WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

APPLiA PL
Związek pracodawców AGD

Przewodnik po RODO dla serwisów sprzętu AGD

RODO 2018

Czerwiec 2018

Spis treści

Niniejszy przewodnik powstał na zlecenie APPLiA Polska. Autorami są specjaliści z zakresu ochrony danych osobowych – prawnicy kancelarii WKB Wierciński, Kwieciński, Baehr Sp. k. Celem przewodnika jest wsparcie serwisów AGD w stosowaniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Przewodnik nie stanowi źródła prawa, a informacje w nim zawarte nie mają charakteru wiążącej interpretacji przepisów RODO.

Regulacje prawne i źródła informacji zakresu danych osobowych

1. Akty prawne:

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)

2. Inne źródła wiedzy:

https://www.giodo.gov.pl/ – strona Generalnego Inspektora Ochrony Danych Osobowych

https://uodo.gov.pl/ – strona Urzędu Ochrony Danych Osobowych z wieloma informacjami i pomocami w dostosowaniu do wymogów RODO

https://rodo.niw.gov.pl/ – ogólnopolska platforma informacyjna w zakresie RODO przygotowana przez Narodowy Instytut Wolności i Generalnego Inspektora Ochrony Danych Osobowych

https://www.mpit.gov.pl/media/50521/PrzewodnikMSP_RODO_2018.pdf – przewodnik po RODO przygotowany na zlecenie Ministerstwa Przedsiębiorczości i Technologii

Czym jest 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) zwane RODO, które obowiązuje od 25 maja 2018 r.

RODO reguluje przetwarzanie danych osób fizycznych. Każda spółka przetwarzająca dane swoich klientów i pracowników musi zrealizować wynikające z Rozporządzenia obowiązki w zakresie zapewnienia zasad przetwarzania danych:

Zgodność z prawem, rzetelność i przejrzystość – przetwarzanie danych osobowych musi się odbywać w granicach prawa, a osoby, których dane dotyczą, muszą być szczegółowo, wyczerpująco oraz w jasny i zrozumiały sposób poinformowane o okolicznościach takiego przetwarzania.

Ograniczenie celu – dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach. Dane zebrane w celu realizacji umowy mogą być wykorzystane w takim właśnie celu, o czym podmiot danych powinien zostać poinformowany.

Minimalizacja danych – dane osobowe, które przetwarza serwis, powinny być odpowiednie, istotne i ograniczone do zakresu niezbędnego dla celów, dla których zostały zebrane.

Prawidłowość – dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe, zostały niezwłocznie usunięte lub sprostowane.

Ograniczenie przechowywania – dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne.

Rozliczalność – administratorzy danych osobowych muszą wykazać przestrzeganie wymienionych zasad ochrony danych. W przypadku postępowania wyjaśniającego prowadzonego przez organ ochrony danych ciężar wykazania zgodnego z prawem przetwarzania ciąży na administratorze. Administrator będzie musiał przedstawić podstawy prawne przetwarzania, np.: umowy z podmiotami danych, zgody, informacje i potwierdzenie ich doręczenia podmiotowi danych itp.

Czy RODO dotyczy serwisów AGD?

RODO dotyczy wszystkich podmiotów mających do czynienia z przetwarzaniem danych osobowych. Nawet w przypadku prowadzenia jednoosobowej działalności gospodarczej należy wdrożyć odpowiednie środki techniczne i organizacyjne dla zapewnienia odpowiedniego poziomu bezpieczeństwa danych osobowych.

Serwisy AGD świadczą usługi naprawy sprzętu, często również jego podłączania, co wymaga przetwarzania danych osobowych klientów, potencjalnych klientów, pracowników i współpracowników.

Słownik najważniejszych pojęć

Administrator: oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innym ustala cele i sposoby przetwarzania danych osobowych.

Anonimizacja: to proces uniemożliwiający ujawnienie tożsamości, służący ochronie danych osobowych.

Dane osobowe: 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 identyfikatorów takich jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Naruszenie ochrony danych osobowych: 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.

Organ nadzoru: niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO, w Polsce funkcję tę dotychczas pełnił Generalny Inspektor Ochrony Danych Osobowych (GIODO), według projektu nowej ustawy o ochronie danych osobowych będzie to Prezes Urzędu Ochrony Danych Osobowych.

Podmiot przetwarzający dane: oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Przetwarzanie: operacja (lub zestaw operacji) na danych osobowych lub zestawach danych osobowych przeprowadzana w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

Pseudonimizacja: 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.

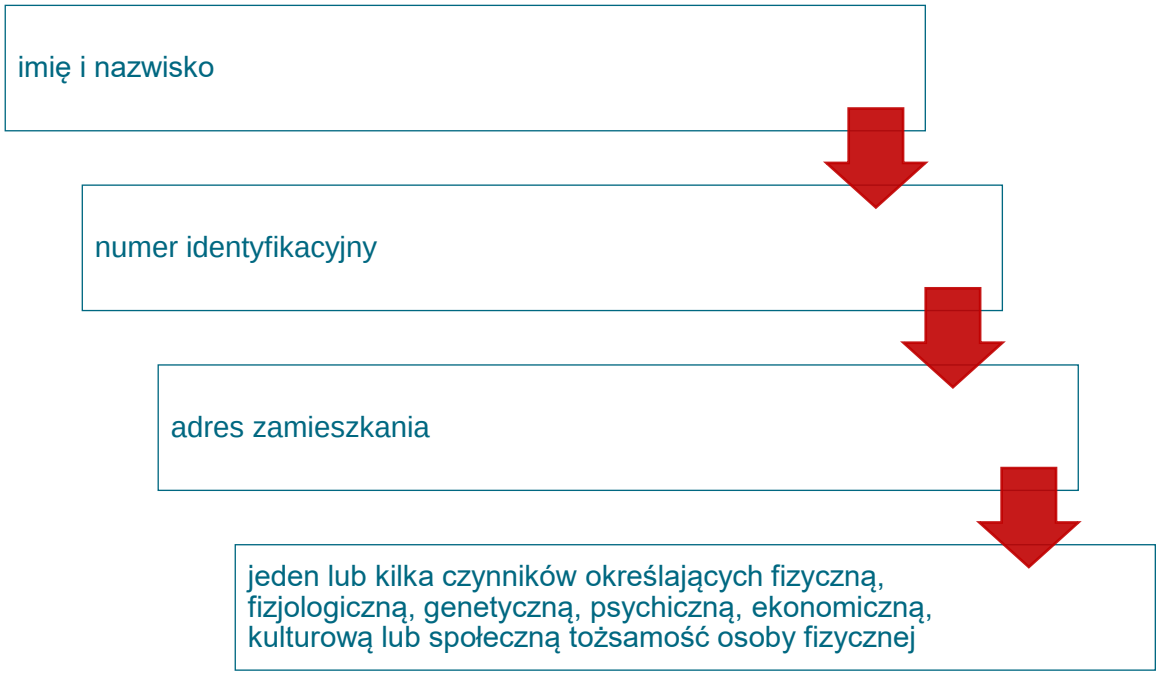
Kiedy serwis przetwarza dane osobowe?
Definicje przetwarzania i danych osobowych

☑ RODO ma zastosowanie zarówno do przetwarzania danych osobowych w formie papierowej, jak i elektronicznej.

