RODO nie nakazuje go prowadzić, ale bez niego będzie trudno kontrolować zleceniobiorców.

WIĘCEJ

# Jak bezpiecznie prowadzić marketing

Przepisy RODO zezwalają na marketing bezpośredni, nie trzeba do tego celu zbierać żadnych dodatkowych zgód. Prawodawca unijny uznał, że marketing jest istotny w działalności przedsiębiorcy, zrównał go zatem z innymi prawnie usprawiedliwionymi celami przetwarzania

danych. Zgodnie z przesłanką z art. 6 ust. 1 lit. f RODO przetwarzanie jest zgodne z prawem, gdy:

**przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.**

Prawo prowadzenia marketingu na takiej podstawie ma pewne wady – wygasa ono wraz z zakończeniem głównego celu przetwarzania danych osobowych (np. z zakończeniem umowy z klientem), a więc jest ograniczone czasowo. Dodatkowo w ramach tej przesłanki dozwolony marketing musi być raczej łagodny, wyważony, nieuciążliwy, spodziewany, niezaskakujący osób, których dotyczy. Z tego powodu warto zbierać dodatkowe zgody, które określa się mianem „marketingowych". Takie zgody pozwalają przedsiębiorcy na więcej, w tym również na bardziej intensywny marketing, także po zakończeniu umowy.

Planując działania marketingowe, należy brać pod uwagę to, jaki kanał komunikacyjny będzie wykorzystywany. Jeśli marketing będzie prowadzony drogą telefoniczną, podczas zbierania zgód należy dodatkowo pamiętać o art. 172 ust. 1 Prawa telekomunikacyjnego:

**Zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę.**

Wymóg uzyskania zgody abonenta czy użytkownika końcowego stanowi obowiązek niezależny od obowiązku dysponowania przez administratora danych podstawą prawną przetwarzania danych osobowych do celów marketingowych.



Natomiast w przypadku marketingu za pomocą poczty elektronicznej należy brać pod uwagę art. 10 ustawy o świadczeniu usług drogą elektroniczną:

1. **Zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.**
2. **Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny.**

# Grupy kapitałowe

W poprzednim stanie prawnym grupy przedsiębiorstw były zupełnie niezauważane przez przepisy o ochronie danych. Każde przedsiębiorstwo było traktowane jako odrębny podmiot – i to bez wyjątków. W RODO wyróżniono grupę przedsiębiorstw (ang. *group of undertakings*) – grupę przedsiębiorstw zależnych od siebie – oraz grupę przedsiębiorców (ang. *group of enterprises*).

RODO pozwala grupom przedsiębiorstw na wyznaczenie jednego inspektora ochrony danych. Zezwala też na wymianę danych osobowych osób zatrudnionych w ramach uzasadnionego interesu, co podkreśla motyw 48 RODO:

**Administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji powiązanych z podmiotem centralnym, mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników. Pozostaje to bez wpływu na ogólne zasady przekazywania danych osobowych w ramach grupy przedsiębiorstw przedsiębiorstwu mieszczącemu się w państwie trzecim.**

Przepisy ułatwiają też wymianę (transfery) danych osobowych w ramach grup, w których skład wchodzą podmioty z państw trzecich – jest temu poświęcony art. 47 RODO.

Aby w grupie przedsiębiorstw korzystać z efektu synergii i prowadzić wspólny marketing, należy przemyśleć dokładnie sposób, w jaki będzie się zbierać dane osobowe. Marketing na podstawie uzasadnionego interesu jest możliwy. Jedna spółka może też promować pozostałe, co w porównaniu do dawniej obowiązujących przepisów stanowi ogromne udogodnienie.

# Polityki ochrony danych

Wyobraźmy sobie ekskluzywną restaurację. Co dla jej właściciela będzie szczególnie ważne? Jakie istotne zasady postępowania chciałby przekazać swoim pracownikom? Pierwsza myśl jest taka, aby przygotowywanie posiłków odbywało się w higienicznych warunkach, wnętrze pozostawało czyste oraz aby zachowano pewną estetykę. Na pewno ważne byłoby też stosowanie odpowiednich receptur, aby potrawy zawsze smakowały i były przyrządzane tak samo dobrze. Istotne jest także zapewnienie określonego standardu obsługi klienta i postępowania w razie reklamacji, a także ustalenie wielu innych zasad, gwarantujących bezproblemowe prowadzenie restauracji. Wszystkie te elementy to sposoby właściciela na uzyskanie i utrzymanie określonego poziomu usług, a także wyraz jego woli stosowania się do ustalonych założeń. Takie kluczowe założenia można nazwać polityką.

W kolejnym kroku ustalone założenia przekłada się na szczegółowe zasady. Przykładowo: posiłki należy przygotowywać w czystej kuchni, ze świeżych składników, a pracownicy powinni nosić odpowiednie ubranie robocze (czepek, fartuch). Te zasady, ze względu na szczegółowość, dzielą się na tzw. standardy i procedury. W tym konkretnym przypadku standard określa, że przed rozpoczęciem pracy należy umyć ręce, procedura zaś uszczegóławia, jak i czym je umyć (np. płynem Impuls 10 SD). Taka szczegółowa dokumentacja to po prostu instrukcja utrzymania czystości i higieny.

RODO nie wymaga, aby podmiot, który przetwarza dane osobowe, przygotował w każdym przypadku polityki bezpieczeństwa – pozostawia to jego ocenie. Przepisy art. 24 ust. 1 i 2 RODO określają, że jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, odpowiednie środki techniczne i organizacyjne obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych. Ten zapis jest bardzo korzystny, gdyż dawniej każdy był zobowiązany mieć polityki, nawet osoba samodzielnie prowadząca jednoosobową działalność gospodarczą. W obecnym stanie prawnym polityki należy posiadać wówczas, gdy jest to potrzebne i gdy wynika to z oceny ryzyka.

Rola polityk jest bardzo istotna. Zasadniczo warto je przygotować i zadbać o ich praktyczność, aby dobrze służyły organizacji. Należy zauważyć, że będą przydatne w przypadku prowadzenia rejestru czynności przetwarzania – rejestr bowiem musi zawierać ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 30 ust. 1 lit. g RODO), a jeśli w organizacji będą polityki, to w rejestrze wystarczy tylko powołać się na nie.

