RODO

W

ORGANIZACJI

Poradnik praktyczny

Autor: **Mateusz Siek**

e-mail: **kontakt@bims.home.pl**

strona internetowa: **bims.info**

Warszawa, grudzień 2018 r.

Szanowni Państwo!

Po dwóch latach okresu przewidzianego na niezbędne działania wdrożeniowe, 25 maja 2018 roku zaczęło obowiązywać rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679, popularnie zwane RODO. Wraz z tą datą wiązano sporo nadziei na lepszą ochroną danych osobowych, a jednocześnie obawiano się kłopotów ze sprostaniem nowym przepisom unijnym – opisywanym wręcz jako drakońskie. Natomiast mało kto spodziewał się, że przez pierwsze pół roku stosowania RODO, najczęściej będziemy mówili o absurdach i szaleństwach towarzyszących jego wdrażaniu.

Ponieważ ochronę danych osobowych określoną w RODO oparto na analizowaniu ryzyka naruszenia praw i wolności osób, których dane dotyczą oraz neutralności technologicznej, rozporządzenie nie daje gotowych rozwiązań, a jedynie wskazuje metodologię właściwego postępowania. Sposób dostosowania organizacji do tych założeń pozostawiono w gestii każdego administratora danych osobowych. Właśnie ta swoboda w doborze metod i środków jest przyczyną tak dużej różnorodności interpretacyjnej jego zapisów.

Jednym z kluczowych elementów sprzyjających właściwemu wdrożeniu RODO w organizacji jest zapewnienie jego znajomości przez wszystkie osoby uczestniczące w procesach przetwarzania danych osobowych. W tym celu powstał niniejszy Poradnik, którego główną ideą jest przedstawienia praktycznych aspektów stosowania omawianego rozporządzenia.

Zapraszam do lektury wszystkie osoby przetwarzające dane osobowe.

Mateusz Siek

Spis treści

1. Definicje

Definicje funkcjonujące w obszarze ochrony danych osobowych zostały zawarte w art. 4 RODO[1]. Poniżej przytoczono jedynie najważniejsze spośród nich, wraz z komentarzem. Niezależnie od tego, w razie wątpliwości związanych z terminologią, jaka może pojawić się w tematyce danych osobowych, szczegółowych wyjaśnień należy szukać w ww. przepisie oraz motywach RODO.

1.1 RODO

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

RODO jest europejskim aktem prawnym, stosowanym bezpośrednio w państwach członkowskich, tzn. że nie wymaga implementacji w polskim systemie prawnym. Określono w nim zasady przetwarzania danych osobowych, którymi należy się kierować we wszystkich procesach związanych z przetwarzaniem takich danych. Ponadto w hierarchii aktów prawnych RODO ma pierwszeństwo przed przepisami krajowymi (ustawy, rozporządzenia itd.). Oznacza to, że w przypadku kiedy polskie przepisy stałyby w sprzeczności z postanowieniami RODO, to właśnie jego zapisy należałoby stosować.

1.2 Dane osobowe

Zgodnie z art. 4 pkt 1 RODO *„»dane osobowe« oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;*”.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

W myśl powyższej definicji o danych osobowych będziemy mówili w przypadku osób, które są zidentyfikowane (wiemy kogo dane dotyczą) lub kiedy łatwo możemy taką osobę zidentyfikować.

Przykład
Stwierdzenie, że „osoba mieszka w Warszawie i ma zielone oczy" nie zawiera danych osobowych, bo nie wiemy, kogo ten opis dotyczy – wielu mieszkańców Warszawy ma zielone oczy.
Natomiast mówiąc, że „Mateusz Siek mieszka w Warszawie i ma zielone oczy" posługujemy się danymi osobowymi: imię, nazwisko, miejsce zamieszkania, kolor oczu, ponieważ wiemy o kim konkretnie mówimy.

O danych osobowym będziemy mówili również w przypadku osoby, którą możemy zidentyfikować pośrednio – podejmując dodatkowe czynności pozwalające ustalić kogo dane dotyczą.

Przykład
„Najmłodszy pracownik naszej firmy należy do związku zawodowego". Choć wprost nie wskazano kto należy do związku zawodowego (dane wrażliwe), to bez problemu możemy ustalić, kto w naszej firmie jest najmłodszy – tym samym, posługując się określeniem „najmłodszy pracownik naszej firmy", pozwalamy na jego pośrednie zidentyfikowanie. Zdanie to będzie zawierało dane osobowe.

Wśród danych osobowych wyróżniamy tzw. **szczególne kategorie danych osobowych (dane wrażliwe)**. Zgodnie z zapisami RODO, dane takie powinny podlegać szczególnej ochronie, ponieważ ujawniają czynniki określające osobę, które mogą być wykorzystywane w sposób dla niej niekorzystny, w tym dyskryminujący. Katalog takich danych został określony w art. 9 RODO i jest to katalog zamknięty, czyli tylko kategorie danych w nim wymienione są uważane za dane wrażliwe. Są to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej oraz dane dotyczących zdrowia, seksualności lub orientacji seksualnej.

Natomiast informacje dotyczące osób zmarłych, fikcyjnych lub prawnych (np. spółki prawa handlowego i ich organy) nie są objęte ochroną przewidzianą w RODO.

1.3 Przetwarzanie

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 myśl powyższej definicji, czynnością przetwarzania będzie praktycznie wszystko, co robimy z danymi osobowymi. Należy zwrócić uwagę na fakt, że również samo przechowywanie danych osobowych jest traktowane jako ich przetwarzanie. Podobnie niszczenie/ usuwanie danych osobowych jest czynnością przetwarzania.

Przykład
W jednej z szaf trzymane są dokumenty zawierające dane osobowe z zakończonego już projektu, które zgodnie z umowami należy jeszcze przez 5 lat przechowywać. Niezależnie od tego, że materiały te nie są już wykorzystywane i faktycznie nikt na nich nie pracuje, to w świetle przepisów RODO cały czas dane te są przetwarzane u administratora – przechowywane.

1.4 Administrator danych osobowych (ADO)

Zgodnie z 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".*

Kluczową cechą wyróżniającą administratora jest możliwość ustalania celów i sposobów przetwarzania danych osobowych. Podmiot, który decyduje o tym, po co zbiera dane osobowe i jak to robi, będzie traktowany jako administrator danych osobowych.

Przykład
Administratorem danych osobowych jest:
- w spółce prawa handlowego - spółka,
- w podmiocie publicznym (np. Ministerstwie Zdrowia) - podmiot publiczny (np. Ministerstwo Zdrowia), chyba że przepisy wskazują dla danego zadania innego administratora, (np. Ministra Zdrowia).
- w jednoosobowej działalności gospodarczej - przedsiębiorca prowadzący tę działalność.

Administrowanie danymi osobowymi wiąże się z licznymi obowiązkami wskazanymi w RODO, a szczegółowo omówionymi w dalszej części Poradnika.

1.5 Podmiot przetwarzający

Zgodnie z art. 4 pkt 8 RODO *„»podmiot przetwarzający« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;”.*

W przypadku kiedy jakiś podmiot realizuje zadanie związane z przetwarzaniem danych osobowych na polecenie innego podmiotu, będzie występował w roli podmiotu przetwarzającego. Nie decyduje o celach i sposobach przetwarzania, ponieważ te są ustalane przez zleceniodawcę (administratora danych). Brak kompetencji w tym zakresie przesądza o byciu podmiotem przetwarzającym. W takim przypadku mówimy o powierzeniu przetwarzania danych osobowych.

Przykład

- Outsourcing usług informatycznych – następuje powierzenie przetwarzania danych osobowych, do których firma informatyczna uzyska dostęp u administratora, w związku z realizacją zleconych zadań.
- Jeżeli w grupie kapitałowej w ramach spółki-matki prowadzone są sprawy kadrowo-płacowe pracowników wszystkich spółek należących do grupy, to spółka-matka będzie podmiotem przetwarzającym w odniesieniu do danych osobowych pracowników pozostałych spółek (z wyjątkiem własnych pracowników, których jest pracodawcą i tym samym administratorem ich danych).
- Prowadzenie księgowości poza strukturą przedsiębiorstwa – powierzenie przetwarzania danych osobowych pracowników i kontrahentów firmie prowadzącej księgowość.

Powierzenie przetwarzania danych osobowych następuje na podstawie umowy (więcej w pkt 5.1.5 Poradnika)

Nie zawsze jednak realizując zadania na zlecenie innego podmiotu będzie dochodziło do powierzenia przetwarzania danych osobowych. Jeżeli podmiot realizujący zadanie będzie przetwarzał dane we własnym imieniu – np. w związku z obowiązkiem prawnym – wtedy będzie ich administratorem.

Przykład

Podmiot leczniczy, który na zlecenie firmy X realizuje usługi medycyny pracy dla pracowników tej firmy będzie administratorem danych osobowych swoich pacjentów (pracowników firmy X) ponieważ przepisy prawa obligują właśnie podmiot leczniczy, a nie pracodawcę, do prowadzenia dokumentacji medycznej.

1.6 Współadministrowanie

Zgodnie z art. 26 ust. 1 RODO „*Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. (…)*”.

Taka sytuacja będzie miała miejsce w przypadku, kiedy więcej niż jednemu podmiotowi przysługują uprawnienia przypisane administratorowi (decydowanie o celach i sposobach przetwarzania danych osobowych) oraz nałożone są na niego obowiązki administratora.

Przykład
- Dwie firmy organizują konkurs na najlepszą pracę naukową – wspólnie ustalają regulamin konkursu, w tym zasady przetwarzania danych osobowych uczestników konkursu (przyjmowanie zgłoszeń, publikacja wyników).
- Spółki celowe w grupie kapitałowej, powołane do realizacja określonego zadania wiążącego się w przetwarzaniem danych osobowych.
- Grupa kapitałowa, której spółki współdzielą bazę CRM.

W przypadku kiedy dochodzi do współadministrowania danymi osobowymi, współadministratorzy są zobowiązani do ustalenia zakresów swojej odpowiedzialności wynikającej z RODO – np. w ramach umowy o współadministrowaniu (więcej w pkt 5.1.6 Poradnika). Ponadto o swoich ustaleniach powinni poinformować osoby, których dane są przetwarzane.