☒ RODO nie ma zastosowania do przetwarzania danych osobowych w ramach działalności osobistej lub domowej.

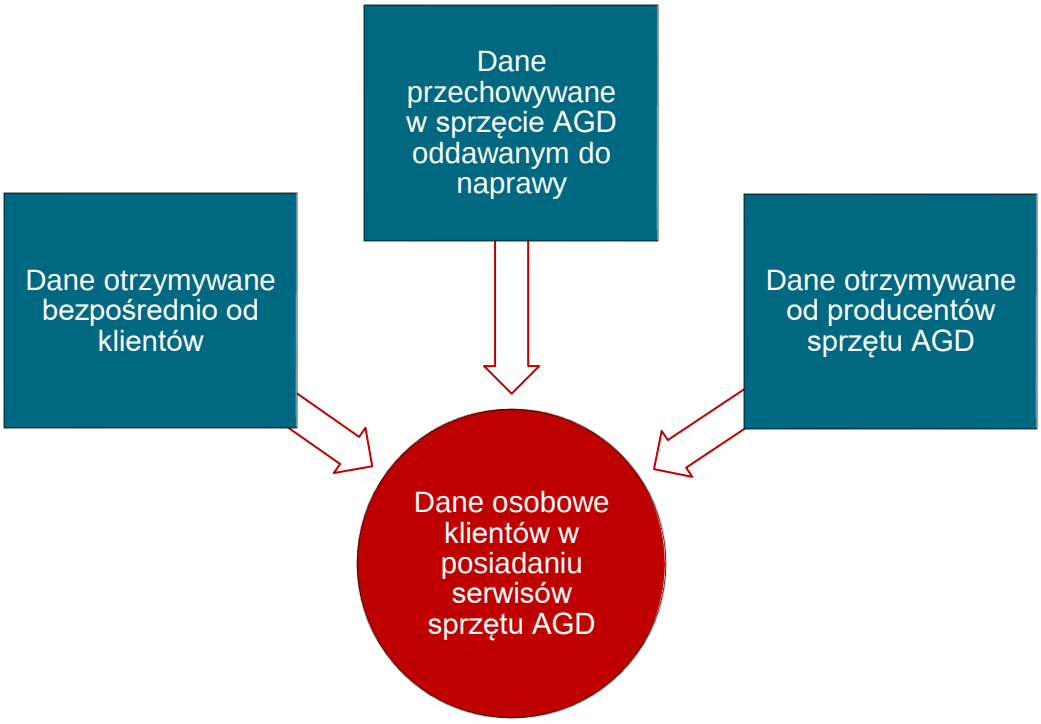
☒ RODO nie ma zastosowania do przetwarzania danych osobowych poza ustrukturyzowaną bazą danych.

Dane osobowe oznaczają informacje, które wprost identyfikują osobę fizyczną lub umożliwiają jej zidentyfikowanie. Możliwa do zidentyfikowania osoba to ta, której tożsamość można ustalić na podstawie posiadanych informacji. Danymi osobowymi w szczególności będą zatem:



Wskazane powyżej kategorie informacji będą uznawane za dane osobowe, jeżeli pozwolą zidentyfikować lub umożliwić zidentyfikowane osoby, której dotyczą – na przykład sam adres zamieszkania lub numer telefonu niekoniecznie musi identyfikować osobę fizyczną.

Dane osobowe klientów w serwisach sprzętu AGD



Dane zawarte w sprzęcie oddawanym do naprawy

- W niektórych nowoczesnych (inteligentnych) urządzeniach AGD przechowywane są dane osobowe ich użytkowników.
- Dane te nie powinny być odczytywane lub kopiowane przez serwisy AGD, chyba że jest to niezbędne do wykonanie naprawy.
- Dane nie mogą być wykorzystywane w innych celach niż wykonanie naprawy.
- Jeżeli zachodzi potrzeba usunięcia danych z urządzenia, to należy o tym poinformować klienta.

DOWÓD PRZYJĘCIA SPRZĘTU DO NAPRAWY

Nr .....

Nazwa firmy .....

adres .....

NIP ..... telefon .....

Nazwa firmy / Nazwisko i imię .....

adres .....

kontakt .....

Nazwa sprzętu ..... model .....

typ ..... numer seryjny .....

szacunkowa wartość sprzętu ..... data produkcji .....

RAZEM

Udziela się gwarancji na jakość wykonanej naprawy na okres .....

Wymagane wykonanie okresowego przeglądu w terminie .....

Jako datę wykonania naprawy ustala się .....

Klient wyraża zgodę na naprawę nie zgłoszonych usterek w powierzonym sprzęcie ☐ TAK ☐ NIE

Klient określa maksymalny koszt naprawy na kwotę .....

W przypadku rezygnacji z naprawy klient zostanie obciążony kosztami ekspertyzy .....

W przypadku nie odebrania sprzętu z naprawy w ciągu ..... dni od wyznaczonego terminu klient zostanie obciążony odsetkami w wysokości ..... % wartości naprawy za każdy dzień spóźnienia.

W przypadku nie odebrania sprzętu z naprawy w ciągu ..... dni sprzęt ulega przepadkowi.

Data / podpis przyjmującego sprzęt

Data odbioru sprzętu / podpis klienta

Zgodność przetwarzania z prawem. Kiedy można przetwarzać dane osobowe?

Artykuł 6 RODO wyróżnia 6 warunków, na podstawie których przetwarzanie danych można uznać za zgodne z prawem. W praktyce działalności serwisów zastosowanie będą miały następujące warunki:

- 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.

  Przykład: Serwis przetwarza dane osobowe klienta na potrzeby realizacji umowy o naprawę sprzętu zawartej z klientem. Serwis nie potrzebuje uzyskiwać zgody klienta na przetwarzania ani jakiegokolwiek innego oświadczenia klienta.

- Przetwarzanie jest niezbędne do **celów wynikających z prawnie uzasadnionych interesów** realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których prawa i wolności osoby fizycznej należy uznać za ważniejsze niż interes administratora, w szczególności, gdy osoba fizyczna jest dzieckiem.