Warto pamiętać, że jednym z obowiązków inspektora ochrony danych (lub określonego podmiotu – jeśli nie wyznaczono inspektora) jest monitorowanie zgodności z wewnętrznymi politykami administratora (art. 39 ust. 1 lit. b RODO). Takie monitorowanie powinno się zaplanować, a następnie udokumentować wykonanie tego obowiązku.

# Zabezpieczenie danych osobowych

Przepis art. 32 ust. 1 RODO wskazuje:

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

W tym artykule użyto określenia „odpowiednie" – łatwo się domyślić, że wybór zabezpieczeń należy do organizacji, to ona musi więc ocenić, czy są one odpowiednie, czy nie są. Ocena zabezpieczeń będzie wynikać z oceny ryzyka dla praw i wolności osób. W niektórych przypadkach ich dobór ułatwi także ocena skutków dla ochrony danych, pomóc mogą również tzw. uprzednie konsultacje. Przepis art. 32 ust. 2 RODO podkreśla, że oceniając, czy stopień bezpieczeństwa jest odpowiedni, należy uwzględnić ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

**Zapewnienie bezpieczeństwa danych osobowych to takie ich przetwarzanie, które nie powoduje zagrożenia dla praw i wolności osób, których te dane dotyczą.**

## TECHNICZNE I ORGANIZACYJNE ŚRODKI BEZPIECZEŃSTWA

Zabezpieczenia danych osobowych można podzielić na techniczne oraz organizacyjne. Organizacyjne środki to nic innego jak organizacja zadań w jednostce w taki sposób, aby podnosić bezpieczeństwo przetwarzanych danych osobowych. Za takie środki uważa się także wdro-

żenie polityk ochrony danych i polityk bezpieczeństwa. Są nimi również m.in.:

- **szkolenie osób zatrudnionych przy przetwarzaniu danych z przepisów dotyczących ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,**
- **nadanie upoważnień do przetwarzania danych osobowych i zobowiązanie do zachowania ich w tajemnicy (bezpośrednio wymagane przez rozmaite akty prawne),**
- **nadanie uprawnień w systemach, adekwatnych do powierzonych obowiązków,**
- **niszczenie dokumentów w ustalony wewnętrznie sposób,**
- **ustawienie monitorów komputerów w sposób uniemożliwiający wgląd osobom postronnym.**

Pośród zabezpieczeń technicznych należy wyróżnić zabezpieczenia fizyczne, np.:

- **zabezpieczenia pomieszczeń, odpowiednie do występujących zagrożeń (właściwy rodzaj drzwi, zabezpieczenie okien – kratami, roletami lub folią antywłamaniową),**
- **system alarmowy,**
- **kontrola dostępu do pomieszczeń,**
- **monitoring z użyciem kamer,**
- **przechowywanie danych w szafach zamykanych na klucz (metalowych i niemetalowych), sejfach i kasach pancernych,**
- **niszczenie danych z użyciem niszczarek bądź przez profesjonalną firmę zewnętrzną.**

Nie sposób nie wspomnieć o zabezpieczeniu danych osobowych w systemach informatycznych. Ten temat obejmuje zagadnienia często opisywane jako cyberbezpieczeństwo danych, co odnosi się do wszystkich danych przetwarzanych komputerowo w organizacji, w tym danych osobowych. W uproszczeniu materia ta dotyczy m.in.:

- **zasad dostępu do danych w systemach informatycznych,**
- **zarządzania uprawnieniami użytkowników oraz dostępami uprzywilejowanymi (administracyjnymi),**
- **polityki haseł,**
- **zasad instalowania poprawek bezpieczeństwa,**
- **kontroli antywirusowej i antyspamowej,**
- **filtrowania ruchu do i z Internetu i sieci publicznych,**
- **rejestrowania zdarzeń z systemów i ich monitorowania,**
- **wykonywania zapasowych kopii danych,**
- **projektowania bezpiecznych rozwiązań informatycznych.**

## USTAWIENIE MONITORA

Wydawałoby się, że ustawienie monitora nie ma większego znaczenia dla ochrony danych osobowych. A jednak! O odpowiednim ustawieniu monitorów powinny pamiętać przykładowo te osoby, które pracują w dużym budynku biurowym. Niektóre biurowce są często całkowicie przeszklone, co może umożliwić niezamierzone udostępnienie danych. Może się zdarzyć, że ktoś, wykorzystując aparat z dużym przybliżeniem (zoomem), sfotografuje zawartość ekranu komputera nawet z budynku naprzeciwko. Jeśli więc na komputerze są przetwarzane poufne dane, warto się zabezpieczyć przed takimi zagrożeniami. Szczególną uwagę należy zwrócić na ustawienie monitorów kadry kierowniczej, która ma dostęp do najbardziej poufnych informacji.

Ważne jest to, aby danych osobowych nie odczytała (nie zapoznała się z nimi) osoba nieupoważniona. Warto też, aby komputer był zabezpieczony wygaszaczem ekranu na hasło – jeśli pracownik zapomni zablokować ekran, po określonym czasie wygaszacz uruchomi się samoistnie. W ten sposób na ekranie nie będą wyświetlane żadne dane, a osoby nieupoważnione nie będą miały do nich dostępu.

## NISZCZENIE DOKUMENTÓW W NISZCZARCE

Dokumenty zawierające ważne informacje nie powinny być wyrzucane do kosza ani na śmietnik. Aby mieć pewność, że przed zutylizowaniem nie trafią w niepowołane ręce, przed wyrzuceniem warto zadbać o ich zniszczenie. Zdarzały się przecież sytuacje, gdy dokumenty zawierające dane osobowe znajdowano na śmietnikach.

Dokumenty należy niszczyć skutecznie. Najłatwiej użyć niszczarki dokumentów. Pracują one w trzech klasach ochrony (oraz na siedmiu poziomach bezpieczeństwa) według normy DIN 66399. Niszczarkę pracującą w klasie drugiej można kupić już za mniej niż 100 zł.