1.7 Przedsiębiorca

Zgodnie z art. 4 pkt 18 RODO *„»przedsiębiorca« oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;”.*

Tym samym, w myśl RODO przedsiębiorca prowadzący jednoosobową działalność gospodarczą traktowany jest jako osoba fizyczna. Oznacza to, że jego dane osobowe podlegają takiej samej ochronie jak dane osobowe wszystkich innych osób fizycznych. Zgodnie z przepisami prawa, w firmie (nazwie) takiej działalności gospodarczej należy umieścić imię i nazwisko przedsiębiorcy – stąd już sama nazwa jednoosobowej działalności gospodarczej objęta jest ochroną przewidzianą w RODO. Będzie to często dotyczyło również adresu siedziby, który bardzo często jest tożsamy z adresem zamieszkania przedsiębiorcy.

Wskazane zasady nie dotyczą jednak osób prawnych oraz ich organów.

Przykład
- „Bezpieczeństwo Informacji Mateusz Siek” – firma objęta ochroną opisaną w RODO.
- „Bezpieczeństwo Informacji Mateusz Siek Sp. z o.o.” – osoba prawna, której danych nie chroni RODO.

Bez znaczenia pozostaje fakt, że dane przedsiębiorców są dostępne publicznie w rejestrze przedsiębiorców CEiDG.

Ww. zasady dotyczą również spółek cywilnych, w których wspólnicy są osobami fizycznymi.

1.8 Inspektor ochrony danych (IOD)

Zgodnie z art. 37 RODO administrator i podmiot przetwarzający może – a w niektórych przypadkach musi – wyznaczyć Inspektora ochrony danych. Obowiązek dotyczy wszystkich podmiotów publicznych oraz tych, których główna działalność polega na monitorowaniu osób na dużą skalę lub przetwarzaniu na dużą skalę danych wrażliwych/ danych o wyrokach skazujących i czynach zabronionych.

Inspektor ochrony danych przede wszystkim ma za zadanie:

- informować i doradzać w zakresie przestrzegania przepisów o ochronie danych osobowych,
- monitorować przestrzeganie przepisów i regulacji wewnętrznych, m.in. poprzez szkolenia i audyty,
- udzielać zaleceń co do oceny skutków,
- pełnić funkcję punktu kontaktowego, zarówno dla osób, których dane są przetwarzane, jak i organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych).

Jak widać, na powyższym wyliczeniu znajdują się zadania o charakterze konsultacyjnym i doradczym. Inspektor nie przejmuje od administratora odpowiedzialności za ochronę danych osobowych, będzie jednak istotnym elementem systemu ochrony danych osobowych. Jednocześnie należy pamiętać o szczególnym usytuowaniu Inspektora w organizacji – podlega on bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego oraz musi być włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

1.9 Naruszenie ochrony danych osobowych

Zgodnie z art. 4 pkt 12 RODO *„»naruszenie ochrony danych osobowych« oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych*”.

Powyższą definicję można sprowadzić do naruszenia jednego z 3 podstawowych atrybutów informacji, tzw. triady CIA (od angielskiego rozwinięcia skrótu):

Poufność (Confidentiality), czyli właściwość polegająca na nieujawnianiu/ nieudostępnianiu danych osobom lub podmiotom nieuprawnionym.

Integralność (Integrity), czyli właściwość wykluczająca wprowadzenia zmian w sposób nieuprawniony – dane są aktualne, prawdziwe i dokładne.

Dostępność (Availability), czyli właściwość polegająca na zapewnieniu dostępu do danych osobie uprawnionej, zawsze gdy tego potrzebuje.

Przykład

- Dochodzi do włamania na serwer firmy X, skutkiem czego włamywacze uzyskują dostęp do danych klientów firmy – naruszenie poufności.
- Na listach obecności umieszcza się adnotację o przyczynie absencji, co jednocześnie ujawnia informację o stanie zdrowie (np. zwolnienie lekarskie) – naruszenie poufności.
- Osoba podająca się za X, żąda od firmy Y dostępu do danych. Pracownicy nie weryfikują tożsamości osoby żądającej i w efekcie ujawniają dane osobie podszywającej się pod X – naruszenie poufności.
- Firma X aktualizuje informacje o klientach w bazie elektronicznej lub rejestrach papierowych – nie zawsze w obu. W efekcie informacje o danym kliencie mogą się różnić między sobą, w zależności od sprawdzanego rejestru, a żaden rejestr nie będzie posiadał w 100% aktualnych danych – naruszenia integralności.
- W wyniku błędu systemu kadrowego, daty urodzenia wszystkich pracowników zostają zmienione o miesiąc – naruszenie integralności.
- Komputery firmy X zostają zainfekowane oprogramowaniem ransomware. Ponieważ nie robiono kopii zapasowych, wszystkie dane zostają nieodwracalnie utracone – naruszenie dostępności.
- Jedyne egzemplarze dokumentów z danymi osobowymi zostają omyłkowo zniszczone, np. zgłoszenia konkursowe – naruszenie dostępności.
- W wyniku ataku DDoS dochodzi do czasowego braku dostępu do danych na serwerze firmy X – naruszenie dostępności.

W przypadku wystąpienia naruszenia ochrony danych osobowych należy dokonać oceny prawdopodobieństwa naruszenia praw i wolności osób fizycznych. M.in. od tego będzie zależało, czy administrator będzie zobowiązany do zawiadomienia o naruszeniu Prezesa Urzędu Ochrony Danych Osobowych lub osób, których dane dotyczą (więcej w pkt 5.1.8 Poradnika).

2. Zasady przetwarzania danych osobowych

W art. 5 RODO opisano generalne zasady dotyczące przetwarzania danych osobowych. W ramach każdego procesu przetwarzania danych, należy postępować zawsze zgodnie z poniższymi zasadami.

2.1. Zgodność z prawem, rzetelność i przejrzystość

Zgodnie z art. 5 ust. 1 lit. a RODO „*Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą*.”.

W myśl tej zasady przetwarzanie danych osobowych dopuszczalne jest wyłącznie w przypadkach opisanych w art. 6 RODO (warunki dopuszczające przetwarzanie danych zwykłych), art. 9 RODO (warunki dopuszczające przetwarzanie danych wrażliwych) oraz art. 10 RODO (warunki dopuszczające przetwarzanie danych dotyczących wyroków skazujących i czynów zabronionych) (więcej w pkt 3 Poradnika). Tym samym aby móc przestrzegać tej zasady, należy dokonywać jedynie takiego przetwarzania, które znajduje swoją podstawę w ww. przepisach.

2.2. Ograniczenie celu

Zgodnie z art. 5 ust. 1 lit. b RODO „*Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami*.”.

Powyższe oznacza, że aby przetwarzanie danych odbywało się zgodnie z RODO, musi odbywać się w konkretnym celu. Administrator musi mieć sprecyzowany cel przetwarzania i jest nim ograniczony. Niedopuszczalne będzie zbieranie danych osobowych „*na wszelki wypadek*”, „*bo mogą się kiedyś przydać*” itp. Również niezgodne z RODO będzie wykorzystywanie danych osobowych w innych celach niż zostały pozyskane.

Przykład
Firma X prowadzi rekrutację do pracy na stanowisko *eksperta ds. ważnych*. Do pracy na tym stanowisku zgłaszają się kandydaci. W międzyczasie firma X rozpoczyna rekrutację na drugie stanowisko, *specjalisty ds. konserwacji powierzchni płaskich*. Ponieważ niewielu kandydatów zgłosiło się do pracy na stanowisku specjalisty, firma X uwzględnia w rekrutacji również wszystkich kandydatów na stanowisko eksperta.
Ponieważ firma X pozyskiwała dane osobowe kandydatów w celu rekrutacji na konkretne stanowisko, powyższym działaniem naruszyła zasadę „ograniczenia celu".

2.3. Minimalizacja danych

Zgodnie z art. 5 ust. 1 lit. c RODO „*Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane*.".

Jest to szczególnie istotna zasada przetwarzania danych osobowych – wyrażona również w innych przepisach RODO, np. we wcześniej wspominanych art. 6 i 9.

Zgodnie z tą zasadą administrator nie może przetwarzać żadnych danych osobowych, które nie są niezbędne do realizacji danego celu/ zadania/ projektu. Fakt, że jakieś informacje mogą ułatwić realizację zadania nie będzie uzasadniał przetwarzania danych nadmiarowych. Również ewentualność potrzeby przetwarzania określonych danych w przyszłości będzie niewystarczająca.

Przykłady
- Organizator konkursu internetowego żąda od uczestników podania adresu zamieszkania, na który wysłana zostanie nagroda. Uczestników jest 100, a nagroda zostanie przyznana tylko jednej osobie. Tym samym pozyskiwanie danych adresowych wszystkich osób jest nadmiarowe. Organizator powinien uzyskać jedynie adres laureata, po rozstrzygnięciu konkursu.
- Pracodawca odnotowuje w dokumentacji pracowniczej, czy dany pracownik pali papierosy. Są to dane osobowe, do przetwarzania których pracodawca nie został uprawniony w Kodeksie pracy ani innych przepisach, a opisana okoliczność nie ma związku z organizacją pracy i obowiązkami pracodawcy. Pozyskiwanie takich danych jest niezgodne z zasadą minimalizacji danych.

W doktrynie wskazuje się, że również przetwarzanie danych osobowych na podstawie zgody osoby, której dane dotyczą, swoim zakresem może obejmować tylko niezbędne dane.

2.4. Prawidłowość

Zgodnie z art. 5 ust. 1 lit. d RODO „*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.*”.

W myśl tej zasady administrator odpowiada za to, czy przetwarzane przez niego dane osobowe są prawidłowe. Aby realizować tę zasadę powinien dbać o to, aby dane były aktualizowane, np. udostępniając możliwość ich aktualizacji i przypominać o tym.

Przykład
Podczas każdej rejestracji do lekarza w przychodni, rejestratorzy pytają klientów, czy dane kontaktowe są aktualne.

2.5. Ograniczenie przechowywania

Zgodnie z art. 5 ust. 1 lit. e RODO „*Dane osobowe 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.*”.

