I. Podstawowe pojęcia

Żeby zrozumieć sens ochrony danych osobowych, należy przyswoić podstawowe pojęcia. Wbrew pozorom nie jest to wiedza tylko akademicka. Znajomość definicji ma kluczowe znaczenie dla interpretacji przepisów RODO i krajowych regulacji dotyczących ochrony danych osobowych.

Dane osobowe

To 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 czynnik bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Administrator danych osobowych

Osoba fizyczna lub prawna, organ publiczny, jednostka 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 wyznaczani

WAŻNE

ADO nie jest np. prezes firmy, który podpisuje umowę o pracę. Pracodawca to firma, która działa np. przez swoje organy - zarząd, który reprezentuje dwóch członków zarządu. To, że oni podpisują umowę, wcale nie oznacza, że to te osoby są ADO. Te osoby jedynie działają w imieniu ADO, a ADO jest sama firma.

Operacje przetwarzania

Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, 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.

Przepisy, wytyczne oraz dokumentacja dotyczące ochrony danych osobowych zawierają w odniesieniu do ich przetwarzania różne pojęcia. Analizując tę tematykę, natykamy się na takie terminy, jak „operacje przetwarzania", „czynności przetwarzania" oraz „rodzaj przetwarzania". Te pojęcia warto również usystematyzować, aby uniknąć używania ich jako synonimów, co jest oczywiście błędem.

Zawarty w RODO zbiór definicji nie obejmuje swym zakresem wszystkich pojęć używanych w powyższym akcie prawnym. Jednocześnie, w samym tekście RODO pojęcia te stosowane są naprzemiennie przy różnych przepisach.

PRZYKŁAD

1. Art. 35 ust. 1: „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".
2. Art. 35 ust. 4: „Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych".
3. Art. 35 ust. 6: „Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.

Jakkolwiek przy zapoznawaniu się z przepisami odbiorca często nie zwraca w pierwszej kolejności uwagi na powyższe różnice, to dowolne używanie tych pojęć może prowadzić do nieporozumień. W konsekwencji terminy te wymagają usystematyzowania.

Za punkt wyjścia powinno posłużyć pojęcie „operacji przetwarzania”. Jest ono o tyle istotne, że pojawia się w kontekście definicji samego przetwarzania danych osobowych.

Zgodnie bowiem 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, takie 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.

Z powyższej definicji wynika zatem, że „operacje przetwarzania” to działania wykonywane na danych osobowych, przy których wykonywaniu dochodzi do przetwarzania tych danych. Innymi słowy, są to wszelkie działania na informacjach o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

PRZYKŁAD

Osoba upoważniona przez administratora danych osobowych ma za zadanie prowadzić wysyłkę newslettera do klientów. W tym celu podejmuje ona na co dzień takie operacje przetwarzania jak np.: pozyskiwanie nowych danych osobowych w postaci adresu e-mail, aktualizowanie adresów e-mail zawartych w bazie klientów, dodawanie do bazy klientów nowych adresów e-mail, korzystanie z ww. adresów e-mail w związku z wysyłką newslettera czy też zabezpieczenie adresów e-mail poprzez utworzenie kopii zapasowej. Może być to również zestaw operacji, kiedy np. wpisanie do bazy danych A adresu e-mail nowego klienta wiąże się z automatycznym przesłaniem tych danych do bazy danych B.

Czynności przetwarzania

Z kolei pojęcie „czynności przetwarzania” - w kontekście obowiązku prowadzenia rejestru czynności przetwarzania - zdefiniował Urząd Ochrony Danych Osobowych w swoim opracowaniu. Otóż, w związku z art. 30 ust 1 RODO czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną osobę lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.

WAŻNE

Przy określaniu operacji przetwarzania kluczową rolę odgrywa konkretne działanie, takie jak pozyskiwanie czy też przechowywanie danych osobowych, natomiast określając czynność przetwarzania bierzemy pod uwagę wspólny cel jednej operacji lub większej liczby operacji, taki jak np. prowadzenie dokumentacji pracowniczej.

Przykładowo, gdy zaobserwujemy, że dana osoba np. drukuje bazę danych osobowych, mamy pewność, że dokonuje ona operacji przetwarzania, natomiast nie wiemy, czy wykonuje ona czynność przetwarzania, ponieważ nie znamy ewentualnego celu dokonania takiego wydruku. Przykład nr 3 ma na celu zilustrowanie różnic pomiędzy tymi pojęciami.

PRZYKŁAD

- Administrator danych osobowych wykonuje czynność przetwarzania o nazwie „Rekrutacja pracowników”. Już z samej nazwy tej czynności możemy wywnioskować, że jej celem jest znalezienie spośród dostępnych kandydatów właściwych osób, które mogłyby podjąć pracę u administratora danych osobowych. Na powyższą czynność przetwarzania składa się jednak sporo operacji przetwarzania, takich jak:
- przechowywanie nadesłanych aplikacji na serwerze; zapisanie nadesłanych aplikacji w konkretnej bazie danych;
- uporządkowanie nadesłanych aplikacji wg przyjętych z góry kryteriów;
- kontakt z kandydatami z wykorzystaniem podanych przez nich danych kontaktowych czy też
- usunięcie po jakimś czasie danych osobowych kandydatów nieprzyjętych do pracy.

Większość administratorów danych osobowych ma obowiązek prowadzenia rejestru czynności przetwarzania, a podmiotów przetwarzających - rejestr kategorii czynności przetwarzania. RODO wyłącza jednak obowiązek prowadzenia tych rejestrów przez podmioty zatrudniające **mniej niż 250 osób, pod warunkiem że** przetwarzanie, którego dokonują:

- nie powoduje ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- ma charakter sporadyczny;
- nie obejmuje szczególnych kategorii danych osobowych, tj. danych wrażliwych wymienionych w art. 9 ust. 1 RODO, lub
- nie obejmuje danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO (art. 30 ust. 5 RODO).

Jak sama nazwa wskazuje, administrator **rejestruje czynności przetwarzania, podmiot przetwarzający zaś - kategorie czynności przetwarzania.**

Konieczne jest zatem wyodrębnienie tych pojęć i prawidłowe umieszczenie w rejestrach.