## NISZCZENIE NOŚNIKÓW DANYCH

Tak jak dokumentów papierowych, na śmietnik nie wolno wyrzucać elektronicznych i magnetycznych nośników danych. Nawet jeśli dane zostały usunięte, należy pamiętać, aby utylizować elektronikę zgodnie z ustawą o zużytym sprzęcie elektrycznym i elektronicznym.

W przypadku taśmowych magnetycznych nośników danych (podobnych do dawnych kaset wideo i magnetofonowych), na których zazwyczaj tworzy się kopie zapasowe, najlepszym sposobem utylizacji będzie rozwinięcie i pocięcie taśmy na kawałki. Szansa na to, że ktoś je poskłada, jest w zasadzie żadna.

Płyty CD i DVD najlepiej zniszczyć w niszczarce (wiele modeli oferuje taką funkcjonalność) lub też po prostu przeciąć na pół nożyczkami. Nie będzie skuteczne znisz-

czenie płyty przez jej porysowanie albo pomazanie flamastrem, ponieważ rysy można wypolerować, a ślady flamastra – zmyć.

W przypadku odsprzedaży lub przekazania w formie darowizny firmowego komputera należy wcześniej pozbawić go danych. Niekiedy wyjmuje się w tym celu dyski i przekazuje urządzenia bez nośników, częściej jednak usuwa się z nich dane, wykorzystując do tego specjalne programy. Należy zapamiętać, że zwykłe usunięcie danych (plików i folderów), a nawet sformatowanie dysku nie usuwa w rzeczywistości plików (a więc i danych osobowych) z powierzchni dysku.

**Pełne formatowanie nie usuwa danych z dysku.**

Czy tzw. pełne formatowanie usuwa dane? Niestety także nie. Jedyna różnica między formatowaniem szybkim a pełnym jest taka, że przy pełnym formatowaniu dysk jest dodatkowo sprawdzany w poszukiwaniu uszkodzonych sektorów. W systemie Windows 10, aby mieć pewność, że z dysku nie da się już nic odczytać, do polecenia formatowania należy dodać dodatkowe parametry:

**format c: /P:2**

Można też skorzystać z darmowego programu Sdelete, który jest dostępny w Internecie[22]. Po usunięciu plików, zamiast nadpisywania dysku danymi, wystarczy uruchomić ten program, wydając polecenie:

**sdelete.exe -p 2 -c c:\.**

Cyfra „2" (podobnie jak w poprzednim przykładzie) wskazuje, ile razy to samo miejsce ma zostać nadpisane, a parametr „c" określa, że na dysku należy „wyczyścić" miejsce zwolnione po usuniętych plikach[23].

WIĘCEJ

[22] https://docs.microsoft.com/pl-pl/sysinternals/downloads/sdelete (dostęp: 17.04.2019 r.).
[23] Program należy uruchomić z tzw. terminala (Start > Uruchom > cmd.exe).

# Terminy usuwania danych osobowych

Podstawową zasadą przetwarzania jest ograniczenie przechowywania, opisane w art. 5 ust. 1 lit. e RODO. Każdy administrator danych z własnej inicjatywy powinien usuwać dane osobowe, gdy skończy się powód, dla którego te dane zebrał. Co więcej, przedsiębiorca musi wiedzieć, ile czasu dane będzie mógł przechowywać, gdyż takie informacje musi podać osobom na etapie zbierania ich danych. Zagadnienia związane z okresem przechowywania danych osobowych w języku branżowym określa się terminem „retencja danych osobowych" (wyraz ten pochodzi od łac. *retentio* – powstrzymywać).

Artykuł 17 RODO, zatytułowany „Prawo do usunięcia danych (»prawo do bycia zapomnianym«)", wymienia sytuacje, w których należy usuwać dane osobowe. RODO nie określa, co należy rozumieć przez usunięcie, ale z ostatnich 20 lat praktyki stosowania przepisów wiemy, że przez usunięcie danych rozumiało się „zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą" (art. 7 pkt 3 dawnej ustawy o ochronie danych osobowych).

Dane osobowe są najczęściej usuwane, gdy:

- **przestały być niezbędne do celów, w których zostały zebrane (art. 17 ust. 1 lit. a RODO),**
- **były przetwarzane na podstawie zgody, a ta została odwołana (art. 17 ust. 1 lit. b RODO).**

W obu przypadkach termin usunięcia będzie zależeć od tego, czy dane będą niezbędne do „ustalenia, dochodzenia lub obrony roszczeń" (art. 17 ust. 3 lit. e RODO) lub czy dane trzeba będzie przechowywać po to, aby zapewnić zgodność z prawem (art. 17 ust. 3 lit. b RODO).



## PRAWO DO ZAPOMNIENIA

Podmiot danych (osoba, której dane dotyczą) ma prawo żądać usunięcia danych oraz zaprzestania ich rozpowszechniania, w tym także usunięcia odnośników albo kopii tych danych przez innych administratorów, po warunkiem że zachodzi co najmniej jednak z następujących przesłanek:

- **dane nie są już potrzebne do celu, do którego zostały zebrane,**
- **osoba cofnęła zgodę na przetwarzanie,**
- **osoba sprzeciwia się np. marketingowi bezpośredniemu,**
- **dane zostały zebrane bezprawnie,**
- **dane nakazuje usunąć wyrok sądu albo decyzja organu nadzorczego.**

Należy pamiętać, że żądanie i obowiązek usunięcia danych nie mają zastosowania, gdy przetwarzanie jest niezbędne m.in. w celu zachowania zgodności z przepisami lub w celu ustalenia, dochodzenia i obrony roszczeń. Zatem jeśli przepisy prawa nakazują dane przechowywać, to nie można ich usunąć, nawet gdy osoba, której dane dotyczą, tego żąda.