  Przykład: Serwis wykonał umowę o naprawę sprzętu, lecz klient zgłasza roszczenia lub klient nie zapłacił. Serwis nie potrzebuje uzyskiwać zgody klienta na przetwarzania ani jakiegokolwiek innego oświadczenia klienta.

- Przetwarzanie danych jest niezbędne dla zapewnienia zgodności z przepisami prawa (**obowiązek prawny**).

  Przykład: Ustawa nakłada na serwis obowiązek przechowywania akt pracowniczych albo faktur klientów.

- Podstawę do przetwarzania może również stanowić **zgoda** na przetwarzanie danych osobowych w jednym lub większej liczbie określonych celów.

  Przykład: Serwis chce promować wśród klientów działalność swoich partnerów albo przekazywać dane osobowe swoim partnerom.

  ☑ **Zgoda na przetwarzanie danych powinna być:**

  - dobrowolna,
  - konkretna,
  - świadoma,
  - jednoznaczna.

  ☒ **Nie można uznać za wyrażenie zgody:**

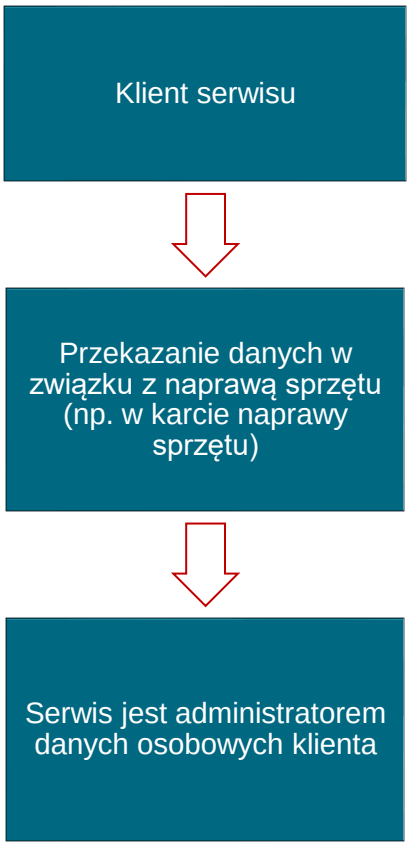
  - milczenia,
  - domyślnie zaznaczonych okienek zgody,
  - braku działania.

Administrator danych a podmiot przetwarzający

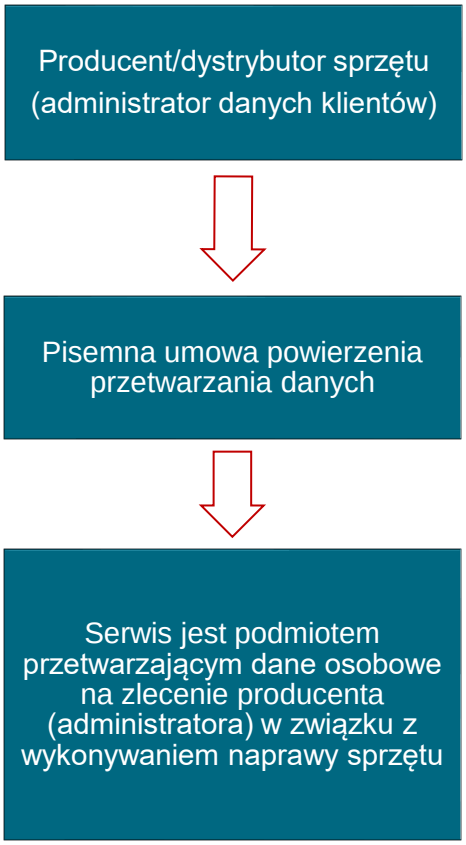
Administrator danych osobowych	Podmiot, któremu dane osobowe zostały przekazane do przetwarzania
samodzielnie lub wspólnie z innymi administratorami danych ustala cele i sposoby przetwarzania danych osobowych	przetwarza dane osobowe **w imieniu administratora**

Zgodnie z podziałem przedstawionym powyżej dane osobowe mogą być przetwarzane bezpośrednio przez administratora, tj. podmiot, który samodzielnie ustala cel, w którym dane osobowe są przetwarzane i sposoby takiego przetwarzania. Dane osobowe mogą być także przetwarzane na polecenie administratora przez inny podmiot (procesora). Procesor, któremu dane osobowe zostały powierzone do przetwarzania na podstawie umowy, nie ma żadnych kompetencji władczych w stosunku do przetwarzanych danych, w szczególności nie ma wpływu na cel i zakres ich przetwarzania.

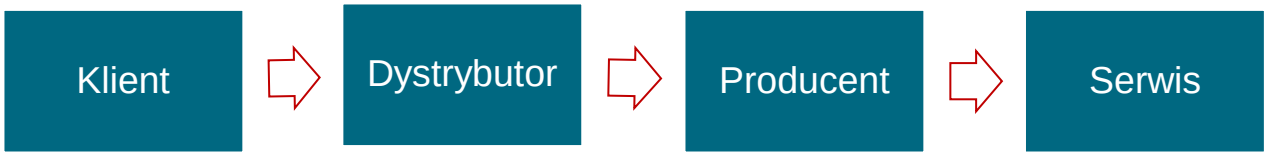
Zbieranie danych osobowych



Powierzenie przetwarzania danych osobowych



Kiedy serwis przetwarza dane osobowe na polecenie administratora?



Dane są najczęściej otrzymywane od producentów sprzętu AGD

- Serwisy otrzymują dane osobowe klientów od producentów sprzętu AGD najczęściej na podstawie umowy powierzenia przetwarzania danych osobowych.
- Administratorem danych osobowych jest producent.

UMOWA POWIERZENIA

Obligatoryjne elementy umowy

- ✓ Rodzaj powierzonych danych i kategorie osób, których dane dotyczą
- ✓ Cel przetwarzania
- ✓ Czas przetwarzania
- ✓ Warunki współpracy administratora z procesorem
- ✓ Warunki dotyczące zakończenia współpracy
- ✓ Klauzula poufności

Fakultatywne elementy umowy

- ✓ Zobowiązanie procesora do zapewnienia odpowiedniego poziomu zabezpieczenia danych osobowych
- ✓ Wskazanie, czy procesor jest (i na jakich warunkach) upoważniony do dalszego powierzania przetwarzania
- ✓ Forma przekazania danych

Czy producent musi objąć dodatkowymi porozumieniami o powierzeniu przetwarzania danych osobowych osoby pracujące dla serwisów autoryzowanych na zasadzie samozatrudnienia, tj. osoby prowadzące własną działalność gospodarczą?

Jeżeli serwis AGD powierza do przetwarzania dane osobowe innemu samodzielnemu podmiotowi, który np.: zatrudnia pracowników, ma własny system IT, tworzy własne zbiory danych, to między stronami powinna zostać zawarta umowa powierzenia przetwarzania danych.