PRZYKŁAD

Przy rekrutacji pracowników jeden cel będzie obejmował wiele cząstkowych operacji niewymagających szczegółowego opisywania w rejestrze, takich jak:

- pozyskiwanie informacji o kandydatach z ofert nadesłanych w wyniku ogłoszenia,
- dokonywanie selekcji tych ofert,
- uzyskiwanie dodatkowych informacji w ramach wywiadów prowadzonych z wybranymi osobami,
- usunięcie danych osób, które nie zostały wskazane do zatrudnienia.

Nie ma w tym przypadku konieczności opisywania osobno każdej z tych operacji wykonywanej na danych w procesie określonym zbiorczo „rekrutacja pracowników", gdyż nie jest to konieczne do scharakteryzowania przetwarzania zgodnie z kryteriami wskazanymi w RODO.

PRZYKŁAD

Analogicznie, przy obsłudze umów sprzedaży jako czynność przetwarzania wpisujemy „obsługa umów sprzedaży", nie dzieląc procesu na inne kategorie, takie jak np. „rejestrowanie danych klienta" czy też „wystawienie faktury".

Przy wyodrębnianiu poszczególnych czynności przetwarzania warto uwzględnić **rzeczywisty podział zadań pomiędzy poszczególne komórki organizacyjne lub osoby w danej jednostce** (np. na dział kadr przechowujący zwolnienia lekarskie i dane dotyczące dzieci pracowników oraz dział księgowy zajmujący się wypłatą wynagrodzeń). Nie ma oczywiście przeszkód, aby w mniejszych podmiotach wyodrębniać jedną kategorię pracowniczą, np. „Prowadzenie ewidencji pracowników i rozliczeń z pracownikami".

WAŻNE

W praktyce przy każdym wpisie w rejestrze czynności przetwarzania na pierwszej pozycji umieszczona była nazwa lub opis czynności przetwarzania, a dopiero następnie pozostałe informacje o danej czynności wymagane przepisami.

Z kolei rozumienie pojęcia **kategorii czynności przetwarzania** będzie szczególnie istotne dla procesorów. Należy je definiować jako **rodzaj usługi** związanej ze zleconymi czynnościami przetwarzania, która jest realizowana przez procesora na zlecenie administratora.

PRZYKŁAD

Przykładowe kategorie czynności przetwarzania:

1) przechowywanie danych klienta (administratora) poprzez udostępnienie mu określonej przestrzeni dyskowej w infrastrukturze przetwarzającego na przechowywanie danych (klient sam zarządza i decyduje o tym, jakie dane tam przechowuje);
2) udostępnienie klientowi (administratorowi) określonej platformy programistycznej (np. serwera WWW wraz z odpowiednim oprogramowaniem do prowadzenia własnej strony internetowej);
3) przechowywanie dokumentacji podatkowej, księgowej, kadrowej i medycznej;
4) prowadzenie dokumentacji podatkowej, księgowej, kadrowej i medycznej.

WAŻNE

W przypadku rejestru kategorii czynności przetwarzania poszczególne wpisy w tym rejestrze powinny być uporządkowane według kategorii przetwarzania

Z kolei w przypadku rejestru kategorii przetwarzania, obok wydzielenia strony z danymi procesora na podobnych zasadach jak opisane wcześniej, warto dla każdego wpisu w rejestrze na pierwszej pozycji umieścić nazwę danej „kategorii czynności przetwarzania" (rodzaj usługi) jako wartości pozwalającej pogrupować wszystkie wpisy.

II. Podstawy przetwarzania danych

Kluczowym problemem dla każdego praco dawcy jest ustalenie, czy w konkretnych okolicznościach można przetwarzać dane osobowe. Tego wymaga reguła legalizmu z art. 5 RODO.

Podstawy przetwarzania danych osobowych zwykłych

Przesłanka 1. ZGODA

Aby zgoda stanowiła legalną przesłankę przetwarzania danych osobowych zwykłych:

- musi być dobrowolna, konkretna, świadoma i jednoznaczna (wyrażenie zgody nie będzie uznawane za udzielone w warunkach dobrowolności, jeśli np. uzależniono od niego wykonanie umowy, w tym świadczenie usługi),
- musi być udzielona w formie oświadczenia, ewentualnie w postaci wyraźnego działania potwierdzającego, z którego wynika, że osoba przyzwala na przetwarzanie dotyczących jej danych osobowych,
- zapytanie o zgodę musi być wyraźnie oddzielone od pozostałych kwestii,
- administrator musi być gotowy do wykazania, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania danych osobowych, spełniającą wskazane kryteria (zasada rozliczalności wskazana w art. 5 RODO).

Przesłanka 2. WYKONANIE UMOWY

Na przesłankę, o której mowa w art. 6 ust. 1 lit. b RODO, można powołać się przede wszystkim, gdy administrator będzie przetwarzał dane osobowe swojego klienta w celu wykonania umowy, którą z nim zawarł.

PRZYKŁAD

Do salonu samochodowego przychodzi potencjalny klient, który chce kupić nowy samochód. W tym celu sprzedawca poprosi go o wiele danych osobowych, który są niezbędne do zrealizowania tej umowy. Sprzedawca powinien jednocześnie spełnić wobec klienta obowiązek informacyjny z art. 13 RODO, wskazując, że celem przetwarzania jego danych osobowych jest zawarcie i zrealizowanie umowy sprzedaży pojazdu, a podstawą prawną zawarta umowa, tj. art. 6 ust. 1b RODO.

Administrator danych będzie działał zgodnie z prawem również w tej sytuacji, kiedy będzie przetwarzał dane osobowe klienta jeszcze przed zawarciem z nim konkretnej umowy, co zostanie zainicjowane przez klienta.

WAŻNE

1. *Podstawa prawna dotyczy osoby, która jest stroną umowy. Nie można zatem jej stosować do innych osób, o których mowa w umowie (w tym przypadku będzie to uzasadniony interes prawny - zobacz w dalszej części publikacji).*
2. *Podstawa prawna dotyczy człowieka. Chodzi o relację pomiędzy administratorem danych osobowych a człowiekiem (B2C). Nie będzie miała zatem zastosowania do relacji przedsiębiorca-przedsiębiorca (B2B).*
3. *Zakres danych może być użyty wyłącznie w celu realizowania umowy, choć w opinii autorów możliwe jest również użycie tego samego zakresu danych w celach marketingowych (w rozumieniu RODO) na podstawie uzasadnionego interesu prawnego. Trzeba jednak o tym poczynić stosowną* wzmiankę w treści klauzuli informacyjnej.