# Co zrobić, gdy dane osobowe wyciekną

Firma Avid Life Media jest właścicielem trzech znanych na całym świecie portali randkowych: Ashley Madison, zachęcającego osoby w związku do zdrady, Established Men, łączącego bogatych mężczyzn z ładnymi, młodymi dziewczynami, oraz Cougar Life, skierowanego do pań szukających osób przeciwnej płci, znacznie młodszych od siebie. Podczas zakładania konta w każdym z tych serwisów podaje się adres e-mail, numer telefonu, zamieszcza własne zdjęcia, pisze parę słów o sobie (wiek, status w związku, informacje o preferencjach, np. jakiego partnera się szuka, jakie ma się fantazje itp.). Za korzystanie trzeba płacić, więc nawet jeśli poda się fałszywe dane w profilu, serwis i tak zna tożsamość użytkownika. W lipcu 2015 r. zrobiło się bardzo głośno o wycieku danych osobowych z portalu Ashley Madison – wykradziono wówczas pełną bazę danych 39 mln użytkowników tego serwisu. Włamywacz postawił wa-

runek, że portal ma zniknąć z Internetu, a gdy tak się nie stało – opublikował wykradzione dane, które mogły być przeglądane przez każdego, kto tylko miał dostęp do Internetu. W tym portalu rejestrowali się także Polacy (ok. 20 tys. kont).

Wczujmy się trochę w rolę użytkownika i pomyślmy, jak taki wyciek mógłby na niego wpłynąć. Co by było, gdyby rodzina, przyjaciele, współpracownicy, szef zobaczyli opisy, historie czatów i fotografie bądź nagrania wideo opublikowane w takim portalu?

O takich wyciekach jesteśmy informowani każdego dnia – wydawałoby się, że nie jest to jakaś wielka rzecz. Opisany incydent był jednak wyjątkowy, bo miał znaczący wpływ na losy osób, które korzystały z portalu i których dane zostały ujawnione. Ponoć niektórzy użytkownicy z powodu wycieku popełnili samobójstwo[24], a społeczność LGBT (ang. *Lesbian, Gay, Bisexual, Transgender*) była zagrożona (w wielu krajach homoseksualizm jest nielegalny, a w niektórych za takie kontakty seksualne grozi kara śmierci). Być może podany przykład jest nieco przesadzony, ale dzięki niemu widać wyraźnie, że niekiedy wyciek danych może mieć znaczący wpływ na osoby, których dane dotyczą.

Nie dziwi więc, że w RODO uregulowano kwestie wycieków danych. Przede wszystkim wprowadzono obowiązek notyfikacji zdarzenia organowi nadzorczemu w terminie do 72 godzin od stwierdzenia naruszenia ochrony danych osobowych, a w szczególnych przypadkach także osobom, których dane dotyczą. Z motywu 85 RODO można wywnioskować, że dzięki odpowiedniej i szybkiej reakcji wpływ na prawa i wolności osób może być mniejszy.

Zawiadomienie organu nadzorczego oraz osób objętych incydentem (naruszeniem) przynosi następujące korzyści:

- **w przypadku poinformowania organu – organ może poinformować administratora o ewentualnej konieczności notyfikowania incydentu osobom, których dane dotyczą.**
- **w przypadku poinformowania osób – uzyskują one wiedzę o ryzykach, co pozwala się im ochronić i przygotować na najgorsze.**

Podmiot przetwarzający nie zgłasza naruszenia do organu, zgłasza je natomiast administratorowi (art. 33 ust. 2 RODO). Umowa z podmiotem przetwarzającym musi zatem regulować kwestie zgłaszania naruszeń do administratora.

Aby móc zgłaszać naruszenia, trzeba posiadać procedurę ich raportowania i umieć je wykrywać (motyw 87 RODO). Operatorzy kluczowi, dostawcy usług cyfrowych i podmioty publiczne przy planowaniu zasad postępowania z naruszeniami mogą je „zintegrować" z zasadami postępowania z incydentami, opisanymi w ustawie o krajowym systemie cyberbezpieczeństwa.

Etapy procesu zarządzania incydentami (naruszeniami) są następujące:

- **przygotowanie – procedury i mechanizmy pozwalające jak najszybciej wykryć i zgłosić naruszenie,**
- **wykrycie incydentu i zgłoszenie go odpowiedniej osobie w organizacji,**
- **klasyfikacja i analiza, tj. określenie rodzaju i stopnia zdarzenia, ocena skutków incydentu i podjęcie decyzji, czy notyfikacja jest konieczna i w jakim zakresie,**
- **postępowanie z naruszeniem – ograniczanie jego rozmiaru, zabezpieczanie dowodów, usuwanie powodów, naprawa lub odzyskiwanie systemów itp.,**
- **notyfikacja – poinformowanie o naruszeniu organu nadzorczego i osób, których dane zostały dotknięte incydentem,**
- **zamknięcie postępowania i lekcje na przyszłość – uzupełnienie rejestru incydentów, analiza, co było powodem naruszenia i wyciągnięcie wniosków, jak można zapobiec podobnym sytuacjom.**

Naruszenia muszą być dokumentowane. Zgodnie z art. 33 ust. 5 RODO:

**Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.**

Każdy pracownik i każdy podmiot współpracujący (zleceniobiorca przetwarzający dane osobowe) powinien wiedzieć, do kogo i jak zgłaszać incydenty. Czas ma w takich sytuacjach ogromne znaczenie – szybka reakcja to mniejsze straty.

Dużą wagę warto przykładać do odpowiedniej komunikacji w sprawie naruszenia bezpieczeństwa informacji. Osoba za nią odpowiedzialna (rzecznik prasowy, ekspert ds. public relations) powinna więc ściśle współpracować z administratorem bezpieczeństwa informacji i innymi zaangażowanymi działami. Brak takiej współpracy może spowodować poważny kryzys zaufania do firmy.

WIĘCEJ

[24] Zob. https://www.inquisitr.com/2362686/police-2-unconfirmed-suicides-of-ashley-madison-hack-victims-names-list-daily-mail-says-it-may-be-3-suicides/ (dostęp: 17.04.2019 r.).

# Kontrola Urzędu Ochrony Danych Osobowych

Prezes UODO ma możliwość kontrolowania nawet tych podmiotów, które nie przetwarzają żadnych danych osobowych – choćby po to, aby się upewnić, że rzeczywiście tak jest. Oczywiście może on kontrolować też podmioty, które przetwarzają dane osobowe w imieniu przedsiębiorcy, tzw. procesorów.