Powyższe oznacza, że administrator nie może przetwarzać danych osobowych dłużej niż jest to niezbędne do realizacji celu w jakim zostały zebrane. W momencie kiedy dany projekt/ zadanie/ cel dobiega końca, dane osobowe przetwarzane w związku z jego realizacją powinny być usunięte/ anonimizowane (więcej w pkt 5.2.1 Poradnika). Wyjątek będzie stanowiło dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

W przypadku podmiotów podlegających przepisom o archiwizacji, dane mogą być przetwarzane dalej, w celu archiwizacji, w okresie wynikającym z tych przepisów.

Przykład
Firma X po zakończeniu rekrutacji przechowuje w swojej dokumentacji CV kandydatów do pracy. Jednak ponieważ ustał cel przetwarzania (zakończono rekrutację), dalsze ich przechowywanie jest niezgodne z zasadą ograniczenia przechowywania – dane powinny być niezwłocznie usunięte.

2.6. Integralność i poufność

Zgodnie z art. 5 ust. 1 lit. f RODO „*Dane osobowe muszą być przetwarzane w sposób zapewniający 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*.”.

Jest to generalna zasada określającego obowiązek nałożony na administratorów oraz podmioty przetwarzające, aby dane osobowe były należycie zabezpieczone. Należy zapewnić ich poufność, integralność oraz dostępność – atrybuty informacji świadczące o jej bezpieczeństwie.

Poufność oznacza, że dane nie będą udostępniane osobom nieuprawnionym (np. ochrona przed tzw. wyciekami danych).

Integralność oznacza, że dane nie będą modyfikowane w sposób nieuprawniony (np. fałszowanie daty urodzenia w celu uzyskania dostępu do treści/ usług).

Dostępność oznacza, że dane będą dostępne w całym przewidywanym okresie przetwarzania (np. nie zostaną zniszczone w sposób niezamierzony).

2.7. Rozliczalność

Zgodnie z art. 5 ust. 2 RODO „*Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie*.”.

Powyższy zapis jest kluczowy w aspekcie prowadzenia dokumentacji ochrony danych osobowych (więcej w pkt 5 Poradnika). W świetle tej zasady, to na administratorze ciąży obowiązek udowodnienia, że przestrzega przepisy RODO. Musi być w stanie wykazać (np. w razie kontroli lub audytu), że wypełnia wszystkie nałożone na niego obowiązki.

Przykład
Choć przepisy RODO nie nakazują aby przekazanie klauzuli informacyjnej było potwierdzane podpisem osoby, której dane dotyczą, to administratorzy często proszą o to, właśnie ze względu na zasadę rozliczalności.

Mając powyższe na uwadze, uzasadnione jest m.in. udzielanie upoważnień do przetwarzania danych osobowych w formie pisemnej, prowadzenie rejestrów upoważnień oraz w uzasadnionych przypadkach wdrożenie Polityki bezpieczeństwa, z którą zapoznają się pracownicy administratora/ podmiotu przetwarzającego.

3. Podstawy przetwarzania

Aby przetwarzanie danych osobowych było zgodne z prawem, musi być spełniony co najmniej jeden z warunków określonych w art. 6 ust. 1 RODO – dla zwykłych kategorii danych osobowych (więcej w pkt 3.1 Poradnika) lub jeden z warunków określonych w art. 9 ust. 2 RODO – dla szczególnych kategorii danych osobowych (więcej w pkt 3.2 Poradnika). Ponadto, jeżeli przetwarzanie dotyczy danych o wyrokach skazujących lub czynach zabronionych należy przestrzegać zasad opisanych w art. 10 RODO (więcej w pkt 3.3 Poradnika).

Jeżeli żaden ze wskazanych warunków nie znajduje zastosowania w danej sytuacji, to przetwarzanie danych osobowych jest niedopuszczalne.

Właściwe określenie podstawy przetwarzania jest szczególnie ważne dla ustalenia jakie prawa przysługują osobie, której dane dotyczą oraz dla rzetelnego spełnienia obowiązku informacyjnego (przygotowania poprawnej klauzuli informacyjnej).

3.1. Dane zwykłe

W art. 6 ust. 1 RODO wskazano 6 warunków, na podstawie których przetwarzanie danych osobowych jest legalne. Wszystkie te warunki są sobie równe – żaden nie jest lepszy/ właściwszy od pozostałych, a kolejność ich wyliczenia nie ma znaczenia.

Możliwe jest, że w danym celu przetwarzania będzie miał zastosowanie więcej niż jeden warunek. Należy jednak pamiętać, że nie wszystkie mogą być ze sobą łączone. Na przykład, jeżeli przetwarzamy dane osobowe na podstawie przepisów prawa, to nie powinniśmy przyjmować w tym samym celu zgody na przetwarzanie.

3.1.1. Zgoda

Zgodnie z art. 6 ust. 1 lit. a RODO „*Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów*.”

Warunki wyrażenia zgody określono szczegółowo w art. 7 RODO. W myśl tych przepisów zgoda musi być dobrowolna. Jest to podstawowa cecha, której brak będzie

jednocześnie oznaczał, że zgoda jest nieważna w świetle przepisów prawa. Omawiana dobrowolność najczęściej może być kwestionowana w trzech przypadkach:

- W relacji pracodawca – pracownik. Brak równowagi stron powoduje ryzyko, że zgoda może być pośrednio wymuszona.
- W relacji podmiot publiczny (administracja publiczna) – klient (obywatel). Tu również mówimy o braku równowagi stron. Ponadto podmioty publiczne powinny działać w granicach i na podstawie przepisów prawa, czyli właściwsze będą dla nich inne podstawy przetwarzania.
- W przypadku kiedy od wyrażenia zgody na przetwarzanie danych osobowych uzależnia się wykonanie usługi.

Co istotne, zgodnie z przepisami RODO, zgodna na przetwarzanie danych osobowych (z wyłączeniem danych wrażliwych) nie musi być wyrażona na piśmie – może być wyrażona poprzez inne wyraźne działanie.

Przykład
Kandydat do pracy w firmie X, poza danymi osobowymi, które mogą być wymagane w celu zawarcia umowy na podstawie Kodeksu pracy, przesyła również dobrowolnie inne dane, np. swoje zdjęcie. Oczywistym jest, że przesyłając te dane, robi to aby firma X – potencjalny pracodawca – przetwarzał je w procesie rekrutacji. Zgoda jest wyrażana poprzez jego wyraźne działanie jakim jest przesłanie tych danych w ramach oferty pracy.

Niezależnie od powyższego, jeżeli zgoda jest wyrażana na piśmie (np. w ramach gotowego formularza) powinna być wyrażana odrębnie od wszelkich innych zgód, czy oświadczeń składanych przez daną osobę. Ponadto osoba, która wyraża zgodę powinna zostać poinformowana o prawie do wycofania zgody w dowolnym momencie oraz o tym, że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Prawa, których realizacji może żądać osoba, której dane są przetwarzane na podstawie zgody:

- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do ograniczenia przetwarzania danych,
- Prawo do usunięcia danych,
- Prawo do przeniesienia danych,
- Prawo do cofnięcia zgody w dowolnym momencie,
- Prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu,
- Prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO).

Żądanie będzie realizowane w przypadkach i na zasadach określonych w RODO (więcej w pkt 4.2 Poradnika).

3.1.2. Umowa

Zgodnie z art. 6 ust. 1 lit. b RODO „*Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – 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 podstawie tego warunku legalne będzie przetwarzanie danych osobowych niezbędnych zarówno do wykonania umowy, jak i przetwarzanych w związku z dążeniem do zawarcia umowy.

Przykład
Dane osobowe w ofercie pracy – kandydat dąży do zawarcia umowy (np. o pracę, zlecenia), której ma być stroną. Na tej podstawie firma prowadzącą rekrutacje może przetwarzać dane osobowe kandydatów. Jednak z uwagi na fakt, że dotyczy to tylko danych niezbędnych do zawarcia umowy, ich zakres będzie ograniczony do kategorii danych wskazanych w Kodeksie pracy. Odnośnie innych kategorii danych, właściwą przesłanką najczęściej będzie zgoda

Wskazując ten warunek należy pamiętać, że będzie on podstawą przetwarzania danych osobowych jedynie osób będących stroną umowy.

Jednocześnie niewłaściwym będzie wskazywanie w umowie, że strona wyraża zgodę na przetwarzanie danych osobowych (niezbędnych do zawarcia umowy), ponieważ przetwarzanie legalizuje już sam fakt dążenia do jej zawarcia i wykonywania.

Prawa, których realizacji może żądać osoba, której dane są przetwarzane na podstawie umowy:

- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do ograniczenia przetwarzania danych,
- Prawo do usunięcia danych,
- Prawo do przeniesienia danych,
- Prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu,
- Prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO).

Żądanie będzie realizowane w przypadkach i na zasadach określonych w RODO (więcej w pkt 4.2 Poradnika).

3.1.3. Obowiązek prawny

Zgodnie z art. 6 ust. 1 lit. c RODO „*Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze*.”.

Wskazany warunek będzie właściwą podstawą przetwarzania w przypadku, kiedy przepis prawa (rangi ustawowej[2]) zobowiązuje administratora do przetwarzania danych osobowych. W przepisie takim musi być wskazany cel przetwarzania.

Ponadto w doktrynie zwraca się uwagę na fakt, że przepisy muszą zobowiązywać administratora do przetwarzania danych osobowych, a nie jedynie dawać mu taką możliwość.

Przykład
Zgodnie z art. 24 ust. 1 ustawy z dnia 6 listopada 2008 r. *o prawach pacjenta i Rzeczniku Praw Pacjenta* na podmiot udzielający świadczeń zdrowotnych nałożono obowiązek prowadzenia dokumentacji medycznej. W art. 25 ust. 1 ww. ustawy wskazano, że dokumentacja medyczna zawiera co najmniej oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości: nazwisko i imię (imiona), datę urodzenia, oznaczenie płci, adres miejsca zamieszkania, numer PESEL (…).

Prawa, których realizacji może żądać osoba, której dane są przetwarzane na podstawie obowiązku prawnego:

- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do ograniczenia przetwarzania danych,
- Prawo do usunięcia danych (w bardzo ograniczonych przypadkach),
- Prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu,
- Prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO).

Żądanie będzie realizowane w przypadkach i na zasadach określonych w RODO (więcej w pkt 4.2 Poradnika).