Przesłanka 3. REALIZACJA OBOWIĄZKU PRAWNEGO

Przetwarzanie danych osobowych będzie dopuszczalne, gdy jest niezbędne do wypełniania obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO). Ta podstawa prawna przetwarzania danych osobowych jest najczęściej wykorzystywana przez administratorów danych w sytuacji, gdy powinność przetwarzania danych osobowych wynika bezpośrednio z konkretnego przepisu. Wówczas cel przetwarzania danych i zakres zbieranych danych wynika bezpośrednio z tej podstawy prawnej. Jeżeli nie, administrator danych, zgodnie z zasadą minimalizacji danych, powinien zbierać wyłącznie te dane, które są niezbędne do realizacji celu.

Przesłanka 4. OCHRONA ŻYWOTNEGO INTERESU

Rozważając zastosowanie art. 6 ust. 1 lit. d RODO jako podstawy przetwarzania danych osobowych, należy ocenić, czy rzeczywiście jest to niezbędne do zapewnienia ochrony żywotnych interesów osoby, takich jak życie czy zdrowie. Zgodnie z motywem 46 preambuły RODO powoływanie się na żywotny interes osoby powinno zaistnieć wyłącznie w ostateczności, jeżeli nie jest możliwe zastosowanie innej podstawy prawa. Jak zauważył prawodawca, przesłanką uzasadniającą powołanie się na art. 6 ust. 1 lit. d RODO będą w szczególności względy humanitarne - klęski żywiołowe, katastrofy czy ważne interesy publiczne.

Przesłanka 5. REALIZACJA ZADAŃ PUBLICZNYCH

Zgodnie z art. 6 ust. 1 e RODO przetwarzanie danych osobowych będzie dopuszczalne, jeśli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

WAŻNE

Nie można skorzystać z tej podstawy, jeżeli:

1. *Dotyczy ona możliwości działania poza granicami zakreślonymi przez prawo - zwłaszcza w kontekście tzw. przepisów kompetencyjnych danych organów (zgodnie z przepisami prawa administracyjnego organy administracji publicznej muszą działać na podstawie prawa i w jego granicach).*
2. *Dotyczy przypadków, w których brak wyraźnego przepisu prawa, ale zadanie należy do zakresu zadań publicznych.*
3. *Może dotyczyć również podmiotów sektora prywatnego, jeśli tylko delegowano na nie zrealizowanie zadania publicznego*

Co istotne tę podstawę prawną należy w pewien sposób czytać łącznie z art. 6 ust. 1 lit. c RODO, zgodnie z którym przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze

Wskazaną podstawą prawną może posługiwać się administrator, który:

- wykonuje zadania publiczne (innymi słowy, zadania realizowane w interesie publicznym, np. zadania własne gminy czy powiatu, oraz zadania zlecone przez organy administracji rządowej),
- sprawuje powierzoną władzę publiczną.

Przesłanka 6. UZASADNIONY INTERES

Zgodnie z art. 6 ust. 1 lit. f RODO przetwarzanie danych osobowych będzie dopuszczalne, jeżeli 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.

WAŻNE

Rozwiązanie to nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego (motyw 47 preambuły RODO).
Celem takim będzie działanie firmy, ale w zakresie przedmiotu jej działalności.

PRZYKŁAD.

1. Firma księgowa świadczy usługi księgowe. Może informować swoich klientów w ramach marketingu bezpośredniego (czyli takiego, który ma trafić do konkretnej wyselekcjonowanej osoby, ta z kolei może pozostawać anonimowa) o promocjach, które zamierza wprowadzić, jeśli klient zachęci do skorzystania z usług tej firmy nowego klienta.
2. Firma szkoleniowa Y oferuje usługi szkolenia bhp. W ramach marketingu chce również reklamować w ramach swojego newslettera ofertę szkoleniową RODO, którą będzie realizowała zaprzyjaźniona z nią firma X.
3. Przedsiębiorca Jan Kowalski podpisał umowę na dostarczenie 1 000 000 nakrętek do słoików przedsiębiorcy Kazimierzowi Nowakowi - ich producentowi. W treści tych umów każdy z nich wskazał konkretnie swoich pracowników, którzy mają koordynować ten projekt, podając ich imię, nazwisko, nr telefonu oraz adres @ (dane służbowe). Każdy z przedsiębiorców mógł tak postąpić ze względu na konieczność przeprowadzenia zakontraktowanego zamówienia, a podstawą tego działania jest prawnie uzasadniony interes każdego z nich.
4. Przedsiębiorca Kazimierz Nowak nie zapłacił przedsiębiorcy Janowi Kowalskiemu za dostarczenie 1 000 000 nakrętek. Przedsiębiorca Jan Kowalski może pozwać swojego dłużnika - przedsiębiorcę Kazimierza Nowaka o zapłatę, powoławszy się na swój uzasadniony interes prawny.
5. Zainstalowanie monitoringu wizyjnego w celu zapewnienia bezpieczeństwa osób i mienia w obszarze objętym kamerami CCTV.

WAŻNE

1. *Ponieważ dla organów publicznych podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca, prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.*
2. *Jeśli klient odmówił wyrażenia zgody marketingowej, nie możesz zakładać, że spróbujesz w ramach innej podstawy prawnej, tj. na bazie twojego uzasadnionego interesu. Odmowa udzielenia takiej zgody jest bezwzględnie wiążąca, nawet jeśli wykorzystałeś w tym zakresie podstawę prawną, którą jest zgoda, a nie prawnie uzasadniony interes.*
3. *Jeśli chcesz prowadzić marketing względem np. potencjalnych klientów (z którymi nie miałeś jakiegokolwiek powiązania), to możesz to robić na podstawie ich prawny będzie podstawą dla twojego marketingu, ale tylko względem tych, którzy twoimi klientami są bądź byli zgody, a nie na bazie swojego uzasadnionego interesu prawnego. Uzasadniony interes*

Nie zapominaj, że kanał komunikacji w celu przedstawienia oferty handlowej (co dotyczy oferty marketingowej i promocyjnej) nie bazuje na prawnie uzasadnionym interesie, ale na zgodzie wyrażonej w trybie przepisów prawa telekomunikacyjnego (kanał telefoniczny) lub usług drogą elektroniczną (kanał e-mail).