**Prezes UODO może skontrolować każdy podmiot.**

Najczęściej sygnałem dającym Prezesowi UODO impuls do kontroli są skargi osób w sprawie naruszenia przepisów o ochronie danych osobowych. Warto zwrócić uwagę, że złożenie skargi do organu nie wiąże się już z koniecznością wniesienia stosownej opłaty, jest więc bardzo prawdopodobne, że najpierw taka skarga zostanie skierowana do organu zamiast do podmiotu naruszającego przepisy. Na szczęście organ na swojej stronie internetowej informuje: „ponieważ Prezes Urzędu jest organem kontrolującym prawidłowość stosowania przepisów o ochronie danych osobowych przez administratora, składający skargę w pierwszej kolejności powinien zwrócić się do administratora w celu realizacji swoich uprawnień”[25]. Dlatego dzięki dbaniu o rzetelne podejście do skarg i reklamacji klientów w zakresie przetwarzania danych osobowych przedsiębiorcy mogą skutecznie zmniejszyć ryzyko wpłynięcia na nich skarg i w konsekwencji – ryzyko kontroli.

Bodźce inicjujące kontrolę mogą pochodzić od podmiotów, z którymi organ podpisał stosowne porozumienia. Przykładowo w 2012 r. podpisano porozumienie z Państwową Inspekcją Pracy (PIP), która zobowiązała się m.in. do zawiadamiania o stwierdzonych, w czasie swoich kontroli, nieprawidłowościach w zakresie zgodności przetwarzania danych z przepisami o ochronie danych osobowych[26].

Zazwyczaj podmiot kontrolowany jest telefonicznie informowany o planowanej kontroli z pewnym wyprzedzeniem. Następnie na piśmie (czasem faksem) przedstawiany jest przedmiot kontroli, z potwierdzeniem terminu i prośbą o przygotowanie określonych materiałów[27]. Nie ma obowiązku odpisywania na zawiadomienie o kontroli. Wyjątkiem jest sytuacja, gdy kontrolowanemu podmiotowi, z uzasadnionych przyczyn, nie odpowiada termin ustalony przez organ. Można wówczas wnioskować o jego zmianę.

Do kontroli warto się przygotować i samemu wcześniej sprawdzić, czy wszystko jest w porządku, zanim sprawdzą to kontrolerzy.

Kontrolerzy, którzy przychodzą na kontrolę, są zobowiązani posiadać imienne upoważnienia do kontroli, chyba że na kontrolę przyjdzie sam Prezes UODO. Nie należy obawiać się legitymowania kontrolerów i sprawdzania ich upoważnień. Sprawdzanie tożsamości i upoważnień rozmaitych kontrolerów, nie tylko z organu nadzorczego, należy przyjąć za dobrą praktykę. Potencjalnie mógłby przecież przyjść pracownik konkurencji, twierdzący, że jest kontrolerem, i uzyskać w ten sposób dostęp do informacji, których normalnie nikt by mu nie ujawnił. W razie wątpliwości zawsze można zadzwonić do UODO (dane są dostępne na jego stronie internetowej[28]) i potwierdzić, czy kontrola faktycznie ma się odbyć oraz czy wskazane osoby są uprawnione do jej przeprowadzenia. Takie działanie nie może zostać uznane za utrudnianie czynności kontrolnych.

Podstawowym obowiązkiem kontrolowanego podmiotu jest umożliwienie przeprowadzenia kontroli. Nie można jej utrudniać ani uniemożliwiać, bo to jest karane (art. 108 ustawy o ochronie danych osobowych). Należy więc wpuścić kontrolerów do firmy, jeśli okażą ważną legitymację i upoważnienie, a następnie umożliwić im przeprowadzenie kontroli. To oznacza, że należy:

- **składać niezbędne wyjaśnienia (pisemne albo ustne; wydruk e-maila jest formą pisemną),**
- **udostępnić żądane dokumenty do wglądu albo kopie (kopie warto przekazywać za protokołem przekazania),**
- **pozwolić na dokonanie oględzin systemów informatycznych, urządzeń i nośników służących do przetwarzania danych osobowych,**
- **umożliwić wgląd w dane osobowe (za pośrednictwem lub pod nadzorem upoważnionej osoby).**

W przeszłości organ zaczynał kontrolę od sprawdzenia dokumentacji. RODO tego nie zmieniło, a nawet ułatwiło sprawę, dzięki wprowadzeniu zasady rozliczalności, która m.in. nakazuje, aby administrator był w stanie wykazać, że przepisy RODO są stosowane (art. 5 ust. 2). W praktyce najłatwiej to wykazać za pomocą dokumentacji.

Na stronach internetowych organu poświęconych dokumentacji zgodnej z RODO[29] dowiadujemy się, jaka

[25] https://uodo.gov.pl/pl/83/154 (dostęp: 17.04.2019 r.).
[26] Zob. http://www.giodo.gov.pl/259/id_art/5767/j/pl (dostęp: 17.04.2019 r.).
[27] Generalny Inspektor Ochrony Danych Osobowych, ABC zasad kontroli przetwarzania danych osobowych, Warszawa 2007, s. 19.
[28] Zob. https://uodo.gov.pl/pl/138/465 (dostęp: 17.04.2019 r.).
[29] https://uodo.gov.pl/pl/138/273

dokumentacja, zdaniem organu, powinna zostać przygotowana. Składają się na nią m.in.:

- **rejestry czynności przetwarzania (art. 30) prowadzone przez podmiot zarówno będący administratorem, jak i występujący w roli procesora,**
- **rejestr naruszeń ochrony danych (art. 33 ust. 5 RODO),**
- **oceny ryzyka i oceny skutków dla ochrony danych (art. 35 ust. 7 RODO),**
- **rejestr osób uprawionych (upoważnionych) do przetwarzania danych.**

Każdy z rejestrów zawiera bardzo istotne dla organu informacje. Przykładowo z rejestru czynności przetwarzania kontrolujący dowie się, jakie dane są przetwarzane, kogo dotyczą, kiedy mają być usuwane, jak są zabezpieczone, czy podmiot jest administratorem tych danych, czy też przetwarza je w czyimś imieniu. Jest to doskonały punkt zaczepienia.