3.1.4. Żywotne interesy

Zgodnie z art. 6 ust. 1 lit. d RODO „*Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – przetwarzanie jest*

[2] W doktrynie funkcjonuje opinia, zgodnie z którą wśród podstaw prawnych przetwarzania danych osobowych dopuszczalne jest również wskazywanie rozporządzeń, z uwagi na ich delegację ustawową.

niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.”.

Jest to warunek, który co do zasady powinien znajdować zastosowanie wyłącznie w sytuacjach, kiedy nie można dokonywać przetwarzania na innej podstawie. W tym kontekście wskazuje się m.in. konieczność monitorowania epidemii, klęski żywiołowe, katastrofy spowodowane przez człowieka, zagrożenie życia.

Praktycznie będzie on miał bardzo rzadkie zastosowanie.

Prawa, których realizacji może żądać osoba, której dane są przetwarzane na podstawie ochrony żywotnych interesów:

- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do ograniczenia przetwarzania danych,
- Prawo do usunięcia danych,
- Prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu,
- Prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO).

Żądanie będzie realizowane w przypadkach i na zasadach określonych w RODO (więcej w pkt 4.2 Poradnika).

3.1.5. Interes publiczny/ władza publiczna

Zgodnie z art. 6 ust. 1 lit. e RODO „*Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.”.*

Jest to warunek bardzo zbliżony do „obowiązku prawnego” opisanego w pkt 3.1.3 Poradnika. Tu również należy odwołać się do przepisu prawa, który nakłada na administratora zadanie realizowane w interesie publicznym lub przyznaje mu władzę publiczną. Administrator może przetwarzać dane osobowe niezbędne do realizacji danego zadania określonego w przepisach prawa. W tym przypadku przepis wskazuje cel przetwarzania, jednak nie musi precyzyjnie wskazywać danych osobowych służących do realizacji tego celu. Ponadto na administratora nie jest nakładany obowiązek przetwarzania danych, a raczej określane jest zadanie wiążące się z przetwarzaniem danych osobowych.

Warunek ten często będzie właściwy dla realizacji zadań przez podmioty publiczne.

Przykład
Dane osobowe przetwarzane w ramach prowadzenia konsultacji społecznych będą przetwarzane na podstawie przyznanej władzy publicznej, m.in. w związku z ustawą z dnia 24 kwietnia 2003 roku *o działalności pożytku publicznego i o wolontariacie* oraz ustawami samorządowymi.

Z uwagi na brak w przepisach prawa precyzyjnego określenia zakresu danych osobowych przetwarzanych na tej podstawie, osobie, której dane dotyczą będzie dodatkowo przysługiwało prawo wniesienia sprzeciwu wobec przetwarzania (więcej w pkt 4.2 Poradnika).

Prawa, których realizacji może żądać osoba, której dane są przetwarzane na podstawie interesu publicznego/ władzy publicznej:

- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do ograniczenia przetwarzania danych,
- Prawo do usunięcia danych (w bardzo ograniczonych przypadkach),
- Prawo do wyrażenia sprzeciwu wobec przetwarzania,
- Prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu,
- Prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO).

Żądanie będzie realizowane w przypadkach i na zasadach określonych w RODO (więcej w pkt 4.2 Poradnika).

3.1.6. Prawnie uzasadniony interes administratora

Zgodnie z art. 6 ust. 1 lit. f RODO „*Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – 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*.”.

W istocie powyższy warunek może być rozumiany bardzo szeroko, bowiem w ten sposób administrator danych może uzasadniać wszelkie czynności przetwarzania, które sprzyjają jego interesom. Powoływanie się na tę podstawę będzie

jednak skuteczne jedynie do czasu wyrażenia przez osobę, której dane dotyczą sprzeciwu (więcej w pkt 4.2 Poradnika).

W myśl przepisów RODO organy publiczne, w ramach realizacji swoich zadań nie mogą powoływać się na tę podstawę. Jest to konsekwencja zasady, zgodnie z którą organy publiczne działają w granicach i na podstawie prawa, a ograniczenie prawa do prywatności obywatela może wynikać jedynie z ustawy (przyjmuje się w praktyce, że również z rozporządzenia z delegacji ustawowej). Kwestią dyskusyjną jest określenie rzeczywistego zakresu zadań organów publicznych. Dominujący głos w tej sprawie przemawia za możliwością wskazywania przez podmioty publiczne tego warunku w zakresie, w jakim nie mają przypisanych zadań (w sferze dominium) czyli np. dochodzenia roszczeń.

Przykład

- Firma X/ podmiot publiczny przetwarza dane osobowe w celu dochodzenia swoich roszczeń – wytoczenia powództwa o zapłatę.
- Firma X przetwarza dane osobowe w celach marketingu bezpośredniego (z zastrzeżeniem, że działania te muszą być w zgodzie z m.in. przepisami ustawy z 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną).

Z uwagi na brak w przepisach prawa precyzyjnego określenie granic przetwarzania danych osobowych przetwarzanych na tej podstawie osobie, której dane dotyczą będzie dodatkowo przysługiwało prawo wniesienia sprzeciwu wobec przetwarzania (więcej w pkt 4.2 Poradnika). Dodatkowo w przepisach zastrzeżono, że sprzeciw w przypadku przetwarzania danych w celach marketingowych będzie skuteczny niezależnie od okoliczności.

Prawa, których realizacji może żądać osoba, której dane są przetwarzane na podstawie uzasadnionego interesu:

- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do ograniczenia przetwarzania danych,
- Prawo do usunięcia danych,
- Prawo do wyrażenia sprzeciwu wobec przetwarzania,
- Prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu,
- Prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO).

Żądanie będzie realizowane w przypadkach i na zasadach określonych w RODO (więcej w pkt 4.2 Poradnika).

3.2. Szczególne kategorie danych osobowych

Zgodnie z art. 9 RODO przetwarzanie szczególnych kategorii danych będzie dopuszczalne wyłącznie w przypadku spełnienia jednego z warunków wymienionych w tym przepisie. Przesłanki wskazane w art. 9 ust. 2 RODO nie są tożsame z przesłankami z art. 6 RODO – są dostosowane do katalogu danych wrażliwych, nie mają tak generalnego charakteru, jak warunki z art. 6 RODO.

Co do zasady przetwarzanie danych wrażliwych będzie czynnością ekstraordynaryjną i powinno wiązać się ze szczególnym sposobem postępowania. Takie dane powinny być zabezpieczone specjalnymi środkami bezpieczeństwa. Należy również każdorazowo zweryfikować, czy przetwarzanie jest uzasadnione przesłanką z art. 9 RODO. W razie jakichkolwiek wątpliwości, zasadnym będzie kontakt z osobą zajmującą się ochroną danych osobowych w organizacji.

3.3. Dane o wyrokach skazujących i czynach zabronionych

Zgodnie z art. 10 RODO „*Przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.*”.

Przepis ten wskazuje szczególne środki postępowania w przypadku danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych. Co do zasady, ta kategoria danych osobowych została wyłączona z katalogu danych wrażliwych, jednak powyższy przepis świadczy o tym, że prawodawca przewidział dla niej specjalny sposób postępowania przy przetwarzaniu.

Swoiste ograniczenie możliwości przetwarzania tego rodzaju danych osobowych wskazuje na ich szczególne znaczenie, a planowane przetwarzanie powinno być poprzedzone konsultacją z osobą odpowiedzialną za ochronę danych osobowych w organizacji.

4. Prawa osób, których dane dotyczą

W stosunku do poprzedniego stanu prawnego, RODO znacząco poszerzyło katalog uprawnień jakie przysługują osobie, której dane dotyczą. Administrator musi umożliwić każdej osobie skuteczną realizację przysługujących jej praw. Należy jednak zaznaczyć, że o tym czy dane uprawnienie będzie faktycznie przysługiwało osobie, której dane dotyczą decydują okoliczności przetwarzania – m.in. podstawa przetwarzania z art. 6 lub 9 RODO.

Uprawnienia opisane w Rozdziale III RODO można podzielić na dwie kategorie: prawo, które administrator powinien realizować z własnej inicjatywy (więcej w pkt 4.1 Poradnika) oraz uprawnienia, które są realizowane na żądanie osoby, której dane dotyczą (więcej w pkt 4.2 Poradnika).

4.1. Obowiązek informacyjny

W związku z przetwarzaniem danych osobowych, na administratora został nałożony obowiązek informacyjny. Jest on realizowany poprzez udostępnianie osobom, których dane dotyczą tzw. **klauzul informacyjnych**, czyli pakietów informacji dotyczących przetwarzania ich danych osobowych.

Umożliwienie zapoznania się ze wspomnianymi klauzulami informacyjnymi powinno być realizowane niezależnie od żądania osoby której dane dotyczą. Natomiast fakt zapoznania się z taką klauzulą nie musi być potwierdzony podpisem, choć ze względu na zasadę rozliczalności często jest to praktykowane (alternatywną formą może być określenie zasad spełniania obowiązku informacyjnego w wewnętrznych procedurach i ewentualne dowodzenie tego poprzez rzeczywiste przykłady).

Przykład

- Przed połączeniem z infolinią banku, rozmówcy mają możliwość zapoznania się z klauzulą informacyjną wybierając tonowo odpowiedni numer.
- Klauzula informacyjna dotycząca monitoringu umieszczana jest w widocznym miejscu, dostępnym dla osób wchodzących w obszar monitorowany.
- Elementem formularza poprzez, który zbierane są dane osobowe jest klauzula informacyjna.

Obowiązek informacyjny może wynikać z dwóch przepisów RODO:
Art. 13 – w przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą albo

Art. 14 – w przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą.

Klauzula informacyjna musi zawierać szereg elementów:

- Wskazanie administratora danych osobowych (oraz dane kontaktowe).
- Dane kontaktowe do Inspektora ochrony danych (jeżeli został wyznaczony).
- Cel i podstawę prawną przetwarzania danych (podstawy prawne zostały omówione w pkt 3 Poradnika).
- Prawnie uzasadniony interes administratora (o ile podstawą przetwarzania jest art. 6 ust. 1 lit. f RODO).
- Informacje o odbiorcach danych.
- Informację o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej (gdy ma to zastosowanie).
- Okres przez, który dane będą przetwarzane.
- Informację o przysługujących prawach (zakres praw powinien być dostosowany do podstawy przetwarzania – więcej w pkt 3 Poradnika).
- Informację o prawie do cofnięcia zgody (jeżeli ma zastosowanie).
- Informację o prawie wniesienia skargi do organy nadzorczego.
- Wskazanie, czy podanie danych osobowych jest wymogiem ustawowym, umownym itp. oraz jakie będą konsekwencje niepodania danych osobowych.
- Informację o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu.
- Ponadto jeżeli dane zostały pozyskane z innego źródła niż od osoby, której te dane dotyczą (art. 14 RODO), należy wskazać to źródło.