Jeżeli serwis AGD współpracuje z osobą prowadzącą działalność gospodarczą albo zleceniobiorcą, a osoba ta nie posiada własnej infrastruktury albo czynności zlecone wykonuje w ramach przedsiębiorstwa serwisu AGD, to z taką osobą nie podpisuje się umowy o powierzenie przetwarzania danych osobowych. W powyższym przypadku osobę taką powinno się upoważnić do dostępu do danych osobowych i objąć zobowiązaniem do zachowania danych w poufności na takiej samej zasadzie jak pracownika.

Serwisy autoryzowane otrzymują zlecenia w systemie CRM, ale część z nich przepisuje te zlecenia do swojej bazy. Czy mogą tak robić?

Tak, serwisy mogą przepisywać zlecenia do swoich baz. Mogą to robić wyłącznie w zakresie, w jakim wykonują usługi dla producenta, tzn. dla wykonania naprawy. Serwisy nie mają możliwości przetwarzania danych dla innych celów, a dane otrzymane od producenta, także zamieszczone w swojej bazie, powinny zostać usunięte po upływie odpowiedniego okresu retencji.

Kiedy serwis przetwarza dane jako administrator? Obowiązki jakie RODO nakłada na administratora

- Serwis jest administratorem danych osobowych swoich pracowników oraz danych osobowych otrzymywanych bezpośrednio od klientów (np. naprawa pogwarancyjna).
- Serwis ponosi odpowiedzialność za odpowiednie przetwarzanie danych osobowych.
- Serwis ma obowiązek przetwarzać dane zgodnie z celem ich zebrania.
- Serwis powinien poinformować klientów (np. w dokumencie przyjęcia sprzętu do naprawy), m. in. o tym, że:
    1. jest administratorem ich danych osobowych
    2. o swoim adresie
    3. o celu przetwarzania danych
    4. o prawach klienta związanych z przetwarzaniem danych

    (więcej informacji w rozdziale „Obowiązek informacyjny”).
- Serwis jest obowiązany do odpowiedniego zabezpieczenia danych (więcej informacji w rozdziale „Jaką dokumentację i zabezpieczenia powinien posiadać serwis?”).
- Jeżeli dane osobowe klienta są zbierane do celów wykonania naprawy, to nie ma konieczności uzyskiwania zgody klienta na przetwarzanie danych osobowych.
- RODO nakłada obowiązek samodzielnego dokonywania oceny ryzyka dla bezpieczeństwa danych osobowych i na tej podstawie dostosowywanie odpowiedniego zabezpieczenia. Czynność wdrożenia środków zabezpieczających nie może być czynnością jednorazową. Serwis jako administrator danych osobowych jest zobowiązany do stałego weryfikowania ryzyka i dostosowywania skutecznych metod zapewniających bezpieczeństwo danych osobowych.
- Serwis jest zobowiązany do wykazania, że czynności przetwarzania są zgodne z RODO, dlatego warto je wprowadzić do swojej działalności w sposób sformalizowany, np. w formie Regulaminu dla Pracowników.

Obowiązek informacyjny

Poniżej, w formie tabeli, przedstawiamy zakres podstawowego obowiązku informacyjnego wynikającego z RODO, który musi być spełniony przez serwisy w stosunku do osób fizycznych, których dane są przetwarzane lub których dane dotyczą, w sytuacjach, gdy dane są pozyskiwane wprost od takich osób. Obowiązek informacyjny powinien być spełniony przez serwis tylko w przypadku, gdy serwis jest administratorem danych. Gdy serwis działa na zlecenie producenta, to producent spełnia ten obowiązek.

Zakres	Uwagi
☑ Dane identyfikacyjne administratora, dane kontaktowe oraz dane przedstawiciela (gdy ma to zastosowanie)	–
☑ Dane kontaktowe inspektora ochrony danych	W przypadku, gdy inspektor ochrony danych został powołany. W przypadku serwisów AGD raczej nie ma obowiązku powołania.
☑ Cel i podstawa przetwarzania.	Należy wskazać wprost cel przetwarzania danych osobowych i poinformować o podstawie, np. jeżeli dane są niezbędne do wykonania umowy, należy o tym poinformować podmiot danych.
☑ Prawo do wycofania zgody (gdy ma to zastosowanie)	Obowiązkowe wyłącznie w przypadku, gdy przetwarzanie danych osobowych opiera się na zgodzie podmiotu danych.
☑ Odbiorcy lub kategorie odbiorców danych	Jeżeli kiedy dane są przekazywane osobom trzecim należy wskazać wprost konkretnych odbiorców lub ich kategorie.
☑ Szczegóły przekazania danych do państwa trzeciego (gdy ma to zastosowanie)	Chodzi o państwa znajdujące się poza obszarem Europejskiego Obszaru Gospodarczego.
☑ Okres, przez który dane będą przechowywane lub kryteria ustalenia tego okresu	Jeżeli można przewidzieć i wprost wskazać taki okres, należy to zrobić np. w czasie niezbędnym do realizacji umowy o naprawę albo monitoringu - jeśli istnieje.
☑ Informacje o prawach osoby, której dane dotyczą, w tym prawo do sprzeciwu wobec marketingu bezpośredniego, prawo do żądania dostępu do danych oraz „prawo do bycia zapomnianym”	–
☑ Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu	Jedynie wtedy, gdy administrator profiluje osoby fizyczne.
☑ Prawo do złożenia skargi do organu nadzorczego	–

Przykładowy wzór klauzuli informacyjnej znajduje się w załączeniu do Przewodnika. Klauzula informacyjna dla podmiotów danych może obejmować wszystkie formy i podstawy przetwarzania.

UWAGA! Jeżeli na terenie serwisu znajduje się monitoring, należy spełnić obowiązek wobec wszystkich osób objętych jego zasięgiem. Nie oznacza to oczywiście, że każdej osobie wchodzącej na teren zakładu należy wręczyć osobny dokument informacyjny. Wystarczy, że obowiązek informacyjny dotyczący monitoringu zostanie powieszony na tablicy w widocznym dla wszystkich miejscu, np. przy wejściu głównym do budynku, na ladzie serwisu.

Uprawnienia klientów

Prawo dostępu do danych

Uprawnienie do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe, a jeżeli tak – uzyskania dostępu do nich oraz do dodatkowych informacji (m.in. o celu przetwarzania, kategoriach danych, informacji o odbiorcach, planowanym okresie przechowywania itd.).

Prawo do sprostowania danych

Uprawnienie do żądania niezwłocznego sprostowania danych osobowych, które są nieprawidłowe.

Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

„Prawo do bycia zapomnianym" – prawo do usunięcia danych

Uprawnienie do żądania niezwłocznego usunięcia danych, jeżeli m.in. dane nie są już niezbędne dla celów, w których zostały zebrane, osoba cofnęła zgodę, na której opiera się przetwarzanie lub dane były przetwarzane niezgodnie z prawem.