Jeśli okaże się, że taki rejestr w ogóle nie jest prowadzony, kontrolerom będą przedstawiane różne wersje tego samego rejestru bądź wyjaśnienia dotyczące rejestru będą chaotyczne czy niespójne, może to doprowadzić do wielu niepotrzebnych problemów, nawet gdy samo przetwarzanie jest zgodne z przepisami. Warto więc mieć taki rejestr, a nawet pokusić się o dopisanie do niego dodatkowych informacji, takich jak np. podstawa prawna przetwarzania czy cykl życia danych tj. w jakich miejscach dane są zbierane, przez kogo, komu przekazywane, w jakich miejscach gromadzone, gdzie archiwizowane, kiedy usuwane.

Z oceny ryzyka i oceny skutków dla ochrony danych kontrolujący dowie się, czy przetwarzanie nie stwarza zbyt dużego ryzyka dla osób i czy zastosowane zabezpieczenia są „odpowiednie". Rejestr naruszeń jest obowiązkowy i pozwoli sprawdzić nie tylko to, czy miały miejsce „wypadki przy pracy", lecz także to, jak sobie z nimi poradzono.

Mimo że prowadzenie dokumentacji nie jest bardzo skomplikowane, warto wesprzeć się specjalistycznym oprogramowaniem, które pozwoli przechowywać ją w jednym miejscu, ułatwi jej prowadzenie, podpowie jakie informacje wpisać, a nawet przypomni o konieczności aktualizacji.

Kontrolerów nie wolno pozostawiać bez opieki – po terenie firmy powinni poruszać się pod nadzorem osoby wyznaczonej przez przedsiębiorcę. Kontrola kończy się protokołem kontroli (art. 88 ust. 1 ustawy o ochronie danych osobowych).

Przepis art. 73 ustawy o ochronie danych osobowych określa, że po zakończeniu postepowania organ może poinformować o wydaniu decyzji na swojej stronie w Biuletynie Informacji Publicznej (BIP), jeśli uzna, że przemawia za tym interes publiczny. To oznacza, że pełne wyniki postępowania w sprawie naruszenia przepisów o ochronie danych osobowych przez przedsiębiorcę mogą być publicznie dostępne. Jest to bardzo duża zmiana w stosunku do poprzednich przepisów. Wcześniej, jeśli publikowano orzeczenia czy decyzje, dane podmiotu będącego ich adresatem były anonimizowane. W przypadku organów publicznych jest nieco inaczej – każdy z nich, jeśli był podmiotem prawomocnej decyzji stwierdzającej naruszenie, musi na swojej stronie internetowej lub na stronie Biuletynu Informacji Publicznej opublikować informację o działaniach podjętych w celu wykonania decyzji.

WIĘCEJ

# Odpowiedzialność karna, administracyjna i cywilna

Rozporządzenie unijne przyniosło ze sobą bardzo wysokie kary, przemawiające do wyobraźni. Zmieniło też model karania za niezgodność. Niezależnie od kar wynikających z przepisów „każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę" (art. 82 ust. 1 RODO).

Nowe przepisy ustanowiły dwa rodzaje kar:

- **w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (art. 83 ust. 4 RODO),**
- **w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (art. 83 ust. 5 RODO).**

Poprzez ustanowienie dwóch różnych maksymalnych wysokości administracyjnej kary pieniężnej wskazuje się, że naruszenie niektórych przepisów RODO może być poważniejsze niż naruszenie innych przepisów. Wyższe progi kar mają zastosowanie do naruszenia:

- **podstawowych zasad przetwarzania, takich jak zgodność z prawem, rzetelność, przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość danych, rozliczalność itd. (art. 5 RODO),**
- **zgodności przetwarzania z prawem, przykładowo**

**gdy nie ma przesłanek legalności przetwarzania danych (art. 6 RODO), zwłaszcza szczególnych kategorii danych osobowych (art. 9 RODO),**

- **praw osób wynikających z art. 12–22 RODO (przejrzyste informowanie, obowiązki informacyjne na etapie zbierania danych, prawo dostępu do danych, prawo do sprostowania danych, prawo do bycia zapomnianym, ograniczenie przetwarzania, sprzeciw, profilowanie itd.),**
- **przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (art. 44–49 RODO),**
- **wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX RODO (przetwarzanie numeru PESEL, przetwarzanie w związku z zatrudnieniem, dostęp do informacji publicznej).**

Dodatkowo wyższe kary będą mieć zastosowanie w przypadku, gdy podmiot nie będzie przestrzegał nakazów organu nadzorczego, wydanych w wyniku korzystania przez organ z uprawnień przewidzianych w art. 58. ust. 2 RODO. Przykładowo gdy organ nadzorczy nakaże ograniczyć przetwarzanie, a ten nakaz nie zostanie uwzględniony, zastosowanie będzie mieć wyższa kara.

Oczywiście są to górne limity kar. Organ nadzorczy ma w każdym przypadku stosować kary skuteczne, proporcjonalne i odstraszające (art. 83 ust. 1 RODO), a także nakładać je w zależności od okoliczności każdego indywidualnego przypadku (art. 83 ust. 2 RODO). Przy ustalaniu wysokości kary pod uwagę brane są m.in. następujące czynniki:

- **charakter, waga i czas trwania naruszenia, cel przetwarzania, liczba poszkodowanych osób, których dane dotyczą, oraz rozmiar poniesionej przez nie szkody,**
- **umyślny lub nieumyślny charakter naruszenia,**
- **recydywa, tj. wszelkie wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego,**
- **działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,**
- **stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków,**
- **sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie.**

Jeśli podmiot dołoży wszelkich starań, aby szkoda była jak najmniejsza, szybko usunie naruszenie, ograniczy jego skutki, zgłosi je do organu nadzorczego w wymaganym czasie i będzie współpracował podczas wyjaśniania naruszenia, a naruszenie było nieumyślne, to można spodziewać się niewielkiej kary, a może nawet organ uzna, że było to „niewielkie naruszenie", o którym mowa w motywie 148 RODO, i zastosuje jedynie upomnienie.