Podstawy przetwarzania danych osobowych szczególnej kategorii

Katalog szczególnych kategorii danych osobowych został określony w art. 9 RODO i jest zamknięty. Są to dane dotyczące:

- pochodzenia rasowego;
- pochodzenia etnicznego;
- poglądów politycznych;
- przekonań religijnych lub światopoglądowych;
- przynależności do związków zawodowych;
- danych genetycznych;
- danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej;
- danych dotyczących zdrowia;
- seksualności;
- orientacji seksualnej.

W stosunku do tych danych przewiduje się odrębne przesłanki przetwarzania.

Lp.	Podstawa przetwarzania danych szczególnych kategorii	Objaśnienie
1.	**wyraźna zgoda** osoby, której dane dotyczą, na przetwarzanie tych danych osobowych w jednym celu lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, że osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych ze szczególnej kategorii	Najprostszą formą udzielenia zgody wyraźnej (która gwarantuje też rozliczalność administratora) z całą pewnością jest jej forma pisemna. Nie można też wykluczyć zgody udzielonej w formie elektronicznej i telefonicznej. Co najistotniejsze, zgoda wyraźna nie powinna przybierać brzmienia „przyjmuję do wiadomości...” ponieważ przyjęcie do wiadomości nie oznacza wyrażenia zgody wyraźnej.
2.	niezbędność przetwarzania celem wypełnienia obowiązków i wykonywania szczególnych uprawnień przez administratora danych osobowych lub osobę, której dane dotyczą, w **dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,** jeżeli tylko jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą	W tym zakresie należy odwołać się do źródeł prawa pracy, przede wszystkim Kodeksu pracy, ale także przepisów innych ustaw i aktów wykonawczych, określających prawa i obowiązki pracowników i pracodawców (np. ustawy o pracownikach samorządowych, Karty Nauczyciela, ustawy o działalności leczniczej), a także postanowień układów zbiorowych pracy i innych opartych na ustawie porozumień zbiorowych, regulaminów i statutów określających prawa i obowiązki stron stosunku pracy (a więc również regulaminów pracy o wynagradzania). Przesłanka ta legalizuje posługiwanie się danymi wrażliwymi kandydata do pracy, jak również pracowników. **Przykład.** Przetwarzanie danych osobowych członków związku zawodowego (przynależność do związku) powiązane z realizacją uprawnienia pracownika do szczególnej ochrony stosunku pracy z art. 32 ustawy o związkach zawodowych albo zwolnienia z obowiązku świadczenia pracy z art. 31 ustawy o związkach zawodowych).
3.	niezbędność przetwarzania celem ochrony **żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody	Należy zwrócić uwagę na szczególną doniosłość tego warunku ze względu na okoliczności, które legalizuje. Chodzi tu przede wszystkim o przypadki ochrony życia i zdrowia osoby, której dane dotyczą lub innej osoby (motyw 46 preambuły RODO). Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych, wyłącznie w przypadkach gdy ewidentnie przetwarzania tego nie można oprzeć na innej podstawie prawnej.
4.	objęcie przetwarzaniem danych osobowych **w sposób oczywisty upublicznionych** przez osobę, której dane dotyczą	Chodzi tu wyłącznie o ewidentny przypadek upublicznienia danych osobowych przez sam podmiot tych danych. **Przykład.** Polityk zamieszcza na portalu społecznościowym filmik z ceremonii zawarcia związku partnerskiego ze swoim partnerem.

5.	niezbędność przetwarzania danych osobowych celem ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy	Wskazana podstawa przetwarzania danych szczególnej kategorii dotyczy przypadków prowadzenia sporów sądowych **Przykład.** Pracodawca zwolnił pracownika, podając jako przyczynę częste absencje wywołane zwolnieniami lekarskimi powodujące dezorganizację pracy. Pracownik pozwał pracodawcę przed sądem pracy. Aby obronić swoje stanowisko, pracodawca musi przedstawić przedkładane przez pracownika zwolnienia lekarskie.
6.	niezbędność przetwarzania danych osobowych do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia	Dane osobowe mogą być przetwarzane na tej podstawie z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 9 ust. 3 RODO, tj. jeżeli są przetwarzane przez - lub na odpowiedzialność - pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe. Przykład. Pracodawca przetwarza dane osobowe o stanie zdrowia kandydata do pracy, odbierając orzeczenie lekarza medycyny pracy w sprawie przeciwwskazań do wykonywania pracy na danym stanowisku. Analogicznie pracodawca przetwarza takie dane pracownika w związku z badaniami okresowymi i kontrolnymi.
7.	niezbędność przetwarzania ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową	

	niezbędność przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą	

III. Obowiązek informacyjny

Jakie informacje administrator podaje podmiotom danych? Jest to istotna informacja także dla pracownika, który może otrzymać od pracodawcy polecenie służbowe przygotowania takiej informacji np. dla klienta.

Zakres informacji

Informacje podawane osobom, których dotyczą zebrane dane osobowe

A. Informacje wspólne dla obu przypadków (art. 13 i 14 RODO), tj. podawane:

- podczas pozyskiwania danych osobowych - w stosunku do zbierania ich od osób, których dane dotyczą - art. 13 RODO - oraz
- w odniesieniu do pozyskania danych osobowych ze źródeł innych niż te osoby - art. 14 RODO

1) tożsamość i dane kontaktowe ADO oraz (jeżeli dotyczy) tożsamość i dane kontaktowe jego przedstawiciela
2) dane kontaktowe inspektora ochrony danych (jeśli dotyczy)
3) cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania
4) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją
5) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu
6) prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO (tj. na bazie prawnie uzasadnionych interesów)
7) informacje o uprawnieniach przysługujących wobec ADO w związku z danymi osobowymi, tj. informacje o prawie:
   - dostępu do danych,
   - do żądania ich sprostowania, usunięcia lub ograniczenia przetwarzania,
   - do wniesienia sprzeciwu wobec przetwarzania,
   - do ich przenoszenia
8) informacje o prawie do cofnięcia zgody na przetwarzanie danych osobowych w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzanie odbywa się na podstawie zgody, o której mowa w art. 6 ust. 1 lit, a) lub art. 9 ust. 2 lit, a) ROPO)
9) informacje o prawie wniesienia skargi do organu nadzorczego
10) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji

międzynarodowej (albo do odbiorcy w państwie trzecim lub organizacji międzynarodowej - w przypadku art. 14 RODO) oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych

11) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby której dane dotyczą

B.I.Informacje podawane osobom fizycznym podczas pozyskiwania ich danych osobowych - dotyczy tylko przypadku zbierania ich od osób, których te dane dotyczą (art. 13 RODO)

1) informacja:

- czy podanie danych osobowych jest wymogiem ustawowym lub umownym albo warunkiem zawarcia umowy oraz
- czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych

B.2. Informacje podawane osobom, których dotyczą zebrane dane osobowe

- obejmuje tylko przypadek pozyskania tych danych ze źródeł innych niż te osoby (art. 14 RODO)
  1) kategorie odnośnych danych osobowych
  2) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - informacja, czy pochodzą one ze źródeł publicznie dostępnych

Kiedy i jak administrator realizuje obowiązek informacyjny

W przypadku zbierania danych od osób, których te dane dotyczą, administrator powinien przekazać stosowne informacje wymagane art. 13 RODO podczas pozyskiwania tych danych. Zasada rozliczalności nakłada na administratora obowiązek wykazania, że przestrzega on przepisów RODO. Dla- tego też administrator powinien móc wykazać, że obowiązek informacyjny wypełnił w wymagany przez art. 13 RODO sposób.

PRZYKŁAD

W przypadku pozyskania danych osobowych podczas wizyty klienta w biurze administratora danych osobowych należy od razu przedłożyć mu do podpisu stosowną klauzulę informacyjną oraz zachować jej podpisany egzemplarz do celów dowodowych.

PRZYKŁAD

W przypadku pozyskiwania danych osobowych przez stronę internetową należy przedstawić treść klauzuli informacyjnej np. w formie widocznego, wyskakującego okienka, umożliwiającego kliknięcie w oświadczenie o treści „zapoznałem się".

PRZYKŁAD

W przypadku monitoringu obok kamery można umieścić krótką informację o tym, kto jest administratorem danych osobowych oraz o jego danych kontaktowych i celach, podstawie prawnej przetwarzania danych osobowych, a także prawach osoby, której dane dotyczą; w tym miejscu należy również zamieścić informację, gdzie jest dostępna pełna treść klauzuli informacyjnej. •

W przypadku zbierania danych osobowych z innych źródeł niż od osoby, której te dane dotyczą, informacje wymagane przez art. 14 ust. 1 i 2 RODO należy podać:

- w rozsądnym terminie po ich pozyskaniu, mając na uwadze konkretne okoliczności przetwarzania danych osobowych, lecz najpóźniej w ciągu miesiąca;
- najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą jeżeli dane osobowe mają być stosowane do komunikacji z tą osobą, lub
- najpóźniej przy pierwszym ujawnieniu danych osobowych innemu odbiorcy - jeżeli administrator danych osobowych planuje takie ujawnienie.

Administrator danych osobowych może być zwolniony z wypełnienia przewidzianego art. 14 ust. 1-4

obowiązku informacyjnego, gdy i w zakresie, w jakim:

- osoba, której dane dotyczą, dysponuje już wymaganymi do podania informacjami;
- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
- pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu ADO podlega, i które przewiduje odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Zawsze jednak musi zrealizować obowiązek informacyjny z art. 13 RODO.

Informacje z art. 13 i 14 RODO powinny być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem, a w stosownych przypadkach dodatkowo wizualizowane, łączone ze standardowymi znakami graficznymi. Ponadto powinny uwzględniać konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych.

WAŻNE

Z „Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679" wynika, że administratorzy danych mogą przyjąć warstwowe podejście do przekazywania informacji wymaganych art. 13 lub 14 RODO. Polega to na przekazywaniu informacji wymaganych przez RODO stopniowo, na kilku poziomach.

IV. Wybrane prawa podmiotów danych

Dla pracownika istotna jest także wiedza, jakie uprawnienia przysługują podmiotom danych i jak je realizować. Dlaczego? Choćby z tego powodu, że to pracownik może odebrać żądanie realizacji danego uprawnienia i może zostać zobowiązany do wykonania działań w celu spełnienia tego żądania.

Dostęp do danych

Administrator ma obowiązek zapewniania dostępu podmiotowi do jego danych, a także do przekazywania mu stosownych informacji.

Informacje, które należy przekazać na żądanie podmiotu danych

- cele przetwarzania
- kategorie odnośnych danych osobowych
- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu
- informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania
- informacje o prawie wniesienia skargi do organu nadzorczego
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą
- odpowiednie zabezpieczenia (o których mowa w art. 46 RODO) związane z przekazaniem - jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej

Sprzeciw

Zgodnie z art. 21 ust. 1 RODO skuteczny sprzeciw może wnieść **osoba, której dotyczą dane** objęte sprzeciwem, względem przetwarzania dotyczących jej danych osobowych opartego na:

- art. 6 ust. 1 lit. e RODO (niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi) lub
- art. 6 ust. 1 lit. f RODO (niezbędność przetwarzania 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).

Krok 1. Zarejestruj sprzeciw

Administrator musi być gotowy na to, że sprzeciw może zostać złożony w każdej formie, np. ustnie w siedzibie administratora danych osobowych, ale też pisemnie za pośrednictwem poczty tradycyjnej, elektronicznej bądź z wykorzystaniem formularza kontaktowego na stronie firmy albo jej profilu w mediach społecznościowych.

Krok 2. Zbadaj zasadność sprzeciwu

Wprawdzie złożenie sprzeciwu dla wywołania jego skutków nie wymaga odrębnej decyzji administratora, niemniej jednak nie oznacza to, że wszystko dzieje się automatycznie. Administrator musi bowiem zbadać, czy dana osoba jest uprawniona do złożenia sprzeciwu.

Krok 3. Przekaż informację zwrotną wnoszącemu

W przypadku braku możliwości realizacji sprzeciwu należy poinformować osobę wnoszącą o tym braku i wskazać przyczyny. Jeżeli zaś istnieje możliwość uzupełnienia braków sprzeciwu, wówczas administrator powinien poprosić o jego uzupełnienie.

Krok 4. Zidentyfikuj treść żądania

Administrator powinien również ustalić treść żądania. Przede wszystkim należy zweryfikować, czy na pewno złożono sprzeciw, czy też jest to inne żądanie, np. ograniczenia przetwarzania.