? Jeżeli klient zażąda usunięcia danych, to kto odpowiada za realizację tego żądania?

Do usunięcia danych osobowych zobowiązane będą wszystkie podmioty je przetwarzające, czyli np. producent (administrator), procesor (serwis).

Zgodnie z RODO procesor zobowiązany jest, w miarę możliwości, pomagać administratorowi danych wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą. Oznacza to, że musi on współdziałać z administratorem danych w zakresie realizacji uprawnień osób, których dane dotyczą.

W związku z tym procesor (a także podprocesorzy działający na jego zlecenie) będzie musiał po zakończeniu przetwarzania powierzonych danych usunąć je lub zwrócić administratorowi danych w zależności od jego woli. Obowiązek ten dotyczy również wszelkich kopii danych, które zostały wykonane.

Za realizację żądania usunięcia danych odpowiada administrator.

UWAGA! Dobrym rozwiązaniem po okresie zakończenia gwarancji jest przechowywanie samego numeru seryjnego. Po numerze seryjnym bowiem będzie można prześledzić historię napraw produktu. Dane osobowe klienta nie będą wówczas przetwarzane.

Czy można odmówić usunięcia danych?

Administrator może odmówić usunięcia danych jeżeli przetwarzanie danych jest nadal konieczne do wykonania umowy albo do wypełnienia obowiązku prawnego albo do wykonania umowy jaka wiąże serwis np.: z producentem.

Jaki sposób usunięcia danych uważa się za spełnienie wymagań?

Przez usunięcie danych osobowych rozumiemy zniszczenie oraz modyfikację danych, które nie pozwolą na ustalenie tożsamości osoby, której dane dotyczą. Usunięcie danych dotyczy wszelkich dokumentów zawierających identyfikujące dane (w tym także dane zapasowe). Usunięcie danych może nastąpić poprzez: zniszczenie (bezpowrotne usunięcie danych) lub anonimizację (usunięcie z dokumentu danych osobowych w taki sposób, aby niemożliwe było ich odczytanie, w przypadku aplikacji informatycznych – przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej albo gdyby przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań).

Prawo do ograniczenia przetwarzania danych

Prawo przysługuje we wskazanych w RODO przypadkach, np. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych.

Prawo do przenoszenia danych

Prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych dostarczonych administratorowi i przesłania ich innemu administratorowi, jeśli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy i w sposób zautomatyzowany.

Prawo do wycofania zgody na przetwarzanie danych

Klient ma prawo wycofać zgodę na przetwarzanie danych osobowych. Wycofanie zgody powinno być tak łatwe jak jej udzielenie.

Co się stanie jak ktoś wycofa zgodę?

Cofnięcie zgody na przetwarzanie danych osobowych może mieć miejsce jedynie w stosunku do danych przetwarzanych na podstawie zgody. Cofnięcie zgody spowoduje zatem obowiązek zaprzestania przetwarzania danych osobowych jedynie w zakresie danych, których zgoda dotyczyła. Dane osobowe przetwarzane na innej podstawie, np. gdy są niezbędne do wykonywania umowy, będą mogły nadal być legalnie przetwarzane. Warto podkreślić, że cofnięcie zgody nie będzie wywierało skutków na legalność przetwarzania danych, które miało miejsce przed cofnięciem zgody.

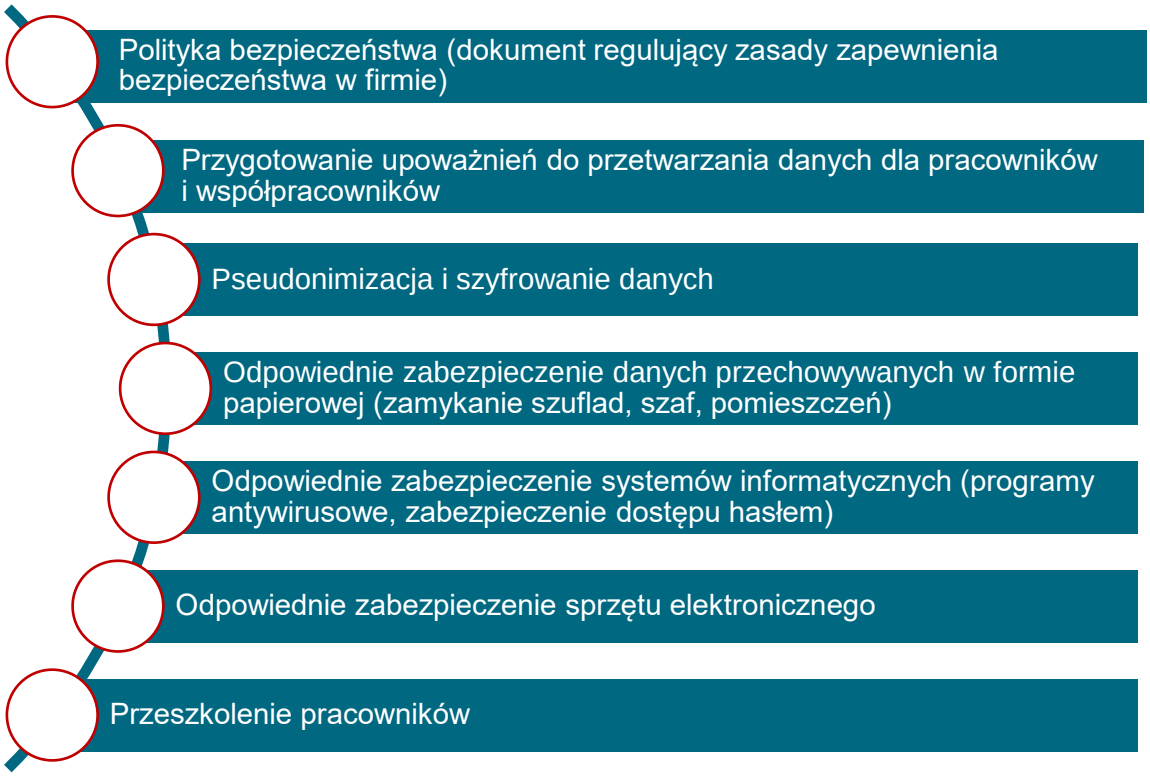
Jaką dokumentację i zabezpieczenia powinien posiadać serwis?

Zgodnie z RODO administratorzy danych osobowych, jak również procesorzy, powinni wdrożyć „odpowiednie środki techniczne i organizacyjne" w celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku związanemu z przetwarzaniem.