Przepis art. 58 ust. 2 RODO jest poświęcony uprawnieniom organu nadzorczego. Niektóre z nich można uznać za swojego rodzaju kary. Przykładowo organ ma prawo wprowadzić czasowe lub całkowite ograniczenie przetwarzania, w tym zakaz przetwarzania, lub nakazać zawieszenie przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej. W przypadku niektórych rodzajów działalności (bankowość, ubezpieczenia) nałożenie takich ograniczeń będzie oznaczało faktyczne zatrzymanie funkcjonowania organizacji.

Ustawa o ochronie danych osobowych także wprowadza przepisy karne. Przepis art. 107 ust. 1 określa:

**Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.**

Ustawodawca przewiduje surowsze kary za przetwarzanie danych szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO. Zgodnie z art. 107 ust. 2 ustawy o ochronie danych osobowych:

**Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.**

Karane jest także utrudnianie kontroli. Stosownie do art. 108 ust. 1 ustawy o ochronie danych osobowych:

**Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.**

W powyższym przepisie użyto wyrazów „udaremnia" i „utrudnia", co oznacza odpowiednio całkowite uniemożliwienie wykonania kontroli oraz doprowadzenie do tego, że kontrola napotka takie przeszkody, że jej cel nie zostanie osiągnięty. Występek ten popełni właściciel firmy, który np. wyda służbom ochrony polecenie, żeby nie wpuszczać inspektorów na teren zakładu. W tym zapisie zawiera się także nierealizowanie żądań, o których mowa w:

- **art. 84 ust. 1 ustawy – niewpuszczenie na teren firmy, odmowa udzielenia wyjaśnień, niedopuszczenie do oględzin urządzeń, nośników itp.,**
- **art. 84 ust. 2 ustawy – niezapewnienie warunków i środków do sprawnego przeprowadzenia kontroli.**

Na pewno utrudnianiem nie będzie sytuacja, w której inspektorzy nie zostaną dopuszczeni do wykonania kontroli, ponieważ nie okazali legitymacji i upoważnienia, które zobowiązani są okazać (art. 81 ust. 1 ustawy). Za utrudnianie nie powinno uznawać się również sytuacji, gdy przedsiębiorca nie dopuści do kontroli osoby, w stosunku do której nie udało się zweryfikować, czy rzeczywiście jest tą, za którą się podaje, i jest upoważniona przez Prezesa UODO do przeprowadzenia kontroli[30].

Zachowania utrudniające lub uniemożliwiające Prezesowi UODO określenie wysokości kary, np. unikanie dostarczenia informacji o przychodach, zagrożone są taką samą karą jak udaremnianie czy uniemożliwianie kontroli (art. 108 ust. 2 ustawy):

**Tej samej karze podlega kto, w związku z toczącym się postępowaniem w sprawie nałożenia administracyjnej kary pieniężnej, nie dostarcza danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarcza dane, które uniemożliwiają ustalenie podstawy wymiaru administracyjnej kary pieniężnej.".**

Ustawa o ochronie danych osobowych penalizuje niestawienie się na żądanie organu lub bezzasadną odmowę złożenia zeznania, wydania opinii, okazania przedmiotu oględzin albo udziału w innej czynności urzędowej w związku z postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych (art. 69 ust. 1). Co ciekawe, kara grzywny może zostać nałożona „także w przypadku, gdy strona odmówiła przedstawienia tłumaczenia na język polski dokumentacji sporządzonej w języku obcym" (art. 69 ust. 3), którego organ ma prawo żądać na podstawie art. 63 ustawy.

Ciekawostką jest, że w ramach dostosowywania przepisów do RODO wprowadzono kary za zmuszanie szantażem do uiszczenia pewnej kwoty w zamian za niezłożenie zawiadomienia do Prezesa UODO czy prokuratury, że przedsiębiorca nie jest zgodny z przepisami (art. 115 § 12 Kodeksu karnego).

Na koniec warto zauważyć, że w Prawie telekomunikacyjnym znajdziemy dodatkowe kary pieniężne – przykładowo za brak odpowiednich zabezpieczeń, brak rejestru naruszeń czy niewypełnianie obowiązków informacyjnych wobec Prezesa UODO bądź abonentów. Kara może wynieść do 3% przychodu z poprzedniego roku kalendarzowego. Obowiązek jej wprowadzenia wynikał z art. 4 ust. 4 oraz art. 15a ust. 1 dyrektywy 2002/58/WE.

[30] Zob. https://uodo.gov.pl/pl/138/465 (dostęp: 17.04.2019 r.).

WIĘCEJ

# Zakończenie

Poradnik miał za zadanie dostarczenie Państwu podstawowej wiedzy z zakresu przepisów o ochronie danych osobowych. Odpowiada m.in. na pytanie, jak przetwarzać dane osobowe oraz jak je zabezpieczać, aby być w zgodzie z obowiązującym prawem. Materiał uzupełniłem o praktyczne rady, wskazujące najważniejsze aspekty stosowania RODO i ustawy o ochronie danych osobowych. Wierzę, że była to dla Państwa cenna lektura.

## Chcesz wiedzieć więcej?

### Strefa RODO
Najważniejsze zmiany i nowości
**ODO24.pl/RODO**

### RODO nawigator
Tekst i praktyczne odesłania
**ODO24.pl/RODO-Nawigator**

### Pomoc ODO 24
Bezpłatne porady
**ODO24.pl/Pomoc**

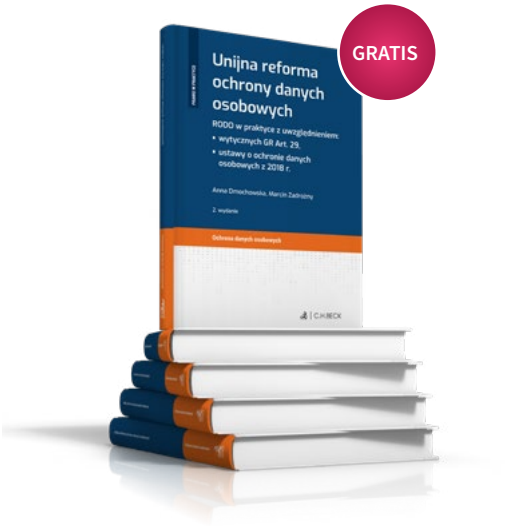
### Biuletyn informacyjny
Tylko to, co najważniejsze
**ODO24./Biuletyn**

**POLECAMY**

# Ochrona danych osobowych
## praktyczny przewodnik dla przedsiębiorców

Dzięki lekturze tej książki przedsiębiorca będzie doskonale wiedział, jakie obowiązki na nim ciążą oraz co musi zrobić, aby być w zgodzie z przepisami. Materiał w niej zawarty adresowany jest przede wszystkim do przedsiębiorców, ale także wszystkich innych osób, które decydują o zbieraniu, przetwarzaniu i zabezpieczaniu danych osobowych.