Krok 5. Zaprzestań przetwarzania danych w zakresie objętym sprzeciwem

Po wykonaniu wszystkich dotychczasowych kroków administrator powinien polecić swojemu personelowi (odpowiedzialnemu za przetwarzanie danych w zakresie objętym sprzeciwem) natychmiastowe zaprzestanie ich przetwarzania.

Krok 6. Przetwarzaj dane mimo sprzeciwu, jeżeli masz inną podstawę ich przetwarzania

Jak już wiadomo, co do zasady sprzeciw dotyczy wyłącznie wykorzystywania danych na podstawie przesłanek z art. 6 ust. 1 lit. e lub f RODO. Jeżeli zatem administrator znajdzie inną podstawę prawną przetwarzania danych osobowych, to może on nadal przetwarzać dane - ale już na bazie nowej podstawy.

Prawo do bycia zapomnianym

Administrator musi ustalić, kiedy żądanie usunięcia danych będzie uzasadnione. Otóż podmiot danych może skutecznie domagać się usunięcia danych osobowych, jeżeli:
dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie danych na podstawie tej zgody i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują okoliczności go wykluczające,
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie UE lub prawie państwa członkowskiego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

WAŻ*NE*

Jeżeli wystąpi choćby jedna z tych okoliczności, wówczas administrator musi bez zbędnej zwłoki usunąć dane osobowe. Jeśli zaś wniosek „o zapomnienie" nie mieści się w żadnej z tych przesłanek, wtedy administrator powinien pozostawić go bez rozpoznania i poinformować podmiot danych o braku możliwości ich usunięcia.

Z drugiej strony danych osobowych nie należy usuwać w zakresie, w jakim ich przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, jeśli tylko prawdopodobne jest, że usunięcie uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- do ustalenia, dochodzenia lub obrony roszczeń.

WAŻNE

Realizacja żądania „zapomnienia" wiąże się z koniecznością wykasowania danych z wszelkich nośników danych, w tym także z kopii zapasowych.

Ograniczenie przetwarzania

Żądanie ograniczenia przetwarzania należy zrealizować w 4 przypadkach. Od tego, w jakim przypadku podmiot danych zażądał ograniczenia, zależy okres jego trwania

Przesłanka ograniczenia	Okres ograniczenia
podmiot danych kwestionuje prawidłowość ich przetwarzania	okres pozwalający administratorowi sprawdzić prawidłowość tych danych
stwierdzono niezgodność przetwarzania danych z prawem, ale podmiot danych sprzeciwia się ich usunięciu	okres, w jakim istnieje niezgodność przetwarzania z prawem
administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne podmiotowi danych do ustalenia, dochodzenia lub obrony roszczeń	
podmiot danych wniósł sprzeciw (z art. 21 ust. 1 RODO)	do momentu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą

Nawet jeśli te warunki są spełnione, to dane będzie można dalej przetwarzać:

- za zgodą podmiotu danych;
- w celu ustalenia, dochodzenia lub obrony roszczeń;
- w celu ochrony praw innej osoby fizycznej lub prawnej;
- z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Jedyne, co administrator może zrobić z danymi podlegającymi ograniczonemu przetwarzaniu, to nadal je przechowywać np. w bazach danych, w dokumentach w segregatorach czy też w korespondencji e-mailowej.

V. Naruszenie ochrony danych

Naruszenie ochrony danych osobowych to wszelkiego rodzaju incydenty (a więc naruszenia bezpieczeństwa, niepożądane zdarzenia) związane z ochroną danych osobowych. To zbiorcze pojęcie

obejmuje wszystkie sytuacje, w których dane osobowe są przetwarzane w sposób niezgodny z:

- przepisami prawa powszechnie obowiązującego - przede wszystkim z RODO;
- regulacjami wewnętrznymi konkretnego administratora danych (polityka bezpieczeństwa, polityka ochrony danych osobowych, instrukcja zarządzania systemami informatycznymi).

RODO wymaga, aby w przypadku gdy dojdzie do naruszenia danych osobowych, administrator danych sam zgłosił takie naruszenie do Prezesa Urzędu Ochrony Danych Osobowych.

Zgłoszenie powinno nastąpić bez zbędnej zwłoki, w miarę możliwości - czyli po prostu najszybciej, jak to jest możliwe. W żadnym jednak przypadku nie powinno to zaistnieć później niż w terminie 72 godzin od stwierdzenia naruszenia. Jeżeli jednak zgłoszenie pojawi się po upływie tych 72 godzin, wówczas administrator danych powinien dodatkowo dołączyć wyjaśnienie przyczyn opóźnienia.

Sporządzając wyjaśnienie przyczyn opóźnienia, warto opisać dokładnie i przekonująco (w miarę potrzeby wykazując to nawet dokumentami), dlaczego do opóźnienia doszło. Jeżeli bowiem Prezes Urzędu Ochrony Danych Osobowych zostanie przekonany, że do opóźnienia doszło bez winy administratora (ponieważ np. w międzyczasie doszło do całkowitej zmiany zarządu albo pożaru siedziby jednostki) i na dodatek opóźnienie nie jest wielkie, to wówczas administrator może uniknąć nałożenia kary pieniężnej albo przynajmniej doprowadzić do jej zmniejszenia.

Z kolei podmiot przetwarzający ma dokonywać zgłoszeń naruszeń administratorowi danych osobowych bez zbędnej zwłoki - nie ma tu żadnych innych zasad, w szczególności ograniczenia do 72 godzin.

RODO przewiduje tylko jeden wyjątek, gdy nie trzeba dokonywać zgłoszenia naruszenia do Prezesa UODO - gdy jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

RODO wymaga, aby administrator dokumentował wszelkie naruszenia ochrony danych osobowych, w tym:

- okoliczności naruszenia ochrony danych osobowych,
- skutki naruszenia,
- podjęte działania zaradcze.

Zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych dokonuje się elektronicznie, z wykorzystaniem formularza dostępnego na stronie internetowej Prezesa Urzędu Ochrony Danych Osobowych.

Administrator powinien zawiadomić osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może to powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Zawiadomienie powinno być dokonane bez zbędnej zwłoki.