Niewłaściwe jest jednak stosowanie tzw. uniwersalnych klauzul informacyjnych, z których odbiorca nie może wywnioskować które konkretnie elementy dotyczą jego przypadku.

Wzór takiej klauzuli informacyjnej może być określony w Polityce bezpieczeństwa danej organizacji, co stanowi dobrą praktykę ułatwiającą przygotowywanie klauzul informacyjnych oraz sprzyja realizacji zasady rozliczalności.

Klauzula informacyjna powinna być przekazana/ udostępniona osobie, której dane dotyczą podczas zbierania od niej danych osobowych. Jeżeli jest to niemożliwe, to właściwym momentem będzie pierwszy kontakt z daną osobą – z zaznaczeniem, że w większości przypadków nawiązywanie kontaktu jedynie w celu przekazania klauzuli informacyjnej będzie działaniem nadmiarowym. W takim przypadku klauzulę informacyjną przekazujemy niejako przy okazji innych działań.

Ponadto należy pamiętać, że administrator ma obowiązek przekazać klauzulę informacyjną danej osobie tylko raz. Przy kolejnych kontaktach przyjmuje się, że osoba której dane dotyczą posiada już informacje wskazane w art. 13 lub 14 (chyba, że uległy one zmianie).

Niekiedy administrator będzie zwolniony z obowiązku informacyjnego. Okoliczności, kiedy klauzuli informacyjnej nie trzeba przekazywać zostały określone zarówno w RODO, jak i w ustawie odo[3]. Z uwagi na szczególne znaczenie obowiązku informacyjnego, wszelkie wyłączenia jego stosowania powinny być konsultowane z osobą odpowiedzialną za ochronę danych osobowych w organizacji, a w razie wątpliwości klauzulę należy przekazać.

Przekazanie klauzuli informacyjnej jest szczególnie ważne ponieważ wskazuje osobie, której dane dotyczą, wszelkie informacje odnośnie przetwarzania jej danych osobowych, w tym również odnośnie przysługujących jej praw. Ma ono również istotny wymiar praktyczny dla administratora danych – jest to komunikat do klienta, o tym, że organizacja funkcjonuje zgodnie z przepisami RODO, a dane osobowe przez nią przetwarzane są bezpieczne.

4.2. Pozostałe uprawnienia

Poza wspomnianym w pkt 4.1 obowiązkiem informacyjnym, osobom, których dane dotyczą będą przysługiwały również pewne uprawnienia realizowane na żądanie:

- Prawo dostępu do danych,
- Prawo sprostowania danych,
- Prawo ograniczenia przetwarzania danych,
- Prawo usunięcia danych (tzw. prawo bycia zapomnianym),
- Prawo przeniesienia danych,
- Prawo wyrażenia sprzeciwu wobec przetwarzania – z powodu szczególnej sytuacji,
- Prawo do cofnięcia w dowolnym momencie zgody na przetwarzanie (o ile dotyczy),
- Prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu,
- Prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (wcześniej GIODO).

Kwestią niezwykle ważną jest, aby realizując takie żądanie mieć pewność, że wniosła je osoba, której dane dotyczą. Sytuacja, kiedy którekolwiek w ww. uprawnień byłoby realizowane na żądanie osoby trzeciej stanowiłaby niezgodność z prawem, a w większości przypadków – naruszenie ochrony danych osobowych. Podstawowym obowiązkiem ADO (oraz jego pracowników) jest poprzedzenie realizacji ww. praw poprzez potwierdzenie tożsamości osoby wnoszącej żądanie ich realizacji.

[3] Ustawa z 10 maja 2018 roku o ochronie danych osobowych.

Nie w każdy przypadku jednak wszystkie ww. uprawnienia będą przysługiwały. Jest to przede wszystkim uzależnione od podstawy przetwarzania danych osobowych, a tym samym zindywidualizowane względem każdej czynności przetwarzania. O przysługujących prawach należy poinformować osobę, której dane dotyczą w ramach klauzuli informacyjnej – z zastrzeżeniem, że informacja ta musi być dopasowana do danego przypadku.

Kolejnym aspektem związanym z prawami osób, których dane dotyczą są wyłączenia ich stosowania. Przepisy RODO (art. 15-22) określają zasady realizacji ww. praw, okoliczności kiedy prawa przysługują oraz w jakich sytuacjach administrator jest zwolniony z ich wykonywania. Niezależnie od decyzji o realizacji prawa albo stwierdzenia, że uprawnienie nie przysługuje lub nie może być zrealizowane osobie, która zwraca się do administratora z żądaniem realizacji któregoś z uprawnień opisanych w Rozdziale III RODO, administrator musi udzielić odpowiedzi.

Należy również pamiętać, że w przypadku kiedy administrator w wyniku analizy prawnej danej sytuacji dochodzi do wniosku, że żądanego uprawnienia nie będzie realizował (zgodnie z przepisami RODO lub ustawy odo), warto aby skonsultował to z osobą odpowiedzialną za ochronę danych osobowych w organizacji.

Realizacja omawianych uprawnień jest nieodpłatna.

Dla lepszej przejrzystości funkcjonowania, kwestie związane z prawami osób, których dane dotyczą powinny być uregulowane w Polityce bezpieczeństwa obowiązującej w organizacji.

5. Obowiązki ADO

Obowiązki administratora danych można podzielić funkcjonalnie na dwie grupy: prowadzenie niezbędnej dokumentacji (więcej w pkt 5.1 Podręcznika) oraz stosowanie faktycznych środków zapewniających bezpieczeństwo danych osobowych (więcej w pkt 5.2 Podręcznika). Natomiast sposoby realizacji tych obowiązków zależą od administratora. Co prawda przepisy RODO wskazują pewne niezbędne elementy dokumentacji, które muszą się w niej pojawić, jednak o jej całokształcie decyduje administrator. Podobnie w przypadku środków bezpieczeństwa, RODO wskazuje jedynie sugerowane metody. To administrator musi – kierując się stanem wiedzy technicznej, kosztami wdrożenia, analizą ryzyka naruszenia praw i wolności oraz uwzględniając charakter, zakres, cele i kontekst przetwarzania – dokonać wyboru, jakie metody ochrony danych osobowych będą najwłaściwsze.

5.1. Dokumentacja

Prowadzenie odpowiedniej dokumentacji ochrony danych osobowych, będzie jednocześnie określało kwestie organizacyjne związane z bezpieczeństwem danych. Właściwe sporządzenie dokumentacji oraz jej faktyczne wdrożenie pozwoli administratorowi zachować kontrolę nad systemem przetwarzania danych osobowych. Ponadto odpowiednie prowadzenia niezbędnej dokumentacji jest wymagane konkretnymi przepisami RODO oraz jest powiązane z zasadą rozliczalności opisaną w pkt 2.7 Poradnika.

5.1.1 Polityka bezpieczeństwa

Zgodnie z art. 24 ust. 2 RODO „*Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych*.”.

Do 24 maja 2018 r. każdy administrator danych musiał prowadzić *Politykę bezpieczeństwa* oraz *Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,* a rozporządzenie wykonawcze do ustawy odo określało niezbędne elementy jakie te dokumenty muszą zawierać. Obecnie, zgodnie z RODO, prowadzenie polityki ochrony danych jest zależne od uznania administratora danych. Mały przedsiębiorca może odstąpić od tworzenia tego rodzaju dokumentów, natomiast większe organizacje będą zapewne posiadały taką politykę, a prawdopodobnie również inne dokumenty – precyzujące zasady ochrony informacji.

Polityka, w praktyce powinna określać podstawowe kwestie związane z realizacją obowiązków wynikających z RODO, a często będzie również określała generalne metody ochrony informacji – nie tylko danych osobowych.

Niezasadnym jest natomiast powtarzanie w polityce zapisów ustaw lub RODO, które są obowiązujące, niezależnie od powielania ich w wewnętrznej dokumentacji. Cenne będzie natomiast opisanie, jak te zapisy są realizowane w organizacji.

Polityka zazwyczaj zawiera informacje o podziale obowiązków w podmiocie, określa kwestie organizacyjne, wskazuje sposoby postępowania, w tym szczególnie w przypadku incydentów/ naruszeń, zasad realizacji praw osób, których dane dotyczą oraz wzory dokumentacji obowiązującej w organizacji

5.1.2 Rejestr czynności przetwarzania

Zgodnie z art. 30 ust. 1 RODO „*Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają.*”.

Dodatkowo przepisy określają minimalny zakres elementów, które muszą być uwzględnione w takim rejestrze (dla każdej czynności przetwarzania). Są to następujące informacje:

- cele przetwarzania;
- opis kategorii osób, których dane dotyczą;
- opis kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
- przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- planowane terminy usunięcia poszczególnych kategorii danych.

Powyższe elementy powinny być określone niezależnie dla każdej czynności przetwarzania.

Przykład

Czynność przetwarzania	Rekrutacja pracowników
Cel przetwarzania	Przyjmowanie ofert pracy, ocena kandydatów, wyłonienie najlepszej oferty i zawarcie umowy
Kategorie osób, których dane dotyczą	Kandydaci do pracy
Kategorie danych	Imię i nazwisko, dane adresowe, dane kontaktowe, informacje o wykształceniu i kwalifikacjach, doświadczenie i staż

	pracy, uprawnienia zawodowe oraz inne dane podane dobrowolnie i z inicjatywy kandydata
Odbiorcy danych	Dane nie są udostępniane (ewentualnie „podmioty świadczące obsługę administracyjno-organizacyjną” albo np. „firma świadcząca obsługę IT”)
Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej	Nie dotyczy
Planowany termin usunięcia danych	Niezwłocznie po zakończeniu procesu rekrutacji

W pozycji „*Kategorie danych osobowych*” należy wymienić wszystkie kategorie danych jakie mogą być przetwarzane przez administratora w ramach danego procesu – danej czynności przetwarzania.