**Książkę otrzymacie Państwo GRATIS na naszych szkoleniach otwartych:**
**Akredytowany kurs IOD, Monitorowanie zgodności, DPIA i analiza ryzyka.**




### Publikacja zawiera:

- **opis najczęściej spotykanych danych osobowych, zwykłych i wrażliwych, wraz z objaśnieniem i przykładami, kiedy określone informacje stanowią dane osobowe, a kiedy nie,**
- **prawie 70 obrazów ilustrujących praktyczne aspekty stosowania RODO (np. konfiguracja wideo-kamerek, oznaczenia obszarów przetwarzania, dokumenty zniszczone prawidłowo i nieprawidłowo),**
- **przykłady prawidłowych i nieprawidłowych klauzul zgody wraz z ich omówieniem,**
- **przykłady zapisów umowy powierzenia,**
- **opisy rzeczywistych sytuacji zarówno prawidłowych, jak i niezgodnych z RODO,**
- **bardzo dokładne wyjaśnienie aspektów szacowania ryzyka i oceny skutków dla ochrony danych,**
- **omówienie uznanych międzynarodowych standardów (norm) ISO w stosowaniu RODO,**

Wyjątkową częścią publikacji jest opis przetwarzania danych osobowych w poszczególnych działach firmy, takich jak np. dział personalny, obsługa klienta, call center, księgowość, sprzedaż itd. Autor pracuje w międzynarodowej grupie kapitałowej i z tego powodu opis stosowania RODO w tego rodzaju grupach stanowi dodatkową wartość.

### Największe atuty publikacji to:

- **przystępny język – pozwala zrozumieć wymagania RODO i innych przepisów osobom bez prawniczego wykształcenia,**
- **przekrojowość – książka opisuje wszystkie kluczowe wymagania RODO,**
- **autor – doświadczony praktyk, który ma na co dzień styczność z praktycznym stosowaniem RODO,**
- **zastosowanie porównań i metafor – ułatwiają one zrozumienie niektórych wyjątkowo trudnych zagadnień,**
- **przykłady, zdjęcia, tabele i schematy – obrazują poruszane zagadnienia, jak też pokazują absurdy lub nieprawidłowe stosowanie przepisów.**

## *Autor*

**Leszek Kępa** – ekspert bezpieczeństwa informacji, autor kilku książek i wielu publikacji na temat ochrony danych osobowych i bezpieczeństwa informacji. Posiada, uznane na całym świecie, certyfikaty CISA (Certified Information Security Auditor), CISM (Certified Information Security Manager) oraz CEH (Certified Ethical Hacker). Jest członkiem ISACA. Absolwent Szkoły Głównej Handlowej, Politechniki Częstochowskiej oraz Akademii Podlaskiej.

# Ochrona Danych Osobowych

**BEZPIECZEŃSTWO INFORMACJI**

## Audyt zgodności

Wykonujemy pełny audyt zgodności z RODO. Badamy zarówno bezpieczeństwo urządzeń, systemów, sieci i aplikacji, jak i poprawność klauzul, regulaminów oraz rejestrów. Doradzamy, jak praktycznie wdrożyć nasze zalecenia.

## DPIA i analiza ryzyka

Analizę ryzyka i DPIA rozumiemy jako fundament RODO – sposób na racjonalizację kosztów ochrony danych oraz troskę o prywatność osób, których dane Państwo przetwarzają.

## Wdrożenie RODO

Wypełniamy „neutralne" technologicznie RODO. Pomagamy dostosować: procesy biznesowe (np. marketing, rekrutacja), środowisko teleinformatyczne, dokumentację ochrony danych.

## Przejęcie funkcji IOD

Pełniąc funkcję IOD, wspomagamy i nadzorujemy organizację w utrzymaniu zgodności z RODO. Działamy szybko i efektywnie dzięki doświadczonym ekspertom z obszaru prawa, IT oraz zarządzania ryzykiem.

## Bieżące wsparcie

Dzięki dostarczanym przez nas narzędziom oraz wiedzy jesteśmy w stanie przyczynić się do monitorowania i rozwoju funkcjonującego u Państwa systemu ochrony danych osobowych.

## Szkolenia otwarte

Dzielimy się wiedzą, pomagamy w zdobyciu umiejętności i wyposażamy w narzędzia, które umożliwią Państwu skuteczne wykonywanie obowiązków związanych z ochroną danych osobowych.

## Szkolenia zamknięte

Dostosowujemy je do potrzeb organizacji oraz specyfiki branży, w której działa. Stawiamy na praktykę – Państwa pracownicy nauczą się wykorzystywać wiedzę o RODO w swojej codziennej pracy.

## E-learning

Nasza platforma pozwala w krótkim czasie (nawet w największej organizacji) przeszkolić personel oraz zweryfikować nabytą wiedzę. Minimalizujemy w ten sposób najczęstszą przyczynę incydentów – nieświadomość pracowników.

## Narzędzia

Dostarczamy rozwiązania pozwalające kontrolować przepływ danych w organizacji, w tym prowadzić niezbędne rejestry oraz zarządzać szkoleniami, incydentami, upoważnieniami etc.

## Usługi powiązane

Pomoc w razie kontroli UODO, wsparcie we wdrożeniu systemu ISO 27001, ISO 20000, ISO 22301, a także dyrektywy NIS (tzw. cyberustawy).

# Jedna specjalizacja

## SZEROKA PERSPEKTYWA

- Przepisy prawa
- Bezpieczeństwo sieci i systemów IT
- Zarządzanie ryzykiem
- Bezpieczeństwo fizyczne
- Wiedza i świadomość personelu

**ODO24.pl**
tel. 22 740 99 00