Wdrażając odpowiednie środki serwisy powinny uwzględnić:

- stan wiedzy technicznej
- koszt wdrożenia
- zakres przetwarzania
- kontekst przetwarzania
- cel przetwarzania
- charakter danych
- ryzyko naruszenia praw

Przykłady odpowiednich środków technicznych i organizacyjnych:



Czy istnieje obowiązek szyfrowania korespondencji z serwisami/producentami?

Szyfrowanie danych osobowych to tylko jedno z rozwiązań, jakie administrator danych lub podmiot przetwarzający może wykorzystać w celu zapewnienia bezpieczeństwa danych. Administratorzy danych w celu zapewnienia bezpieczeństwa wdrażają odpowiednie środki techniczne i organizacyjne, uwzględniając stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Szyfrowanie danych nie jest obowiązkiem wskazanym w RODO. Chociaż szyfrowanie jest dobrym sposobem zabezpieczenia danych osobowych, można je zastąpić innym środkiem adekwatnym do elementów wymienionych wyżej.

Ile czasu można przetrzymywać dane klienta dotyczące zgłoszeń gwarancyjnych i pogwarancyjnych? Jeżeli klient zażąda usunięcia danych ze zgłoszenia, czy również należy usunąć dane w dokumentach finansowych?

Dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (zasada minimalizacji).

Administrator danych może także przetwarzać dane dopóki jest to niezbędne do wykonania obowiązku prawnego. W tym przypadku dane klienta mogą być przechowywane przez okres trwania gwarancji, a także przedawnienia roszczeń. W przypadku gdy w ramach naprawy na wymienioną część został przyznany oddzielny okres gwarancyjny – dane powinny być przechowywane do zakończenia okresu gwarancyjnego przysługującego na wymienioną część.

Dokumenty finansowe zawierające dane osobowe, zgodnie z art. 80 ustawy o ordynacji podatkowej, można usunąć po upływie 5 lat, licząc od końca roku kalendarzowego, w którym upłynął termin wygaśnięcia prawa do zwrotu nadpłaty podatku.

Rejestr przetwarzania danych

Prowadzenie rejestru czynności przetwarzania to obowiązek, który ma zastąpić dotychczasowe formalne rejestrowanie zbiorów danych osobowych. Administratorzy lub podmioty przetwarzające powinni prowadzić rejestr czynności przetwarzania, jeżeli zatrudniają co najmniej 250 osób. W przypadku jednak, gdy zatrudniają mniej niż 250 osób, ale przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych wskazany obowiązek dalej istnieje. Serwisy są zatem zobowiązane w pierwszej kolejności do ustalenia, czy w przypadku ich działalności taki obowiązek istnieje. W naszej ocenie może się zdarzyć, że serwisy będą zobowiązane do prowadzenia rejestru. Sam rejestr czynności przetwarzania może być prowadzony w formie elektronicznej. Musi on zawierać co najmniej:

- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych i ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Przykładowy wzór rejestru czynności przetwarzania znajduje się w załączeniu Przewodnika.

Dokumentacja i obsługa w przypadku naruszenia ochrony danych osobowych

Jednym z najważniejszych obowiązków, jakie wprowadza RODO, jest obowiązek poinformowania Prezesa Urzędu Ochrony Danych Osobowych o wykrytym naruszeniu.

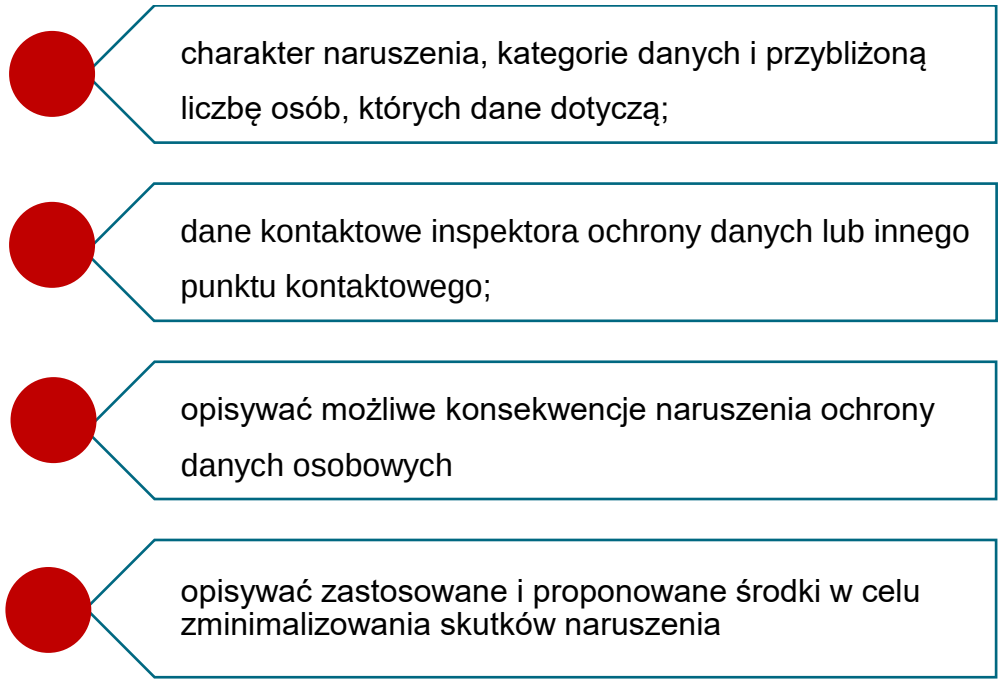
Nie wszystkie incydenty podlegają jednak obowiązkowi zgłoszenia. Zgłosić należy incydenty dotyczące naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Z tego obowiązku zwolnione są również incydenty, w przypadku których jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Zgłoszeniu do organu nadzorczego nie będą podlegały takie incydenty jak:

- **zgubienie teczki lub laptopa z dokumentami zawierającymi dane osobowe, jeśli teczka została odnaleziona;**
- **przypadkowy kontakt klienta z dokumentem zawierającym dane osobowe innej osoby,**
- **pozostawienie dokumentu w widocznym miejscu w samochodzie.**

Na zgłoszenie przewidziano 72 godziny od wykrycia incydentu, a jeżeli dokonuje się go po tym terminie, dołączyć należy również wyjaśnienie przyczyn opóźnienia.

Zgłoszenie powinno zawierać:



Informacje o wykrytym incydencie przekazywane są przez administratora do odpowiedniego organu nadzorczego, jak również do osób, których dane dotyczą.

W przypadku, gdy serwis jest podmiotem przetwarzającym, informację o incydencie powinien przekazać administratorowi danych (producentowi).

Wzór zgłoszenia znajduje się pod adresem: https://uodo.gov.pl/pl/134/233

ORGAN NADZORU

Administrator nie jest zobowiązany do dokonywania zgłoszenia do organu nadzoru, jeżeli mało prawdopodobne jest, aby naruszenie mogło powodować ryzyko naruszenia praw i wolności osób fizycznych.