W pozycji dotyczącej *odbiorców danych* nie wskazuje się konkretnych osób które będą miały dostęp do danych w ramach upoważnienia udzielonego przez administratora (pracownicy), ale wszystkie podmioty zewnętrzne, którym będą lub mogą być takie dane udostępniane.

Bardzo ważne jest aby Rejestr czynności przetwarzania był prowadzony na bieżąco i aktualizowany w przypadku jakiejkolwiek zmiany lub pojawiania się nowej czynności przetwarzania.

Ponadto w rejestrze należy wskazać:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych oraz
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Praktyka wskazuje, że przy sporządzaniu Rejestr czynności przetwarzania przydatny może być Rejestr zbiorów danych osobowych, jeżeli taki był prowadzony w danym podmiocie.

Rejestr czynności przetwarzania powinien być prowadzony w formie pisemnej – papierowej lub elektronicznej. Ważne jest również, aby pozycje dotyczące środków bezpieczeństwa nie były powszechnie udostępniane.

Prowadzenie Rejestru może być zadaniem Inspektora ochrony danych, o ile został on wyznaczony w podmiocie.

Rejestru natomiast nie muszą prowadzić podmioty zatrudniające mniej niż 250 osób, chyba że czynności przetwarzania, które wykonują:

- mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie mają charakteru sporadycznego,
- obejmują szczególne kategorie danych (wskazane w art. 9 RODO) lub
- dotyczą wyroków skazujących i czynów zabronionych (o czym mowa w art. 10 RODO).

Rejestr czynności przetwarzania jest przydatnym instrumentem mapującym procesy przetwarzania w organizacji, dlatego jego prowadzenia jest zalecane niezależnie od ww. wyjątków.

5.1.3 Rejestr wszystkich kategorii czynności

Zgodnie z art. 30 ust. 2 RODO „*Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, (…).*”.

Dodatkowo przepisy określają minimalny zakres elementów, które muszą być uwzględnione w takim rejestrze (dla każdej czynności przetwarzania). Są to następujące informacje:

- imię i nazwisko lub nazwa oraz dane kontaktowe administratora, w imieniu którego działa podmiot przetwarzający oraz inspektora ochrony danych;
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
- przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Wskazane elementy powinny być opisane niezależnie dla każdej czynności przetwarzania wykonywanej w imieniu administratora.

Przykład

Dane administratora i Inspektora ochrony danych	Administrator Danych S.A. ul. Administratora Danych 1 00-000 Miasto e-mail: ado@ado.pl Inspektor ochrony danych: iod@ado.pl
Kategorie przetwarzań	Obsługa i prowadzenie dokumentacji kadrowej i płacowej

Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej	Nie dotyczy

W pozycji „*Kategorie przetwarzań*” należy wskazać rodzaj usługi realizowanej na zlecenie administratora.

Ponadto w Rejestrze należy wskazać:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych oraz
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

W Rejestrze wszystkich kategorii czynności przetwarzania ewidencjonuje się wszelkie procesy, które zostały powierzone do realizacji przez administratora danych. Tym samym jest to rejestr prowadzony w przypadku, kiedy podmiot funkcjonuje w roli podmiotu przetwarzającego. Czynności opisane w tym rejestrze nie znajdą miejsca w Rejestrze czynności przetwarzania prowadzonym przez ten sam podmiot, ponieważ dotyczą danych osobowych, którymi podmiot ten nie administruje – ma je jedynie powierzone do przetwarzania. Będą natomiast figurowały w Rejestrze czynności przetwarzania prowadzonym przez ich administratora.

Rejestr wszystkich kategorii czynności przetwarzania powinien być prowadzony w formie pisemnej – papierowej lub elektronicznej. Ważne jest również, aby pozycje dotyczące środków bezpieczeństwa nie były powszechnie udostępniane.

Prowadzenie Rejestru może być zadaniem Inspektora ochrony danych, o ile został on wyznaczony w podmiocie.

Rejestru natomiast nie muszą prowadzić podmioty zatrudniające mniej niż 250 osób, chyba, że czynności przetwarzania, które wykonują:

- mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie mają charakteru sporadycznego,
- obejmują szczególne kategorie danych (wskazane w art. 9 RODO) lub
- dotyczą wyroków skazujących i czynów zabronionych (o czym mowa w art. 10 RODO).

Rejestr wszystkich kategorii czynności przetwarzania jest przydatnym instrumentem mapującym procesy przetwarzania w organizacji, dlatego jego prowadzenia jest zalecane niezależnie od ww. wyjątków.

5.1.4 Klauzule informacyjne

Jednym z elementów dokumentacji wymaganej od administratora są klauzule informacyjne. Choć nie stanowią one dokumentów systemu ochrony danych osobowych w podmiocie, to jednak ciężko wyobrazić sobie realizowanie zadań związanych z przetwarzaniem danych osobowych bez stosowania klauzul informacyjnych.

Klauzule informacyjne to pakiety informacji dotyczących przetwarzania danych osobowych, kierowane do osób, których dane dotyczą – w ten sposób realizowany jest obowiązek informacyjny.

Klauzule informacyjne powinny być dostosowane do każdego zadania realizowanego przez administratora, tak aby ich adresat dokładnie wiedział przez kogo, w jakim celu oraz w jaki sposób przetwarzane są jego dane osobowe oraz jakie przysługują mu w związku z tym prawa.

Szczegółowy opis przygotowania i stosowania klauzul informacyjnych został opisany w pkt 4.1 Poradnika.

5.1.5 Umowy powierzenia przetwarzania danych

W procesie administrowania danymi osobowymi może dochodzić do sytuacji kiedy przetwarzanie nie jest realizowane przez administratora. Z uwagi na uwarunkowania organizacyjne może on zlecić jakieś zadanie związane z przetwarzaniem danych osobowych innemu podmiotowi. W takiej sytuacji będziemy mówili o powierzeniu przetwarzania danych osobowych podmiotowi przetwarzającemu (więcej w pkt 1.5 Poradnika). Opisana sytuacja będzie miała miejsce m.in. w przypadku outsourcingu.

Przykład
Firma X zleca firmie Y przygotowanie imiennych zaproszeń na konferencję. Firma Y będzie w tej sytuacji przetwarzała w imieniu i na polecenie Firmy X dane osobowe osób zapraszanych. Aby przetwarzanie tych danych było zgodne z RODO, firmy powinny zawrzeć umowę powierzenia przetwarzania danych osobowych.

W ww. okolicznościach niezbędne jest zawarcie umowy powierzenia przetwarzania danych (może to być również regulowane innym instrumentem prawnym). Zawarcie takiej umowy jest nieodpłatne ponieważ leży w interesie obu stron. Administrator dokumentuje i legalizuje w ten sposób udostępnienie administrowanych przez siebie danych osobowych innemu podmiotowi, a podmiot przetwarzający legalizuje fakt przetwarzania przez siebie wskazanych danych osobowych.

Należy jednak pamiętać, że wskazana relacja będzie miała miejsce jedynie w przypadku kiedy podmiot przetwarzający dokonuje przetwarzania danych osobowych w imieniu administratora. W konsekwencji może to dotyczyć również sytuacji kiedy sam administrator nie ma rzeczywistego kontaktu z danymi powierzonymi.

Przykład
Firma X lub podmiot publiczny zleca Firmie Y zorganizowanie konferencji naukowej. W tym celu Firma Y rozsyła imienne zaproszenia oraz prowadzi listę obecności na konferencji. Firma X nie jest jednak zainteresowana listą uczestników, a jedynie przekazem medialnym. *De facto* przetwarzania dokonuje się na polecenie Firmy X, jednak Firma X nie będzie miała faktycznego kontaktu z danymi osobowymi uczestników konferencji.

Zgodnie z art. 28 RODO umowy powierzenia przetwarzania danych osobowych powinny regulować cały szereg różnych kwestii organizacyjnych. W tym m.in. zapewnić administratorowi danych możliwość realizacji audytów bezpieczeństwa danych osobowych w podmiocie przetwarzającym, zobowiązanie do współdziałania przy realizacji praw osób, których dane dotyczą, zobowiązanie do zawiadamiania o naruszeniach, oraz określać zakres powierzenia.

W praktyce często stosuje się wzory umów, które mogą stanowić załącznik do Polityki bezpieczeństwa danej organizacji.

Zapisy dotyczące powierzenia przetwarzania danych osobowych mogą stanowić odrębną umowę lub być częścią umowy głównej.

Należy również pamiętać, że powierzenie przetwarzania danych osobowych do podmiotu spoza Europejskiego Obszaru Gospodarczego (kraje UE + Norwegia, Islandia oraz Lichtenstein) jest obwarowane szczególnymi zasadami opisanymi w Rozdziale V RODO.

5.1.6 Umowy o współadministrowaniu

Zgodnie z art. 26 RODO „*(…) W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.*”.

Poza samodzielnym administrowaniem danymi osobowymi lub działaniem na polecenie administratora, w praktyce zdarzają się również projekty, gdzie dwóch lub więcej administratorów danych wspólnie ustala cele i sposoby przetwarzania danych osobowych. W takim przypadku mówimy o współadministrowaniu danymi (więcej w pkt 1.6 Poradnika).

Współadministrowanie danymi osobowymi wymaga określenia podziału odpowiedzialności w zakresie realizacji uprawnień osób, których dane są przetwarzane. Będzie to dotyczyło zarówno realizacji obowiązku informacyjnego, jak i pozostałych praw, opisanych w Rozdziale III RODO (więcej w pkt 4 Poradnika). Współadministratorzy mogą również wyznaczyć wspólny punkt kontaktowy dla osób, których dane są przetwarzane – ma to usprawnić realizację uprawnień, tak aby dwóch lub więcej Inspektorów ochrony danych nie działało niezależnie od siebie.

Ponadto współadministratorzy w ramach tych ustaleń często określają zakres i sposób przepływu danych osobowych pomiędzy sobą oraz stosowane w tym celu środki bezpieczeństwa. W praktyce spotyka się również regulowanie kwestii dotyczących zakresu odpowiedzialności w razie ewentualnych naruszeń.