Zawiadomienie powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej:

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- możliwe konsekwencje naruszenia ochrony danych osobowych;
- środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

WAŻNE

Zawiadomienia nie trzeba dokonywać, gdy:

- *administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;*
- *administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;*
- *zawiadomienie wymagałoby niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje*

publiczny komunikat lub zastosowany zostaje podobny środek i za jego pomocą osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób

PRZYKŁAD

Sytuacje, w których wg Grupy Roboczej konieczne jest zawiadomienie
podmiotu danych o naruszeniu:

- wiadomość e-mail w ramach marketingu bezpośredniego wysłano do odbiorców w polach „do:" lub „dw:", tym samym umożliwiając każdemu odbiorcy wgląd w adresy e-mail innych odbiorców;
- dane osobowe znacznej liczby studentów omyłkowo wysłano do niewłaściwej listy adresowej, na której znajduje się ponad 1000 odbiorców;
- szpitalna dokumentacja medyczna była niedostępna przez 30 godzin w wyniku cyberataku;
- administrator prowadzi internetową platformę handlową, a j ego klienci znajdują się w wielu państwach członkowskich; platforma pada ofiarą cyberataku i atakujący publikuje w Internecie identyfikatory użytkownika, hasła i historię zakupów;
- administrator prowadzi usługę internetową, a wyniku cyberataku na tę usługę nastąpił wyciek danych osobowych osób fizycznych.

VI. Bezpieczeństwo danych osobowych

Bezpieczeństwo danych osobowych oznacza przede wszystkim ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Pracodawca wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. RODO wskazuje m.in. na:

- pseudonimizację i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

To jednak nie jedyne możliwe środki bezpieczeństwa.

O tym, jakie środki bezpieczeństwa danych osobowych są stosowane w danym zakładzie pracy, decyduje pracodawca. Decyzja w tym zakresie jest poprzedzana przeprowadzeniem analizy ryzyka. Nie w każdym zakładzie pracy środki te będą więc takie same.

Można wyróżnić następujące środki bezpieczeństwa:

- prawne - regulacje prawne wewnątrzzakładowe, obowiązujące u administratora danych osobowych,
- organizacyjne - rozwiązania administracyjne,
- techniczne:
- informatyczne - środki elektroniczne służące zachowaniu bezpieczeństwa i integralności przetwarzanych danych,
- fizyczne.

WAŻNE

Pracownik musi przestrzegać przepisów wewnątrzzakładowych przyjętych u danego pracodawcy.

Środkami prawnymi służącymi bezpieczeństwu przetwarzanych danych mogą być:

- polityka prywatności,
- instrukcja zarządzania systemem informatycznym,
- polityka czystego biurka i czystego ekranu,
- ewidencja osób upoważnionych do przetwarzania danych osobowych,
- wykaz budynków i pomieszczeń gdzie przetwarza się dane osobowe,

- wykaz systemów i programów używanych do przetwarzania danych osobowych.

Przyjęte wewnątrzzakładowe akty prawne mogą nosić inne nazwy. Niezależnie od użytego nazewnictwa pracownicy mają obowiązek ich przestrzegania, pod warunkiem, że te akty są zgodne z RODO.

Środki organizacyjne

Nie każdy pracownik może mieć dostęp w równym stopniu do wszystkich danych osobowych. Pracodawca określa, którzy pracownicy mogą odczytywać lub zapisywać konkretne dane osobowe, np.: pracownik sekretariatu może mieć dostęp do danych z książki kontaktowej w postaci imion, nazwisk, firm i adresów - do danych wykonawców czy serwisu).

WAŻNE

Pracownik może przetwarzać dane osobowe tylko w takim zakresie, w jakim został upoważniony przez pracodawcę. Przetwarzanie danych bez odpowiedniego upoważnienia lub z przekroczeniem jego zakresu stanowi naruszenie, które powinno zostać zgłoszone pracodawcy i IOD (w zależności od ustaleń w danym zakładzie pracy).

Pracownicy powinni stosować się do wewnątrzzakładowych wytycznych regulujących np. następujące kwestie:

- do czego i kto się może logować,
- kto ma dostęp do jakich kluczy,
- kto przyznaje uprawnienia do poszczególnych systemów (np. finansowo- -księgowego, danych o nieobecnościach),
- jak postępować w sytuacji naruszenia bezpieczeństwa danych osobowych (np. stwierdzenia wykradzenia danych logowania do systemów IT),
- jak często należy zmieniać hasła dostępu do systemów informatycznych.

Środki informatyczne

a) Pracownicy powinni przestrzegać również następujących reguł (jeżeli zostały wprowadzone):
b) szyfrowanie nośników pamięci,
c) okres przechowywania elektronicznych nośników informacji zawierających dane osobowe,
d) sporządzanie kopii zapasowych,
e) szyfrowanie wiadomości e-mail,
f) obowiązek zainstalowania oprogramowania antywirusowego na komputerze służbowym lub prywatnym używanym do celów służbowych.

Środki fizyczne

Środkami ochrony fizycznej są środki chroniące pomieszczenia, sprzęt, infrastrukturę czy nawet sam personel administratora danych osobowych. Ochrona również dotyczy zdarzeń mogących zaistnieć fizycznie i realnie: wandalizm, kradzież, włamanie, klęska żywiołowa, terroryzm, podszycie się pod pracownika administratora danych osobowych. Środki fizyczne powinny chronić wszelkie rzeczywiście istniejące w przestrzeni obiekty, służące do przetwarzania danych osobowych lub biorące udział w takim przetwarzaniu.

Fizyczne środki bezpieczeństwa danych osobowych możemy podzielić na:

a) pasywne - zapobiegające albo opóźniające zagrożenia, np. ogrodzenie, zamek, zasuwa, łańcuch, krata, sejf, kasetka, Kensington Lock,
b) aktywne - wykrywające zagrożenia albo im przeciwdziałające, np. monitoring audio/wideo, nadajnik GPS, czujki ruchu, alarm przeciwwłamaniowy, czytnik biometryczny (poniekąd jest to zabezpieczenie także pasywne), system gaśniczy.

PRZYKŁAD

Z jakimi środkami fizycznymi mogą spotkać się pracownicy?
przechowywanie danych w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi);

- przechowywanie danych w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej;
- przechowywanie danych w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności

na włamanie;
- przechowywanie danych w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej;
- przechowywanie danych w pomieszczeniu wyposażonym w system alarmowy przeciwwłamaniowy;
- przechowywanie danych w pomieszczeniu objętym systemem kontroli dostępu;
- przechowywanie danych w pomieszczeniu kontrolowanym przez system monitoringu z zastosowaniem kamer przemysłowych;
- przechowywanie danych w pomieszczeniu, które w czasie nieobecności zatrudnionych tam pracowników jest nadzorowane przez służbę ochrony;
- przechowywanie danych w pomieszczeniu, które przez cała dobę jest nadzorowane przez służbę ochrony;
- przechowywanie danych w zamkniętej, niemetalowej szafie;
- przechowywanie danych w zamkniętej metalowej szafie;
- przechowywanie danych w zamkniętym sejfie lub kasie pancernej;
- przechowywanie kopii zapasowych lub archiwalnych zbioru danych osobowych w zamkniętej niemetalowej szafie;
- przechowywanie kopii zapasowych lub archiwalnych zbioru danych osobowych w zamkniętej metalowej szafie;
- przechowywanie kopii zapasowych lub archiwalnych zbioru danych osobowych w zamkniętym sejfie lub kasie pancernej;
- przetwarzanie danych w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach;
- przechowywanie danych w pomieszczeniu zabezpieczonym przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy;
- niszczenie dokumentów zawierających dane osobowe po ustaniu przydatności w sposób mechaniczny za pomocą niszczarek dokumentów.

Usuwanie, pseudonimizacja, anonimizacja

Wpływ na bezpieczeństwo przetwarzania danych mają także procesy takie jak usuwanie danych, pseudonimizacja i anonimizacja. Należy odróżniać te pojęcia.

Usuwanie danych

Dane osobowe powinny zostać usunięte bezzwłocznie, jeżeli są zbędne do realizacji celu, dla którego zostały zebrane. Dane powinny być więc usunięte kiedy nie są już potrzebne w kontekście celu dla którego zostały pobrane - kiedy administrator nie ma prawa przetwarzać danych osobowych. Usunięcie danych oznacza definitywne wykasowanie danych z wszelkich nośników danych, w tym także z kopii zapasowych. Obowiązkiem usuwania danych mogą być obarczeni pracownicy.

Anonimizacja

Jeżeli pracodawca nie ma już podstawy prawnej do przetwarzania danych osobowych (np. z powodu przedawnienia) ale z jakichś przyczyn chce zachować umowy, może te umowy zmodyfikować przez usunięcie danych osobowych z treści umów (wyczernienie, wykreślenie, wycięcie w sposób trwale uniemożliwiający odczytanie danych). Obowiązek wykonywania czynności anonimizacyjnych może zostać nałożony na pracowników.

Pseudonimizacja

O ile usunięcie danych osobowych czy to poprzez zniszczenie dokumentu czy anonimizację prowadzi do całkowitej niemożności odtworzenia tożsamości danych osobowych, o tyle spseudonimizowane dane osobowe to takie dane, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej. Po pseudonimizacji mamy więc nadal do czynienia z informacjami o możliwej do zidentyfikowania osobie fizycznej.

Przykłady naruszeń bezpieczeństwa

1. Pracownik zaniechał instalacji oprogramowania antywirusowego i firewalla na komputerze prywatnym używanym do celów służbowych, wskutek czego doszło do wykradnięcia danych osobowych klientów.
2. Pracownik omyłkowo wysłał wiadomość e-mail do osoby, która nie była uprawniona do dostępu do danych osobowych zawartych w tej wiadomości. Dane te nie były zaszyfrowane, mimo, że tak przewidywała obowiązująca u pracodawcy polityka bezpieczeństwa.
3. Pracownik wysłał tę samą wiadomość e-mail do kilku odbiorców, wpisując w polu: „adresaci" wszystkie adresy e-mail, wskutek czego każdy z odbiorców ma możliwość podglądu adresu skrzynki mailowej innych odbiorców (a adresy te pozwalają na identyfikację osób fizycznych, przez co stanowią dane osobowe).
4. Pracownik miał wykonać anonimizację danych w niektórych dokumentach. Zdecydował się na użycie korektora, przez co dane nadal można było odczytać.
5. Podczas sprzątania biura pracownik omyłkowo wraz z makulaturą wyrzucił do kosza archiwalne dokumenty zawierające dane osobowe. Nie doszło więc do zniszczenia tych danych i niestety stały się one dostępne dla nieuprawnionych.
6. Pracownik nie zamknął pomieszczenia z dokumentacją zawierającą dane osobowe na klucz, wskutek czego dostęp do pomieszczenia mogły zyskać osoby postronne.
7. Pracownik wyniósł bez zgody pracodawcy dokumenty zawierające dane osobowe poza firmę.
8. Pracownik trzymał na biurku kartkę z loginem i hasłem do wewnątrzzakładowego oprogramowania zawierającego dane osobowe. Kartka była widoczna dla osób postronnych.

Co grozi pracownikowi

Pracownik musi jednak liczyć się z odpowiedzialnością za spowodowanie naruszenia ochrony danych osobowych w zakładzie pracy:

Odpowiedzialność materialna

Jeżeli przez naruszenie doszło do wyrządzenia szkody pracodawcy (pracodawca został obciążony karą pieniężną przez Prezesa UODO lub musiał zapłacić odszkodowanie podmiotowi danych), wówczas w trybie roszczenia regresowego pracodawca może zażądać odszkodowania od pracownika. W przypadku wyrządzenia szkody z winy nieumyślnej odszkodowanie nie może przekraczać równowartości 3-miesięcznego wynagrodzenia pracownika.

Odpowiedzialność porządkowa

Nawet jeśli pracodawca nie został ukarany za naruszenie ochrony danych osobowych spowodowanych przez pracownika, to i tak pracownik może zostać ukarany karą porządkową upomnienia lub nagany za naruszenie porządku pracy. Kara ulega zatarciu (usunięciu z akt osobowych pracownika) po roku nienagannej pracy.

Zwolnienie dyscyplinarne

W skrajnych przypadkach, jeżeli uchybienie pracownika będzie nosiło znamiona ciężkiego naruszenia podstawowych obowiązków pracowniczych, pracodawca może rozwiązać z pracownikiem umowę o pracę bez wypowiedzenia. Ta sankcja może być stosowana w skrajnych przypadkach, np. gdy uchybienie spowodowało wyciek danych osobowych na dużą skalę.