Jeżeli jednak ryzyko takie wystąpi, **administrator powinien zgłosić naruszenie w ciągu 72 godzin.**

OSOBA KTÓREJ DANE DOTYCZĄ

W przypadku, gdy naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator jest zobowiązany bez zbędnej zwłoki powiadomić o tym osobę, której dane dotyczą.

Powyższy obowiązek nie dotyczy sytuacji, gdy:

administrator wdrożył odpowiednie techniczne oraz organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczyło naruszenie.

Czy jest się czego bać?
Sankcje, roszczenia, ryzyko biznesowe

RODO przewiduje możliwość nakładania przez organ nadzoru kar finansowych obok lub zamiast innych sankcji. Organy nadzoru są zobowiązane do zapewnienia, aby wymierzane administracyjne kary pieniężne były „skuteczne i odstraszające".

SANKCJE

W RODO przewidziano szeroki katalog sankcji, które mogą być nałożone na administratorów danych osobowych. Wśród sankcji administracyjnych w RODO wskazano w szczególności:

- wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania;
- udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania;
- nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
- nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;

- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
- nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
- nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

KARY PIENIĘŻNE

Oprócz środków wskazanych powyżej organ nadzorczy może nałożyć administracyjne kary pieniężne. W RODO przewidziano dwie kategorie kar, które różnią się między sobą ich wysokością maksymalną. Wśród administracyjnych kar pieniężnych występują kary pieniężne w wysokości do 10 000 000 euro lub do 2% całkowitego, rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Do tej kategorii należy np. takie przewinienie jak niedopełnienie obowiązku zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowy. W innych przypadkach organ nadzorczy może nałożyć karę pieniężną w wysokości do 20 000 000 mln euro lub do 4% całkowitego, rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Karę w tej wysokości organ nadzorczy może nałożyć w szczególności w przypadku naruszenia podstawowych zasad przetwarzania, w tym warunków uzyskania zgody lub naruszenia praw osób, których dane dotyczą.

Nałożenie kary administracyjnej nie zawsze będzie jedynym możliwym do nałożenia środkiem. Mogą bowiem zaistnieć sytuacje, w których naruszenie będzie „niewielkie” i nie będzie się wiązać z dużym ryzykiem dla praw lub wolności osób, których dane są przetwarzane. Wówczas organ nadzorczy będzie mógł zastąpić karę pieniężną upomnieniem. Decyzja dotycząca wyboru środka będzie jednak należeć do organu. „Upomnienie” to tylko możliwość, a nie obowiązek organu, nawet w przypadku niewielkich naruszeń. Niemniej jednak w przypadku osób fizycznych organ będzie musiał zbadać, czy kara pieniężna nie stanowi zbyt dużego obciążenia i w przypadku takiej nieproporcjonalności zastosować „upomnienie”.

Ustalając karę organ zwraca uwagę na:

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, jak również liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
- umyślny lub nieumyślny charakter naruszenia;
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego;
- wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;

- stopień współpracy z organem nadzoru;
- kategorie danych osobowych, których dotyczyło naruszenie;
- sposób, w jaki organ nadzoru dowiedział się o naruszeniu;
- jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki – przestrzeganie tych środków;
- wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

ROSZCZENIA OSÓB FIZYCZNYCH

W ramach RODO przewidziano również możliwość dochodzenia roszczeń przez osoby, które poniosły szkodę w wyniku naruszenia przepisów RODO. Osoby fizyczne będą mogły wystąpić z roszczeniem do sądu wobec administratora danych lub podmiotu przetwarzającego. Powyższe dotyczy zarówno szkody materialnej, jak i niematerialnego uszczerbku. Administrator danych osobowych będzie mógł się w takim przypadku bronić, w szczególności wykazując, że nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

Sprawdź, czy jesteś przygotowany: lista informacji i dokumentów do przygotowania w związku z RODO

Co zrobić, przygotowując się do RODO?

- ✓ Zrób audyt przetwarzania danych osobowych w swojej organizacji, aby wiedzieć, z jakimi danymi masz do czynienia, w jakich systemach są przetwarzane, gdzie i jakie „stare dane" są przechowywane itp.
- ✓ Stwórz Regulamin dla pracowników, który w szczególności będzie zawierać:
  - Opis realizacji żądań osób, których dane dotyczą np. żądania usunięcia danych
  - Opis zarządzania incydentami, w tym spełnienia obowiązku poinformowania o incydencie
  - Postanowienia dotyczące retencji danych – ile czasu dane mogą być przetwarzane/przetrzymywane przez serwis
- ✓ Opracuj wzór rejestru czynności przetwarzania danych osobowych, o ile będzie obowiązkowy
- ✓ Zrealizuj obowiązek informacyjny

Co zrobić w zakresie zabezpieczenia danych?

- ✓ Sprawdź, czy dane w systemach informatycznych są należycie zabezpieczone. W szczególności – czy jest zainstalowane odpowiednie oprogramowanie zapewniające ochronę przed nieuprawnionym dostępem (np. antywirus, firewall) i czy jest ono aktualizowane
- ✓ Sprawdź, czy istnieje możliwość dostępu do danych przechowywanych w postaci materialnej przez osoby nieuprawnione

Przykładowe wzory

Wejście w życie RODO skutkuje koniecznością opracowania lub aktualizacji wzorów klauzul informacyjnych oraz zgód. Poniżej przedstawiamy ich przykłady, które po odpowiednim dostosowaniu do stanu faktycznego mogą być stosowane w praktyce serwisów.

Wzór klauzuli informacyjnej

Poniższy wzór dotyczy obowiązku informacyjnego wymaganym przy wspomnianym pozyskiwaniu (art. 13 RODO).

1. Administratorem Pani/Pana danych osobowych jest Serwis ABC Sp. z o. o. (dalej: „ABC")
2. Dane osobowe będą przetwarzane w celu zawarcia i realizacji umowy o naprawę sprzętu na podstawie art. 6 ust. 1 lit. b RODO.
3. ABC będzie przetwarzać następujące dane:
    - Imię i nazwisko
    - Data urodzenia
    - Dane adresowe
    - Numery telefonów
4. Odbiorcami danych osobowych są: pracownicy i współpracownicy ABC, zewnętrzna firma księgowa, technicy.
5. Dane osobowe przechowywane będą przez okres 10 lat.
6. Przysługuje Pani/Panu żądanie dostępu do Pani/Pana danych osobowych, ich zmiany, usunięcia lub przenoszenia, a także prawo do ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania. Przysługuje Pani/Panu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Wzór upoważnienia

Upoważnienie do przetwarzania danych dla pracownika

Niniejszym, działając w imieniu Serwisu ABC, upoważniam:

Imię i nazwisko upoważnionej osoby (dalej „Pracownik”)	Dane osobowe objęte zakresem upoważnienia	Data nadania upoważnienia
[●]	1. Dane osobowe Klientów (imię i nazwisko) 2. Dane osobowe innych pracowników / współpracowników *[Zalecamy każdorazowe dostosowywanie zakresu danych w upoważnieniu do danego pracownika. Możliwe, że zakres niezbędnych w upoważnieniu danych będzie różny, będzie zależny m. in. od obejmowanego stanowiska itp.]*	Upoważnienie jest ważne do czasu zakończenia stosunku pracy lub odwołania.