O zasadniczej treści uzgodnień informowane są osoby, których dane dotyczą – praktycznym rozwiązaniem jest implementowanie tych ustaleń w klauzuli informacyjnej. Natomiast same ustalenia zazwyczaj mają formę odrębnej umowy, porozumienia lub są wplecione w treść innych dokumentów zatwierdzanych przez współadministratorów.

5.1.7 Upoważnienia

Sama idea upoważnień sprowadza się do umocowania danego pracownika do przetwarzania danych osobowych w imieniu administratora lub podmiotu przetwarzającego.

Przepisy RODO nie wskazują wprost obowiązku udzielania upoważnień pracownikom administratora/ podmiotu przetwarzającego, a tym bardziej nie określają formy takiego upoważnienia (pisemna/ elektroniczna/ ustna). Pośrednio obowiązek ten wywodzony jest jednak z art. 28, 29 oraz 32 RODO.

Kwestią otwartą pozostaje forma, choć aby pozostawać w zgodzie z zasadą rozliczalności, należy w jakiś sposób udokumentować tę czynność – najprostszą metodą jest forma pisemna.

W praktyce znane są również metody udzielania upoważnień do przetwarzania danych osobowych w zakresach obowiązków. W takim przypadku zakres upoważnienia można bezpośrednio odnieść do zakresu zadań.

Ponadto literalne rozumienie RODO zobowiązuje do „polecenia" przetwarzania. W doktrynie wskazuje się dwie możliwości: polecenie wyrażone wprost albo wynikające z umowy o pracę/ zlecenia. Wydaje się, że pewniejszą formą jest jednak dosłowne użycie tego sformułowania w upoważnieniu lub właśnie zakresie zadań.

W upoważnieniu należy również określić zobowiązanie osoby upoważnionej do zachowania tajemnicy oraz pouczenie o odpowiedzialności.

Wzory upoważnień mogą stanowić załącznik do Polityki bezpieczeństwa.

5.1.8 Notyfikacja naruszeń

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*.".

Oznacza to, że u każdego administratora powinien funkcjonować rejestr naruszeń, w którym będą odnotowywane podstawowe kwestie związane z wystąpieniem ewentualnego naruszenia. Jest to rejestr prowadzony niezależnie od zgłoszeń naruszeń do Prezesa Urzędu Ochrony Danych Osobowych, czy zawiadamiania osób, których dane dotyczą. Więcej o naruszeniu ochrony danych osobowych w pkt 1.9 Poradnika.

W przypadku naruszeń ochrony danych osobowych, które mogą skutkować ryzykiem naruszenia praw lub wolności osób fizycznych – administrator jest zobowiązany bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin od stwierdzenia naruszenia, zgłosić je do Prezesa Urzędu Ochrony Danych Osobowych. PUODO będzie uwzględniał sposób w jaki dowiedział się o naruszeniu przy ewentualnym wydawaniu ostrzeżeń, nakazów, udzielaniu upomnień lub nakładaniu kar pieniężnych. Warto pamiętać, że jeżeli administrator sam nie zgłosi naruszenia, to pozostaje spore prawdopodobieństwo, że zrobi to ktoś inny.

Urząd Ochrony Danych Osobowych przygotował formularz zgłoszenia naruszenia ochrony danych osobowych, którego uzupełnienie zapewnia, że administrator przekazuje wszystkie wymagane informacje. Zgłoszenie powinno być rzetelne i w miarę możliwości wyczerpujące, a sam formularz liczy sobie 6 stron. Aby w terminie 72 godzin przekazać kompletne zgłoszenie – pożądane jest dynamiczne działanie już od momentu stwierdzenia naruszenia.

Ponadto, jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizyczny, to zgodnie z art. 34 RODO, administrator jest zobowiązany do zawiadomienia o nim – bez zbędnej zwłoki – osoby, które dane dotyczą. Od

powyższego obowiązku zostały przewidziane wyjątki, jednak ich zastosowanie należy oceniać indywidualnie dla każdego przypadku i najlepiej w konsultacji z osobą odpowiedzialną za ochronę danych osobowych w organizacji.

5.1.9 Analiza ryzyka i ocena skutków przetwarzania

Z zapisów art. 32 ust. 2 RODO pośrednio wynika zalecenie prowadzenia **analizy ryzyka**. Powinna ona wskazywać, czy stopień bezpieczeństwa danych osobowych jest odpowiedni. W tym celu uwzględnia się w szczególności 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. Taka analiza ryzyka zazwyczaj oparta jest o dane z Rejestru czynności przetwarzania oraz Rejestru wszystkich kategorii czynności. O ile jej prowadzenie jest rekomendowane dla każdej czynności przetwarzania, to w przepisach nie ma szczególnych regulacji wskazujących obowiązek lub zasady jej prowadzenia.

Inaczej przedstawia się kwestia **oceny skutków** przetwarzania. Zgodnie z art. 35 RODO „*Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych*.”.

Przepisy jasno wskazują jakie elementy musi zawierać taka ocena skutków, kiedy i dla jakich czynności przetwarzania należy ją przeprowadzić (katalog określony w przepisach oraz lista czynności wskazana przez organ nadzorczy) oraz jakie dalsze obowiązki może generować. Jeżeli na podstawie przeprowadzonej oceny administrator ustali, że przetwarzanie może powodować wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

Dokonując oceny skutków administrator konsultuje się z inspektorem ochrony danych.

W doktrynie zwraca się jednak uwagę na zapis wskazujący, że oceny należy dokonać przed rozpoczęciem przetwarzania. Uwzględniając jednak zasadę tzw. ochrony opartej na ryzyku zalecane jest uzupełnienie oceny skutków również dla już trwających czynności przetwarzania.

5.2. Środki bezpieczeństwa

Zgodnie z art. 32 ust. 1 RODO „*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 (…).*”.

Z powyższego zapisu jasno wynika, że ochrona danych osobowych zgodna z RODO nie oznacza jedynie prowadzenia stosownej dokumentacji, czy przetwarzania danych w granicach prawa, ale również oznacza konieczność zastosowania odpowiednich zabezpieczeń technicznych i organizacyjnych. Dane osobowe powinny być chronione w sposób praktyczny oraz rzeczywisty.

Przysłowiowe już „*szafy zgodne z RODO*”, w niektórych przypadkach faktycznie mogą okazać się wyposażeniem niezbędnym. Jednocześnie w innych miejscach – pozostają tylko uciążliwym RODO-absurdem.

5.2.1 Anonimizacja/ pseudonimizacja

Jednym ze środków technicznych i organizacyjnych, o których mowa w art. 32 RODO, służących do zapewnienia odpowiedniego poziomu bezpieczeństwa jest **pseudonimizacja**. Jej definicja znajduje się w art. 4 pkt 5 RODO: „»*pseudonimizacja« oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej*”. Innymi słowy, jest to odwracalny proces zastąpienia danych osobowych innymi informacjami – niepozwalającymi na identyfikację danej osoby lub ich nietrwałe usunięcie.

Przykład

- Generowanie numerów wniosków/ zgłoszeń, które są udostępniane jedynie wnioskodawcom. Następnie przy otwartej komunikacji posługiwanie się tymi numerami zamiast danymi osobowymi – lekarz wywołuje pacjentów poprzez numer jaki otrzymują przy rejestracji.
- Dziennikarz opisując jakąś historię zamienia imiona bohaterów (oraz miejsce wydarzeń) – sam natomiast posiada informacje pozwalające powiązać postacie autentyczne, ze zmyślonymi imionami.
- Bank przypisuje klientowi tzw. token, którym klient będzie się posługiwał w kontaktach z bankiem, zamiast swoim imieniem i nazwiskiem.

Pseudonimizacji nie należy mylić z **anonimizacją**. Różnica polega na tym, że proces pseudonimizacji jest odwracalny, a anonimizacja jest nieodwracalna. Usunięcie danych osobowych w ramach anonimizacji będzie jednocześnie oznaczało ich bezpowrotne zniszczenie.

5.2.2 Szyfrowanie i hasła

Wśród środków technicznych i organizacyjnych, o których mowa w art. 32 RODO, służących do zapewnienia odpowiedniego poziomu bezpieczeństwa wskazano m.in. **szyfrowanie**. Metodę tę należy stosować adekwatnie do okoliczności przetwarzania, w tym szczególnie do ryzyka naruszenia ochrony danych osobowych oraz wiążącego się z nim ryzyka naruszenia praw i wolności osoby, której dane dotyczą. Innymi słowy, im większe niebezpieczeństwo niosą czynności przetwarzania oraz im bardziej newralgiczne informacje są przetwarzane, tym bardziej powinno się je zabezpieczać.

Przykład

- Przesyłanie mejli wewnątrz firmy (pomiędzy komputerami podłączonymi do tej samej sieci) zawierających dane osobowe nie musi wiązać się z koniecznością ich szyfrowania.
- Natomiast wysyłanie mejlem dokumentów zawierających dane osobowe do podmiotów zewnętrznych, np. kontrahentów czy księgowości może wymagać zaszyfrowania tych dokumentów.

W tym celu można stosować dostępne na rynku programy szyfrujące lub korzystać z funkcjonalności oprogramowania pocztowego.

Dobrą praktyką jest również szyfrowanie mobilnych nośników danych, które siłą rzeczy są bardziej narażone na kradzież/ zgubienie. Należy jednak pamiętać, że o konieczności szyfrowania nie decyduje sama podatność na naruszenia ochrony danych osobowych, ale również treść danych – np. szczególnym kategoriom danych oraz dużym zbiorom należy zapewnić wyższy poziom bezpieczeństwa niż danym zwykłym lub ich niewielkim zbiorom.

Rekomendowanym działaniem jest również przesyłanie hasła niezależnym kanałem komunikacji, np. zaszyfrowane dane mejlowo, a hasło smsem.

Zasadnym jest także ustanawianie **haseł** dostępu do urządzeń i systemów służących przetwarzaniu danych osobowych. Zgodnie z aktualnymi zaleceniami nie musza to być hasła 8-znakowe zmieniane co miesiąc. Dużo ważniejszą cechą haseł jest ich niepowtarzalność (różne hasła do różnych systemów) oraz ich nietuzinkowość. Niestety badania wskazują, że nadal sporą popularnością cieszy się „Admin1", „123qwe", czy hasła powtarzające login. Koniecznie trzeba też zmieniać hasła

ustanawiane domyślnie lub hasła fabryczne. Bazy takich haseł są dostępne w Internecie.

W przypadku dużej liczby haseł, można korzystać z tzw. menadżerów haseł, czyli programów zapamiętujących je za nas.

5.2.3 Kopie zapasowe

Tworzenie kopii zapasowych jest nie tylko dobrą praktyką, ale wynika również z RODO. Zgodnie z art. 32 RODO „*zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego*" jest jedną z metod zapewnienia odpowiedniego poziomu bezpieczeństwa. W tym celu często wprowadza się zasady tworzenia kopii zapasowych danych przetwarzanych w systemach informatycznych lub odwzorowywania cyfrowego danych przetwarzanych tradycyjnie (papierowo). Tego rodzaju działanie może ustrzec organizację przed krytycznymi konsekwencjami naruszeń ochrony danych osobowych. Ważny elementem tych zasad jest określenie częstotliwości sporządzania kopii zapasowych, miejsca przechowywania kopii oraz osób odpowiedzialnych za to zadanie. Należy podkreślić, że kopie zapasowe powinny być przechowywane w sposób całkowicie odseparowany od głównych nośników informacji, np. niezależny serwer, dysk zewnętrzny, chmura informacyjna.

Przykład

- Firma X dysponuje dwiema niezależnymi serwerowniami, zlokalizowanymi w różnych miejscach. Serwery jednej, służą za miejsce przechowywania kopii zapasowych drugiej.
- Kopie zapasowe są przechowywane w chmurach informacyjnych (pod warunkiem stosownego uregulowania prawnego tej formy oraz zapewnienia przez dostawcę takich usług odpowiednich środków bezpieczeństwa).
- W jednoosobowej działalności gospodarczej, przedsiębiorca przechowuje kopie zapasowe na dedykowanym do tego dysku zewnętrznym.

Systematyka tworzenia kopii zapasowych może być różna, w zależności od organizacji oraz zasobów technicznych i technologicznych. W przypadku podmiotów posiadających własne serwery należy niezależnie określić zasady sporządzania kopii zapasowych dla stacji roboczych (komputerów) oraz dla serwerów.

5.2.4 Polityka czystego biurka/ czystego ekranu oraz kontrola dostępu

Jedną z najprostszych metod podniesienia poziomu bezpieczeństwa danych osobowych przetwarzanych przez pracowników jest wdrożenie **polityki czystego biurka**. Zgodnie z jej zasadami, po zakończeniu pracy wszelkie dokumenty oraz inne nośniki informacji powinny być należyci zabezpieczone przed dostępem osób

nieuprawnionych. Innymi słowy, należy schować je do szafy, biurka lub w inne miejsce ograniczające do nich dostęp. Ponadto, podczas pracy zaleca się aby na stanowisku pracy znajdowały się tylko faktycznie potrzebne dokumenty i materiały. Dzięki tej praktyce, zminimalizowane zostanie ryzyko ich przypadkowego zniszczenia lub ujawnienia.

Często serwis sprzątający wykonuje swoje zadania po godzinach pracy danego podmiotu. Pracownicy serwisu nie są upoważnieniu do przetwarzania danych osobowych (praktyka udzielania im upoważnień jest błędna), dlatego też nie powinni mieć umożliwionego dostępu do takich danych.

Drugą metodą zaczerpniętą z norm jakości ISO, jest **polityka czystego ekranu**. W myśl tej zasady, należy chronić dostęp do systemów informatycznych, w których przetwarzane są dane osobowe, poprzez każdorazowe blokowanie komputera w sytuacji czasowego opuszczenia stanowiska pracy, a w razie zakończenia pracy – wyłączanie komputerów. Ponadto monitory komputerów powinny być ustawione w sposób uniemożliwiający osobom postronnym wgląd do nich. Praktycznym rozwiązaniem jest dodatkowo ustawianie automatycznych wygaszaczy ekranów, blokujących komputer.

Kontrola dostępu jest kolejną metodą pozwalającą zminimalizować ryzyko naruszenia poufności, integralności lub dostępności informacji, a w tym danych osobowych. Jej stosowanie polega na ograniczaniu dostępu do obszarów, w których przetwarza się dane osobowe. Może być to realizowane na różnych poziomach:

- Kontrola dostępu do obiektu – metoda pozwalająca podnieść poziom bezpieczeństwa na najwyższym poziomie ogólności. Polega na tym, że tylko upoważnione osoby mają dostęp do obiektu lub tylko zweryfikowane osoby mogą mieć taki dostęp.

Przykład
- Wejście do firmy (dalej niż recepcja/ punkt ochrony) możliwe jest tylko dla posiadaczy karty dostępu.
- Wejście do urzędu możliwe jest tylko dla osób, które zostaną wpisane do księgi wejść (odnotowana zostanie ich tożsamość).

- Kontrola dostępu do pomieszczeń – metoda, zgodnie z którą tylko upoważnione osoby mogą mieć dostęp do poszczególnych pomieszczeń.

Przykład
Tylko upoważnione osoby (figurujące na liście dostępu, przekazywanej do punktu ochrony/ recepcji) mogą pobierać klucze do pomieszczeń. Dany pracownik, może pobrać klucz tylko do swojego pokoju.

- Wyznaczenie stref bezpieczeństwa – metoda polegająca na określeniu obszarów wewnątrz obiektu, do których dostęp jest ograniczony. W ten sposób można tworzyć również warstwowe uprawnienia dostępu. W praktyce metoda ta jest łączona z kontrolą dostępu do obiektu oraz kontrolą dostępu do wybranych pomieszczeń.

Przykład
W organizacji wyznaczono 3 strefy bezpieczeństwa: Strefa I – dostęp do obiektu i pomieszczeń gospodarczych; Strefa II (indywidualna) – dostęp do pomieszczeń służbowych, określany indywidualnie dla każdego pracownika, Strefa III – dostęp do pomieszczeń szczególnie chronionych (serwerownia, archiwum, laboratorium itp.), również określany indywidualnie dla wybranych pracowników.

Ograniczenie dostępu do obiektu/ strefy/ pomieszczenia może polegać na ograniczeniu uprawnień wstępu (osoby nieuprawnione nigdy nie mogą przebywać w danym obszarze) lub ograniczeniu prawa decydowania o wstępie do obiektu/ strefy/ pomieszczenia (tylko uprawnione osoby mogą otwierać wyznaczone obszary – pobieranie kluczy, posiadanie karty dostępu – natomiast za ich zgodą w obiekcie/ strefie/ pomieszczeniu mogą znajdować się również inne osoby).

5.2.5 Inne środki bezpieczeństwa

Ochrona realizowana przez wyspecjalizowaną firmę – jest to środek bezpieczeństwa zapewniający ogólną ochronę obiektu, a przy tym podnosi również poziom bezpieczeństwa danych osobowych. Może polegać zarówno na ochronie fizycznej – pracownik ochrony dozoruje dany obszar na miejscu, odpowiada za kontrolę dostępu, obchody, interwencje; dozorze zdalnym lub automatycznym – wprowadzenie kart dostępu, instalacja systemu alarmowego, zdalny monitoring.

Monitoring – monitoring jest elementem ochrony (choć może występować również w innych celach, w kontekście przetwarzania danych osobowych). Może on polegać na monitoringu wizyjnym, monitoringu poczty elektronicznej oraz innych formach monitoringu (np. GPS w samochodach służbowych, GPS i bilingi w służbowych telefonach komórkowych, monitorowaniu ruchu w Internecie). Szczegółowe kwestie dotyczące monitoringu zostały opisane w poradniku opracowanym przez Prezesa Urzędu Ochrony Danych Osobowych. Monitoring zazwyczaj będzie wiązał się z przetwarzaniem danych osobowych osób monitorowanych.

Aktualizacje – wszelkie systemy i programy komputerowe powinny być zawsze na bieżąco aktualizowane. Instalowanie aktualizacji jest jednym z fundamentalnych elementów bezpieczeństwa teleinformatycznego. Brak najnowszej aktualizacji w praktyce oznacza duży wzrost podatności na ataki. Dlatego też rekomendowane jest

wymuszenie instalowania aktualizacji oprogramowania na wszystkich stacjach roboczych i serwerze – poprzez rozwiązania systemowe lub organizacyjne.

Należy również pilnować, aby systemy operacyjne zainstalowane na komputerach posiadały wsparcie techniczne (czyli aby dostawca oprogramowania nadal zapewniał opracowywanie i udostępnianie niezbędnych aktualizacji). W przeciwnym razie, system operacyjny należy traktować jako nieaktualny – o zwiększonej podatności na ataki.

Audyty i kontrole – „*regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania*" jest jedną z metod opisanych w art. 32 RODO. Będzie to najczęściej realizowane poprzez audyty wewnętrzne/zewnętrzne. Takie audyty powinny być realizowana systematycznie, tak aby mieć stałą kontrolę nad skutecznością i poprawnością doboru przyjętych technicznych i organizacyjnych środków bezpieczeństwa. Audyty są również jednym z zadań Inspektora ochrony danych.

6. Podsumowanie

Ciężko wskazać najważniejsze zagadnienia z wyżej opisanych tematów, każdy bowiem odnosi się do elementarnych kwestii związanych z ochroną danych osobowych. Żadnego nie można pominąć, czy bagatelizować, a ich znajomość jest obowiązkiem każdego administratora oraz podmiotu przetwarzającego (oraz ich pracowników).

Opisane w Poradniku zagadnienia są jedynie podstawowymi kwestiami związanymi z ochroną danych osobowych – określonymi w RODO. W praktyce administratorzy danych mogą mierzyć się z niezliczonymi, szczególnymi przypadkami, których nie omówiono w ramach tych ogólnych zagadnień. Będzie to np. kwestia bezpieczeństwa teleinformatycznego, monitoringu wizyjnego i innych jego form, przetwarzania transgranicznego, w tym przedstawicielstwa.

Jeżeli w danym podmiocie został wyznaczony Inspektor ochrony danych, będzie on właściwą osoba do precyzowania wszelkich niejasności, informowania o właściwym sposobie stosowania RODO itp. W innym przypadku należy śledzić stronę Urzędu Ochrony Danych Osobowych, na której publikowane są zalecenia i wytyczne lub korzystać z konsultacji z ekspertami zewnętrznymi.