Pracownik przetwarza dane wyłącznie w zakresie niezbędnym do wykonania obowiązków wynikających z Umowy o pracę, lub po otrzymaniu polecenia ABC lub innego pracownika/współpracownik (w formie pisemnej, w tym elektronicznej).

Pracownik jest zobowiązany do zachowania w ścisłej tajemnicy wszelkich informacji stanowiących dane osobowe, w szczególności dane o wrażliwym lub poufnym charakterze należące do ABC, do których będzie miał dostęp w ramach wykonywania niniejszej umowy. Pracownik zobowiązuje się przestrzegać regulaminów i polityk ABC dotyczących przetwarzania danych osobowych.

_____

PODPIS

Wzory zapisów Regulaminu przechowywania dokumentów i elektronicznych nośników zawierających dane osobowe

1. Nośniki zawierające dane osobowe przechowywane są po godzinach pracy w zamykanych na klucz szafach/pomieszczeniach. Pomieszczenia wchodzące w skład obszaru, o którym mowa powyżej, zamykane są po godzinach pracy na klucz.
2. Osoby upoważnione zobowiązane są do przechowywania kluczy do szaf służących przechowywaniu nośników danych osobowych w sposób uniemożliwiający dostęp do tych kluczy przez osoby nieupoważnione do przetwarzania danych osobowych.
3. Część dokumentacji przechowywana jest w wyznaczonym w tym celu archiwum, znajdującym się w pomieszczeniu biurowym nr [●].
4. Pracownicy zobowiązani są do okresowego archiwizowania dokumentów zawierających dane osobowe. Archiwizacja odbywa się poprzez przekazanie dokumentów osobom wyznaczonym w serwisie [●], które zobowiązane są przetransportować dokumenty do [np. wykorzystywanego archiwum zewnętrznego].
5. Pracowników obowiązuje zasada czystego biurka i zasada czystej drukarki dla zminimalizowania zagrożenia uzyskania dostępu do danych osobowych przez osoby nieupoważnione. Pracownicy upoważnieni do przetwarzania danych w [●] zobowiązane są do pracy z dokumentami stanowiącymi nośnik danych osobowych w taki sposób, by na stanowisku pracy znajdowały się w danym momencie wyłącznie te dokumenty, które są wykorzystywane w realizacji bieżącego zadania. Po zakończeniu realizacji zadania oraz po godzinach pracy dokumenty zawierające dane osobowe umieszcza się w zamykanych na klucz szafach/pomieszczeniach lub pomieszczeniach archiwum.
6. Osoby upoważnione korzystające ze wspólnych urządzeń drukujących, drukując dokumenty stanowiące nośniki danych osobowych, zobowiązane są do drukowania tych dokumentów w mniejszych partiach oraz niepozostawiania tych dokumentów po wydruku na podajniku urządzenia drukującego.
7. Zawsze należy blokować stację roboczą przy opuszczaniu stanowiska pracy. Należy zadbać, aby komputer miał ustawiony automatyczny wygaszacz ekranu, który po upłynięciu krótkiego czasu bezczynności blokuje dostęp do danych, jakie się na nim znajdują. Należy dopilnować, aby wznowienie pracy na komputerze było możliwe dopiero po wpisaniu hasła dostępu.
8. Przystępując do pracy z systemem informatycznym, pracownik zobowiązany jest do zweryfikowania, w miarę posiadanej wiedzy i istniejących możliwości, stanu zabezpieczeń stacji roboczej oraz systemu informatycznego. Rozpoczęcie pracy z systemem informatycznym następuje poprzez uruchomienie stacji roboczej oraz przeprowadzenie operacji logowania poprzez wprowadzenie identyfikatora użytkownika (pracownika) oraz hasła dostępu.
9. Pracownik zobowiązany jest do dokonania blokady stacji roboczej w przypadku tymczasowego zaprzestania pracy z systemem informatycznym połączonego z opuszczeniem stanowiska pracy oraz w każdym przypadku, gdy zachodzi niebezpieczeństwo uzyskania przez osoby nieupoważnione wglądu w wyświetlone na monitorze dane osobowe. Blokada stacji roboczej następuje poprzez zastosowanie kombinacji klawiszy ctrl+alt+del lub „flag button"+ L (dla MS Windows). Odblokowanie stacji roboczej następuje po wprowadzeniu identyfikatora użytkownika oraz hasła dostępu.
10. Zakończenie pracy z systemem informatycznym odbywa się poprzez zamknięcie wszelkich uruchomionych programów i aplikacji oraz przeprowadzenie operacji wylogowania.
11. Monitory urządzeń służących do przetwarzania danych osobowych znajdujące się w pomieszczeniach, do których dostęp mają osoby nieupoważnione, winny być ustawione w sposób uniemożliwiający tym osobom uzyskanie wglądu do wyświetlanych danych osobowych.

Wzór rejestru czynności przetwarzania

Rejestr czynności przetwarzania Serwisu ABC

Nazwa czynności przetwarzania	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa podmiotu przetwarzającego i dane kontakowe** *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1** *(jeżeli jest to możliwe)*
	Art. 30 ust. 1 pkt b	**Art. 30 ust. 1 pkt c**	**Art. 30 ust. 1 pkt c**	**Art. 30 ust. 1 pkt f**	**Art. 30 ust. 1 pkt d**	**Art. 30 ust. 1 pkt d**	**Art. 30 ust. 1 pkt g**
Realizacja naprawy	Przetwarzanie jest niezbędne dla zrealizowania zlecenia o naprawę sprzętu.	Klienci	Imię i nazwisko, adres zamieszkania lub pobytu, numer telefonu, adres e-mail.	10 lat od czasu zakończenia naprawy.	Nie dotyczy.	Pracownicy działu obsługi klienta, technik.	Zastosowano pseudonimizację i szyfrowanie danych Zapewniono zdolność szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego Zapewniono zdolność do ciągłego zapewnienia poufności, integralności dostępności i odporności systemów i usług przetwarzania Zapewniono testowanie, mierzenie, ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania