Grupa PPF

Polityka Ochrony Danych

SPIS TREŚCI

Wstęp

Zasady unijne dotyczące ochrony danych zmieniają się wraz z nowymi ramami regulacyjnymi. Ogólne rozporządzenie o ochronie danych (**RODO**) ma na celu zrewidowanie niektórych wymogów w zakresie ochrony danych i wprowadzenie szerszych praw dla osób, których dane dotyczą, nowych obowiązków w zakresie rozliczalności dla przedsiębiorstw oraz stałych ograniczeń w zakresie międzynarodowego przekazywania danych.

W ramach odpowiedzialności społecznej Grupa PPF zobowiązuje się do przestrzegania międzynarodowych przepisów dotyczących ochrony danych. Niniejsza polityka ochrony danych („**Polityka Ochrony Danych**") oparta jest na ogólnie przyjętych, podstawowych zasadach ochrony danych. Zapewnienie ochrony danych jest podstawą wiarygodnych relacji biznesowych, a zgodne z prawem i prawidłowe przetwarzanie danych osobowych przez Grupę PPF jest niezwykle ważne dla sukcesu jej działalności.

W celu prowadzenia swojej działalności Grupa PPF musi gromadzić dane osobowe dotyczące osób, z którymi współpracuje. Do takich osób należą pracownicy (obecni, byli i przyszli), klienci, dostawcy i inni kontrahenci. Przedmiotowe informacje obejmują zasadniczo imię i nazwisko, adres, adres e-mail, w przypadku pracowników: datę urodzenia, liczbę dzieci, stan cywilny, numer ubezpieczenia społecznego i numer identyfikacji podatkowej, nazwisko panieńskie matki itp., zgodnie z wymogami prawa. Bez względu na to, w jaki sposób powyższe dane osobowe są gromadzone, zapisywane i wykorzystywane (np. na komputerze lub innych nośnikach cyfrowych, w formie drukowanej, na papierze lub w formie obrazów), muszą one być przetwarzane w sposób prawidłowy, aby zapewnić zgodność z podstawowymi zasadami prawa.

Niniejsza Polityka Ochrony Danych obowiązuje w stosunku do wszystkich spółek należących do Grupy PPF (każda z nich: „**PPF**") oraz ich pracowników. Niniejsza Polityka Ochrony Danych dotyczy wszelkiego przetwarzania danych osobowych. Dane zanonimizowane, np. w przypadku ocen lub badań statystycznych, nie podlegają niniejszej Polityce Ochrony Danych.

Polityka Ochrony Danych składa się z następujących trzech części:

- **Podstawowe zasady dotyczące danych:** Rozdział 2 opisuje ogólne zasady, których PPF musi przestrzegać przetwarzając dane osobowe (np. ograniczenie celu, minimalizacja danych, prawidłowość itp.)

- **Rozliczalność:** PPF musi na bieżąco wdrażać środki w celu wykazania zgodności. Jest to nowy wymóg wynikający z RODO. W Rozdziale 3 opisaliśmy środki, które PPF musi wdrożyć, aby stać się organizacją, którą można rozliczyć za ochronę prywatności (np. prowadzenie szkoleń, prowadzenie ewidencji czynności w zakresie przetwarzania danych, wdrożenie polityki ochrony danych itp.).

- **Sankcje**: jedną z kluczowych zmian wynikających z RODO są sankcje, które mogą zostać nałożone w przypadku naruszenia zasad ochrony danych. W Rozdziale 4 wyjaśniamy podstawowe kwestie dotyczące nowych sankcji.

Niniejsza Polityka Ochrony Danych obejmuje uznane na poziomie międzynarodowym zasady ochrony danych bez zastępowania istniejących przepisów krajowych. Stanowi ona uzupełnienie krajowych przepisów dotyczących ochrony danych i krajowych polityk prywatności. Odpowiednie przepisy prawa krajowego i polityki prywatności będą miały pierwszeństwo w przypadku, gdy będą one sprzeczne z Polityką Ochrony Danych lub w przypadku, gdy będą miały bardziej rygorystyczne wymogi niż przewidziane w Polityce Ochrony Danych. PPF odpowiada za zgodność z Polityką Ochrony Danych i zobowiązaniami prawnymi, mając na uwadze powyższe reguły kolizyjne.

Zgodność z Polityką Ochrony Danych i obowiązującymi przepisami dotyczącymi ochrony danych jest regularnie sprawdzana w drodze audytów ochrony danych i innych kontroli.

Zarządy spółek z Grupy PPF są odpowiedzialne za przetwarzanie danych w obszarze swojej odpowiedzialności. W związku z tym są one zobowiązane do zapewnienia zgodności z wymogami prawnymi w zakresie ochrony danych i wymogami zawartymi w Polityce Ochrony Danych. Zarządy są również odpowiedzialne za zapewnienie środków organizacyjnych, kadrowych i technicznych, tak by wszelkie czynności przetwarzania danych odbywały się zgodnie z przepisami o ochronie danych. Aby spełnić ten wymóg, Grupa PPF będzie dokonywać corocznego przeglądu informacji o ochronie danych osobowych. W razie potrzeby zobowiązuje się do modyfikowania ogłoszenia o ochronie danych oraz zgody osób, których dane dotyczą. Przegląd dokumentacji jest koordynowany przez menedżerów HR lokalnie, z udziałem wszystkich odpowiednich działów i pracowników.

Wszelkie pytania dotyczące RODO oraz sposobu, w jaki PPF będzie zobowiązana do stosowania się do niniejszej Polityki Ochrony Danych można kierować do Osoby Odpowiedzialnej za Ochronę Danych. Jeżeli mają Państwo jakieś pytania, można się z nami skontaktować pod adresem: dataprivacy@ppfeurope.com.

1. WSTĘP

1.1 Jakie są przepisy dotyczące ochrony danych i kiedy mają zastosowanie?

W lokalizacjach, w których Grupa PPF prowadzi działalność główne obowiązujące przepisy dotyczące ochrony danych i prywatności to:

- Lokalne regulacje prawne dotyczące ochrony danych
- Unijne Ogólne rozporządzenie o ochronie danych 679/2016 (RODO) (obowiązujące od 25 maja 2018 r.)

Przepisy dotyczące ochrony danych obowiązują przy przetwarzaniu:

- danych osobowych w sposób w całości lub w części zautomatyzowany; lub
- danych osobowych, które stanowią część zbioru danych (lub gdy dane mają stanowić część zbioru danych).

Kluczowymi terminami są „dane osobowe", „przetwarzanie", „zautomatyzowanie" i „zbiór danych".

1.2 Czym są dane osobowe?

Dane osobowe są bardzo szerokim pojęciem (patrz ramka).

Nawet jeśli informacje same w sobie nie pozwalają na zidentyfikowanie osoby, której dotyczą, mogą nadal być kwalifikowane jako dane osobowe.

Dane osobowe to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, które samodzielnie lub w połączeniu z innymi informacjami, identyfikują daną osobę. Osoba możliwa do zidentyfikowania to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub co najmniej jeden znak szczególny związany z jej tożsamością fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną.

Ma to miejsce na przykład, gdy informacje:

- są wykorzystywane w celu oceny, traktowania w określony sposób lub wpływania na status lub postępowanie danej osoby; lub
- mogą mieć wpływ na prawa i interesy danej osoby.

Jeżeli dane osobowe zostały zakodowane, spseudonimizowane lub zaszyfrowane, w większości przypadków nadal stanowią dane osobowe. Dane osobowe przestają być danymi osobowymi, jeśli zostały zanonimizowane tak, że technicznie niemożliwe jest powiązanie zanonimizowanych danych z osobą, której dotyczą.

Dane osobowe nie są ograniczone do danych dotyczących życia prywatnego osoby (np. prywatny adres domowy). Dane dotyczące życia zawodowego osoby fizycznej mogą również kwalifikować się jako dane osobowe (np. bezpośredni numer telefonu w biurze).

Przykładami informacji, które w zależności od okoliczności mogą stanowić dane osobowe, są:

- Szczegółowe informacje dotyczące wynagrodzenia pracownika i rachunku bankowego wprowadzonego do jednego z systemów informatycznych
- Wiadomość e-mail o incydencie z udziałem pracownika, zawierająca jego imię i nazwisko
- Notatnik przełożonego zawierający informacje o pracowniku.

Przykładami informacji, które w zależności od okoliczności najprawdopodobniej nie będą stanowić danych osobowych, są:

- Raport porównawczy dotyczący wyników różnych kampanii, niezawierający żadnych szczegółów dotyczących poszczególnych osób
- Raport na temat wyników rozmów przeprowadzonych z odchodzącymi pracownikami, jeśli wszystkie odpowiedzi są zanonimizowane i niemożliwe jest przypisanie wyników do poszczególnych osób.

Niektóre kategorie wrażliwych danych osobowych są objęte specjalną ochroną. Wrażliwe dane osobowe obejmują dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, lub przynależność do związków zawodowych oraz przetwarzanie dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczących stanu zdrowia, życia seksualnego lub orientacji seksualnej osoby fizycznej.

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

Przykładem wrażliwych danych osobowych byłoby odniesienie się do faktu, że pracownik pracuje na pół etatu z przyczyn medycznych z powodu kontuzji stopy.

Przetwarzanie wrażliwych danych osobowych jest zasadniczo zabronione, z wyjątkiem przetwarzania na ściśle określonych warunkach, np. gdy jest to niezbędne do ochrony żywotnych interesów danej osoby, gdy osoba fizyczna wyraziła zgodę na przetwarzanie lub przetwarzanie jest konieczne na potrzeby obrony roszczeń prawnych.

Załącznik 1 do niniejszej Polityki Ochrony Danych zawiera łatwy w użyciu schemat, który pomaga określić, czy dane stanowią dane osobowe.

1.3 Czym jest przetwarzanie?

Termin przetwarzanie jest zdefiniowany bardzo szeroko (patrz ramka).

Większość czynności podejmowanych przez spółkę w odniesieniu do danych osobowych będzie stanowiło przetwarzanie, na przykład:

- Prowadzenie akt osobowych
- Monitoring CCTV (chyba że system CCTV działa na obszarze, który jest niedostępny dla osób fizycznych)
- Prowadzenie bazy danych CRM z danymi osób kontaktowych klientów PPF

- Przesyłanie biuletynów na adresy e-mail powiązane z konkretną osobą (np. jan.kowalski@firma.pl)

- Przechowywanie danych osobowych na serwerze

1.4 Czym jest „zautomatyzowanie" i „zbiór danych"?

Zautomatyzowanie zasadniczo odnosi się do systemów informatycznych (serwerów, sieci, komputerów stacjonarnych, laptopów, tabletów, smartfonów, kamer CCTV itp.).

W związku z powyższym każdorazowe wykorzystanie systemu informatycznego do przetwarzania danych osobowych stanowi przetwarzanie i podlega przepisom dotyczącym ochrony danych. Przepisy dotyczące ochrony danych mają zastosowanie, nawet jeśli dane osobowe są wykorzystywane wyłącznie w papierowym zbiorze.

Na przykład plik zatytułowany „Urlop Pracowników" zawierający alfabetyczne przekładki prawdopodobnie będzie stanowić zbiór danych, a przepisy o ochronie danych będą miały do niego zastosowanie.

1.5 Kto kontroluje dane osobowe?

Przepisy o ochronie danych rozróżniają „administratorów" i „podmioty przetwarzające".

Administrator określa *cele i sposób* przetwarzania danych osobowych. Może to robić samodzielnie lub wspólnie z innymi organizacjami. Oznacza to, że administrator sprawuje ogólną kontrolę nad tym, dlaczego i w jaki sposób dane są przetwarzane.

Aby ustalić, czy jesteś administratorem, należy określić, która organizacja podejmuje decyzję:

- o gromadzeniu danych osobowych i podstawie prawnej ich gromadzenia;

- jakie dane osobowe gromadzić, tj. treść danych;

- o celu lub celach, w których dane mają być wykorzystywane;

- w odniesieniu do których osób gromadzić dane;

- czy ujawnić dane, a jeśli tak, komu;

- czy ma zastosowanie prawo dostępu przysługujące osobie, której dane dotyczą oraz inne prawa przysługujące osobom albo czy mają zastosowanie wyłączenia; oraz

- jak długo przechowywać dane lub czy wprowadzić nierutynowe zmiany w danych.

Zbiór danych oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Powyższe decyzje mogą być podjęte wyłącznie przez administratora w ramach ogólnej kontroli nad przetwarzaniem danych.

Zgodnie z warunkami umowy z administratorem i jego umową, podmiot przetwarzający może podjąć decyzję:

- jakie systemy informatyczne lub inne metody będą wykorzystywane w celu gromadzenia danych osobowych;

- w jaki sposób przechowywać dane osobowe;

- o szczegółach zabezpieczeń związanych z danymi osobowymi;

- o środkach wykorzystywanych do przesyłania danych osobowych pomiędzy organizacjami;
- o środkach stosowanych do pobierania danych osobowych dotyczących określonych osób;
- o sposobie zapewniania przestrzegania harmonogramu przechowywania danych; oraz
- o środkach używanych do usuwania danych lub dysponowania nimi.

Powyższe wykazy nie są wyczerpujące, lecz wskazują różnice pomiędzy rolami administratora i podmiotu przetwarzającego. Wskazują one, że podmiot przetwarzający ma swobodę w wykorzystywaniu swojej wiedzy technicznej w zakresie podejmowania decyzji o tym, jak wykonywać określone czynności w imieniu administratora. Nie może jednak podjąć żadnej nadrzędnej decyzji, na przykład decyzji o celu wykorzystywania danych osobowych bądź o ich treści. Takie decyzje może podejmować wyłącznie administrator.

1.6 Dlaczego rozróżnienie pomiędzy „administratorami" a „podmiotami przetwarzającymi" jest ważne?

Obowiązki w zakresie ochrony danych, które mają zastosowanie do administratorów danych i podmiotów przetwarzających nie są tożsame.

Na administratorów często nałożonych jest więcej obowiązków wynikających z przepisów o ochronie danych niż na podmioty przetwarzające. Na przykład, gdy podmiot przetwarzający wykryje naruszenie ochrony danych, zobowiązany jest poinformować o tym administratora, a administrator danych może być zobowiązany do powiadomienia o naruszeniu organy ochrony danych osobowych (a czasami nawet osoby, których naruszenie dotyczy).

Ponadto administratorzy i podmioty przetwarzające muszą zawrzeć pisemną umowę stanowiącą, że podmiot przetwarzający:

- będzie przetwarzał dane wyłącznie na polecenie administratora;
- zobowiąże do zachowania poufności pracowników podmiotu przetwarzającego i zaangażowanych przez niego podwykonawców;
- zapewni, że nie udostępni danych osobom trzecim, z wyjątkiem podwykonawców upoważnionych przez administratora;
- podejmie wszelkie odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiedni w odniesieniu do ryzyka;
- będzie korzystać z usług podwykonawcy wyłącznie, jeżeli administrator udzieli uprzedniej (szczegółowej lub ogólnej) zgody na piśmie, nakładając jednocześnie na podwykonawcę takie same obowiązki w zakresie ochrony danych, jakie obowiązują podmiot przetwarzający;
- będzie pomagać administratorowi w wywiązywaniu się z obowiązków administratora w zakresie zapewnienia bezpieczeństwa danych, powiadamiania o zdarzeniach naruszających ochronę danych, obsługi żądań osób, których dane dotyczą oraz przeprowadzania ocen skutków dla ochrony prywatności;
- wedle decyzji administratora, usunie wszystkie dane lub zwróci je administratorowi po wygaśnięciu lub zakończeniu świadczenia usług oraz usunie istniejące kopie (chyba że wykonawca jest prawnie zobowiązany do przechowywania danych, w którym to przypadku wykonawca nie może przechowywać danych dłużej niż jest to wymagane przepisami prawa); oraz

- zaakceptuje wszelkie kontrole prowadzone przez administratora w celu weryfikacji przestrzegania przez wykonawcę umowy oraz spełnienia przez wykonawcę zobowiązań prawnych w zakresie ochrony danych.

Zwykle przy korzystaniu z danych osobowych PPF będzie kwalifikowany jako administrator. W przypadku udostępniania danych osobowych podmiotom zewnętrznym (np. zewnętrznym usługodawcom), należy sprawdzić, czy dana osoba trzecia będzie działać w charakterze administratora czy podmiotu przetwarzającego. W tym drugim przypadku podmiot zewnętrzny powinien przetwarzać dane wyłącznie w imieniu Państwa spółki i powinien zawrzeć z PPF pisemną umowę zawierającą niektóre postanowienia dotyczące ochrony danych.

Jeżeli PPF określi sposób przetwarzania wspólnie z innym administratorem, należy zawrzeć porozumienie w celu ustalenia w przejrzysty sposób odpowiedzialności poszczególnych stron w zakresie obowiązków przetwarzania, w tym w odniesieniu do osób, których dane dotyczą, w szczególności obowiązków informacyjnych (patrz pkt 2.3).

2. KLUCZOWE ZASADY OCHRONY DANYCH

Każda operacja przetwarzania danych musi być zgodna z następującymi kluczowymi zasadami ochrony danych. Dane osobowe muszą być:

1. Przetwarzane w oparciu o podstawę prawną (warunki przetwarzania)

2. Przetwarzane w ograniczonych celach (zasada ograniczania celów)

3. Przetwarzane w przejrzysty sposób w stosunku do osoby, której dane dotyczą (zasada przejrzystości)

4. Adekwatne, stosowne oraz ograniczone do danych niezbędnych do celów, w których są przetwarzane (zasada minimalizacji danych)

5. Prawidłowe i w razie potrzeby uaktualniane (zasada prawidłowości)

6. Przechowywane nie dłużej niż jest to konieczne do celów, w których są przetwarzane, a następnie niszczone lub anonimizowane (zasada ograniczenia przechowywania)

7. Przetwarzane zgodnie z prawami osób, których dane dotyczą

8. Przetwarzane w sposób bezpieczny i z zachowaniem poufności (zasada integralności i poufności)

9. Przekazywane odbiorcom spoza UE wyłącznie po spełnieniu określonych warunków

Poniżej przedstawiamy dalsze wyjaśnienie każdej z powyższych zasad.

2.1 Warunki przetwarzania

PPF może przetwarzać dane osobowe wyłącznie, gdy spełniony zostanie jeden (lub więcej) z następujących warunków:

- Osoba, której dane osobowe dotyczą, wyraziła zgodę na przetwarzanie;

- Przetwarzanie jest konieczne:

    - w związku z umową, którą dana osoba zawarła; lub

    - ponieważ dana osoba zwróciła się do PPF z prośbą o wykonanie danej czynności, by mogła zawrzeć umowę;

- Przetwarzanie jest konieczne ze względu na prawny obowiązek, który ma zastosowanie do PPF (inny niż zobowiązania wynikające z umowy);

- Przetwarzanie jest konieczne w celu ochrony „żywotnych interesów" osoby. Powyższy warunek dotyczy wyłącznie przypadków zagrożenia życia, na przykład, gdy historia medyczna danej osoby jest ujawniana szpitalowi, w którym osoba ta przebywa po ciężkim wypadku przy pracy;

- Przetwarzanie jest konieczne w celu realizacji interesu publicznego lub sprawowania władzy publicznej nadanej administratorowi danych.

- Przetwarzanie jest konieczne w związku z uzasadnionymi interesami PPF (lub dowolnej osoby trzeciej, której ujawniane są dane), wobec których charakteru nadrzędnego nie mają interesy lub prawa podstawowe osób, których dane są przetwarzane (uzasadniony interes)

Dalsze wskazówki na temat każdej z podstaw przetwarzania znajdują się w Załączniku 2.

Podstawy prawne przetwarzania wrażliwych danych osobowych są bardziej rygorystyczne, w związku z czym wrażliwe dane osobowe mogą być przetwarzane, głównie jeśli:

- Osoba, której dane dotyczą udzieliła zgody na przetwarzanie; lub

- Przetwarzanie jest konieczne w celu wywiązania się z obowiązku prawnego.

2.2 Przetwarzanie przy ograniczeniu celu (zasada ograniczenia celu)

Dane osobowe mogą być przetwarzane wyłącznie w określonych celach, o których powiadomiono osobę, której dane dotyczą w chwili zebrania danych po raz pierwszy.

Oznacza to, że dane osobowe nie mogą być gromadzone w jednym celu i wykorzystywane w innym. W przypadku konieczności zmiany celu, dla którego przetwarzane są dane, konieczne będzie poinformowanie osoby, której dane dotyczą o nowym celu przed rozpoczęciem przetwarzania, przy czym może być konieczne uzyskanie jej uprzedniej zgody.

2.3 Przejrzyste przetwarzanie (zasada przejrzystości)

Osobom należy przekazać określone informacje na temat przetwarzania ich danych osobowych. Informacje, które należy przekazać zależą od tego, czy dane osobowe zostały uzyskane bezpośrednio od osób fizycznych.

Informacje muszą być przekazywane w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny oraz być formułowane jasnym i prostym językiem. PPF nie może pobierać opłat za przekazanie przedmiotowych informacji.

Poniższa tabela zawiera zestawienie informacji, które należy przekazać osobom na danych etapach.

Jakie informacje należy przekazać?	Dane uzyskane bezpośrednio od osoby	Dane, które nie zostały uzyskane bezpośrednio od osoby
Dane identyfikacyjne i kontaktowe administratora danych i inspektora ochrony danych (jeżeli PPF wyznaczyła inspektora ochrony danych)		

Jakie informacje należy przekazać?	Dane uzyskane bezpośrednio od osoby	Dane, które nie zostały uzyskane bezpośrednio od osoby
Cel przetwarzania oraz podstawę prawną przetwarzania		
W stosownych przypadkach uzasadnione interesy administratora danych lub osoby trzeciej		
Kategorie danych osobowych		
Wszelkich odbiorów lub kategorie odbiorców danych osobowych		
Szczegółowe informacje dotyczące przekazywania danych do państw trzecich oraz zabezpieczeń		
Okres przechowywania danych oraz kryteria stosowane w celu określenia okresu przechowywania danych		
Istnienie każdego z praw osób, których dane dotyczą (prawa dostępu, poprawiania, usuwania, ograniczania przetwarzania danych osobowych itp.)		
Prawo do cofnięcia zgody w dowolnym momencie, w stosownych przypadkach		
Prawo do wniesienia skargi do organu nadzorczego		
Źródło, z którego pochodzą dane osobowe oraz czy pochodzą one z publicznie dostępnych źródeł		
Czy przekazanie danych osobowych stanowi część wymogu lub zobowiązania prawnego lub umownego oraz możliwe konsekwencje nieprzekazania danych osobowych.		

Jakie informacje należy przekazać?	Dane uzyskane bezpośrednio od osoby	Dane, które nie zostały uzyskane bezpośrednio od osoby
Istnienie zautomatyzowanego procesu podejmowania decyzji, w tym profilowania oraz informacje o sposobie podejmowania decyzji, znaczeniu i konsekwencjach.		

Poniższa tabela opisuje, kiedy PPF zobowiązana jest przekazać wyżej wskazane informacje.

	Dane uzyskane bezpośrednio od osoby	Dane, które nie zostały uzyskane bezpośrednio od osoby
Kiedy należy przekazać informacje?	W momencie uzyskania danych od osoby.	• W rozsądnym terminie od chwili uzyskania danych (w ciągu jednego miesiąca); • Jeżeli dane są używane do komunikowania się z osobą, najpóźniej w momencie pierwszego kontaktu; lub • Jeżeli przewidywane jest ujawnienie danych innemu odbiorcy, najpóźniej przed ujawnieniem danych.

2.4 Adekwatność, stosowność oraz ograniczenie do danych niezbędnych do osiągnięcia celów przetwarzania (zasada minimalizacji danych)

Zgodnie z RODO należy gromadzić wyłącznie te dane osobowe, które są potrzebne do określonych celów. Należy również upewnić się, że gromadzone dane osobowe są wystarczające do celów, w których zostały zgromadzone.

Nie należy przechowywać większej ilości danych niż jest potrzebna. Przechowywane dane nie powinny również zawierać nieistotnych informacji.

W przypadku wrażliwych danych osobowych szczególnie ważne jest, by zebrać lub zachować wyłącznie minimalną ilość potrzebnych informacji.

Jeśli potrzebne są jedynie konkretne informacje o danych osobach, należy zebrać je wyłącznie w odniesieniu do tych osób - w odniesieniu do innych osób informacje te mogą być nadmierne i nieistotne. Na przykład, pracodawca przechowuje dane dotyczące grup krwi wszystkich pracowników. Niektórzy z nich wykonują niebezpieczną pracę, a informacje te są potrzebne w razie wypadku. W przypadku pozostałej części pracowników takie informacje będą jednak prawdopodobnie nieistotne i nadmierne.

Nie należy przechowywać danych osobowych na wypadek, gdyby stałyby się one przydatne w przyszłości. Dopuszczalne jest jednak przechowywanie informacji dotyczących przewidywalnego zdarzenia, które może nigdy nie nastąpić, jak w powyższym przykładzie dotyczącym grup krwi.

2.5 Dane prawidłowe i w razie potrzeby uaktualniane (zasada prawidłowości)

RODO nakłada zobowiązania, by zapewnić prawidłowość przetwarzanych danych osobowych. O ile to konieczne, dane muszą być również uaktualniane.

Aby zachować zgodność z powyższymi przepisami, należy:

- podjąć uzasadnione kroki, aby zapewnić prawidłowość uzyskiwanych danych osobowych;
- upewnić się, że źródło danych osobowych jest jasne;
- uważnie rozważyć wszelkie wyzwania związane z prawidłowością informacji; oraz
- rozważyć, czy istnieje konieczność uaktualnienia informacji.

2.5.1 Kiedy dane osobowe są „prawidłowe" lub „nieprawidłowe"?

RODO nie definiuje terminu „prawidłowy", lecz stanowi, że dane osobowe są nieprawidłowe, jeśli są błędne lub wprowadzają w błąd co do dowolnego faktu. Zwykle jest to oczywiste, czy informacje są prawidłowe, czy też nie. Na przykład, jeśli dana osoba przeprowadziła się z Budapesztu do Pragi, zapis wskazujący, że obecnie mieszka w Budapeszcie jest oczywiście nieprawidłowy. Jednak zapis wskazujący, że osoba ta kiedyś mieszkała w Budapeszcie pozostaje prawidłowy, mimo że osoba ta już tam nie mieszka. Należy zawsze zachować jasność co do tego, co dany wpis ma wskazywać.

2.5.2 Czy dane osobowe zawsze muszą być aktualne?

To zależy od tego, do czego informacje są wykorzystywane. Jeśli informacje są wykorzystywane do celu, który opiera się na aktualności informacji, powinny one być aktualizowane. Na przykład w przypadku podwyżki dokumentacja płacowa pracownika powinna być uaktualniana.

W innych okolicznościach będzie to równie oczywiste, gdy informacje nie będą wymagały uaktualnienia.

2.5.3 Czym są „uzasadnione kroki"?

Zależy to od okoliczności, w szczególności od charakteru danych osobowych i celu ich wykorzystywania. Im ważniejsze jest zachowanie prawidłowości danych osobowych, tym większy wysiłek należy włożyć w jej zapewnienie. W związku z powyższym w przypadku wykorzystywania danych przy podejmowaniu decyzji, które mogą znacząco wpłynąć na daną osobę lub innych, należy dokładać więcej starań w celu zapewnienia ich prawidłowości. Może to wiązać się z koniecznością uzyskania niezależnego potwierdzenia prawidłowości danych. Na przykład większość pracodawców będzie musiała sprawdzić dokładne dane dotyczące wykształcenia, kwalifikacji i doświadczenia zawodowego osób ubiegających się o pracę, jeśli będzie to niezbędne w odniesieniu do konkretnego stanowiska oraz w przypadku konieczności uzyskania wiążącej weryfikacji.

2.6 Przechowywanie danych nie dłużej niż jest to konieczne do celów, w których są przetwarzane, a następnie ich niszczenie lub anonimizowanie (zasada ograniczenia przechowywania)

RODO nie określa żadnych konkretnych minimalnych lub maksymalnych okresów przechowywania danych osobowych. Zamiast tego stwierdza, że dane osobowe przetwarzane do jakiegokolwiek celu lub celów nie będą przechowywane dłużej niż jest to konieczne w związku z danym celem lub celami.

W praktyce oznacza to, że należy:

- przeanalizować okres przechowywania danych osobowych;
- rozważyć cel lub cele, dla których informacje są przechowywane, aby zdecydować, czy (i jak długo) je przechowywać;
- bezpiecznie usunąć informacje, które nie są już potrzebne do danego celu lub celów;
- aktualizować, archiwizować lub bezpiecznie usuwać informacje, jeśli staną się one nieaktualne.

2.7 Przetwarzanie danych zgodnie z prawami osób, których dane dotyczą

Osobom fizycznym przysługuje szereg praw, gdy ich dane osobowe są przetwarzane.

2.7.1 Prawo do otrzymywania informacji

Patrz Rozdział 2.3.

2.7.2 Prawo dostępu do danych osobowych

Osoby mają prawo do uzyskania:

- Potwierdzenia, że ich dane są przetwarzane;
- Dostępu do swoich danych osobowych; oraz
- Innych dodatkowych informacji - w dużej mierze odpowiadających informacjom, które powinny być zawarte w informacji o przetwarzaniu danych (patrz Rozdział 2.3).

PPF zobowiązana jest bezpłatnie przekazać kopię wspomnianych informacji. PPF może jednak pobrać „opłatę w rozsądnej wysokości”[1]:

- Gdy żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, szczególnie jeśli ma charakter ustawiczny; lub
- Aby spełnić żądania dotyczące kolejnych kopii tych samych informacji. Nie oznacza to, że dozwolone jest pobieranie opłat za wszystkie kolejne żądania dostępu.

Po otrzymaniu żądania dostępu, należy dostarczyć żądane informacje bezzwłocznie, a najpóźniej w ciągu jednego miesiąca od otrzymania przedmiotowego żądania.[2]

W przypadku, gdy żądania są w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności w związku z ich ustawicznym charakterem, PPF może:

- Pobrać opłatę w uzasadnionej wysokości, uwzględniającą administracyjne koszty udzielenia informacji; lub
- Odmówić udzielenia odpowiedzi. W przypadku odmowy udzielenia odpowiedzi na żądanie, należy wyjaśnić danej osobie przyczynę odmowy, informując ją o przysługującym jej prawie do złożenia skargi do właściwego organu nadzorczego i jej prawie do wszczęcia postępowania sądowego. PPF musi przekazać przedmiotowe informacje bez zbędnej zwłoki, najpóźniej w ciągu jednego miesiąca.

W przypadku otrzymania żądania dostępu, w pierwszej kolejności należy zweryfikować tożsamość osoby kierującej żądanie, np. prosząc osobę, której dane dotyczą o przesłanie zeskanowanej kopii dowodu tożsamości.

Jeśli żądanie zostało przesłane w formie elektronicznej, należy podać informacje w powszechnie używanym formacie elektronicznym (na przykład w formacie Word, Excel, PDF).

2.7.3 Prawo do sprostowania

Osoby mogą zwrócić się do PPF o sprostowanie ich danych osobowych przechowywanych przez PPF, jeśli dane te są nieprawidłowe lub niekompletne. Jeśli osoba zwróci się do PPF o sprostowanie

---

1 Wysokość opłaty musi wynikać z kosztów administracyjnych związanych z przekazaniem informacji.

2 Okres ten można przedłużyć o kolejne dwa miesiące w przypadku otrzymania złożonych bądź licznych żądań. W takim przypadku należy poinformować daną osobę w ciągu jednego miesiąca od otrzymania żądania i wyjaśnić, dlaczego konieczne jest wydłużenie tego okresu.

dotyczących jej danych osobowych oraz jeśli PPF ujawniła przedmiotowe dane osobom trzecim (na przykład nieprawidłowy wiek członka kadry kierowniczej wskazany w rocznym sprawozdaniu PPF), PPF musi poinformować daną osobę:

- O sprostowaniu, o ile to możliwe; oraz
- W stosownych przypadkach o osobach trzecich, którym dane zostały ujawnione.

PPF musi odpowiedzieć na żądanie sprostowania w ciągu jednego miesiąca.[3]

W przypadku braku podjęcia działań w odpowiedzi na żądanie sprostowania, należy wyjaśnić danej osobie przyczynę niepodjęcia działań, informując ją o przysługującym jej prawie do złożenia skargi do właściwego organu nadzorczego i jej prawie do wszczęcia postępowania sądowego.

2.7.4 Prawo do usunięcia danych

Prawo do usunięcia danych jest również znane jako „prawo do bycia zapomnianym". Podstawową zasadą przedmiotowego prawa jest umożliwienie danej osobie żądania usunięcia danych osobowych w przypadku, gdy nie ma istotnych powodów, by PPF kontynuowało przetwarzanie danych osobowych.

Prawo do usunięcia danych nie zapewnia całkowitego „prawa do bycia zapomnianym". Osobom fizycznym przysługuje prawo do usunięcia ich danych osobowych oraz do zapobiegnięcia ich przetwarzaniu w określonych okolicznościach:

- Gdy dane osobowe nie są już potrzebne w związku z celem, w którym PPF pierwotnie gromadziła/przetwarzała dane.
- Gdy osoba wycofa zgodę;
- Gdy dana osoba wniesie sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione interesy PPF w dalszym przetwarzaniu danych osobowych;
- Dane osobowe były przetwarzane niezgodnie z prawem;
- Usunięcie danych jest konieczne w celu wywiązania się z obowiązku prawnego;
- Dane osobowe są przetwarzane w odniesieniu do oferowania dziecku usług lub produktów za pośrednictwem Internetu.

Istnieją pewne szczególne okoliczności, w których prawo do usunięcia nie ma zastosowania, a PPF może odmówić rozpatrzenia żądania. Na przykład PPF może odmówić spełnienia żądania usunięcia danych w przypadku, gdy dane osobowe są przetwarzane z następujących powodów:

- W celu wywiązania się z obowiązku prawnego (np. gdy PPF zobowiązana jest przetwarzać dane pracowników w celu realizacji nałożonych na nią czynności zgodnie z lokalnym ustawodawstwem dotyczącym zabezpieczenia społecznego w Czechach, na Węgrzech, w Holandii, Polsce, w Słowacji, w Szwecji, we Włoszech, w Niemczech);
- W celu realizacji zadania leżącego w interesie publicznym lub w celu sprawowania władzy publicznej; lub
- Dochodzenia bądź obrony roszczeń prawnych.

2.7.5 Prawo do ograniczenia przetwarzania

[3] Jeżeli żądanie sprostowania jest złożone, powyższy termin może zostać przedłużony o dwa miesiące.

Osoby mogą zwrócić się do PPF o ograniczenie przetwarzania ich danych osobowych. Gdy przetwarzanie jest ograniczone, PPF może przechowywać dane osobowe, lecz nie może ich dalej przetwarzać. PPF może następnie zachować wystarczająco dużo informacji o osobie, w celu zapewnienia, by ograniczenie przetwarzania było przestrzegane w przyszłości.

PPF będzie zobowiązana do ograniczenia przetwarzania danych osobowych w następujących okolicznościach:

- W przypadku, gdy dana osoba zakwestionuje prawidłowość danych osobowych, PPF powinna ograniczyć przetwarzanie do czasu zweryfikowania prawidłowości danych osobowych;

- W przypadku, gdy dana osoba wniesie sprzeciw wobec przetwarzania (jeśli przetwarzanie było konieczne w celu wykonania zadania leżącego w interesie publicznym lub w celu związanym z prawnie uzasadnionymi interesami) i rozważa się, czy prawnie uzasadnione podstawy PPF są nadrzędne w stosunku do podstaw danej osoby;

- W przypadku, gdy przetwarzanie jest niezgodne z prawem, a dana osoba wniesie sprzeciw wobec usunięcia danych i zamiast tego zażąda ograniczenia przetwarzania;

- W przypadku, gdy PPF nie potrzebuje już danych osobowych, ale są one potrzebne osobie do ustalenia, dochodzenia bądź obrony roszczeń.

2.7.6 Prawo do przenoszenia danych

Prawo do przenoszenia danych umożliwia osobom uzyskanie i ponowne wykorzystanie ich danych osobowych do własnych celów w ramach różnych usług. Prawo to umożliwia łatwe przenoszenie, kopiowanie lub przesyłanie danych osobowych z jednego środowiska IT do drugiego w bezpieczny sposób, bez utrudnień w zakresie użyteczności.

Prawo do przenoszenia danych ma zastosowanie wyłącznie (po spełnieniu każdego z poniższych trzech kryteriów):

- W odniesieniu do danych osobowych przekazanych administratorowi;

- W przypadku, gdy dane są przetwarzane na podstawie zgody osoby lub w celu realizacji umowy; oraz

- W przypadku, gdy przetwarzanie odbywa się w sposób zautomatyzowany[4].

W przypadku otrzymania żądania przeniesienia danych PPF zobowiązana jest do przekazania danych osobowych w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego formacie. Formaty otwarte obejmują pliki CSV, XML lub JSON. Odczyt maszynowy oznacza, że informacje są ustrukturyzowane w taki sposób, by oprogramowanie mogło wyodrębnić określone elementy danych.

W przypadku wystosowania żądania przez daną osobę PPF może być zobowiązana do przesłania danych bezpośrednio do innej organizacji, jeśli jest to technicznie wykonalne. PPF nie musi jednak wprowadzać ani utrzymywać systemów przetwarzania, które są technicznie kompatybilne z systemami innych organizacji.

2.7.7 Prawo do sprzeciwu

Osoby mają prawo do wniesienia sprzeciwu wobec:

---

4 Patrz punkt 1.4 w celu uzyskania dalszych informacji o „sposobie zautomatyzowanym”.

- przetwarzania opartego na prawnie uzasadnionych interesach lub wykonywaniu zadania leżącego w interesie publicznym / sprawowaniu władzy publicznej (w tym profilowania);

- marketingu bezpośredniego (w tym profilowania); oraz

- przetwarzania w celach badań i statystyk naukowych/historycznych.

W jaki sposób PPF przestrzega prawa do sprzeciwu?

i) W przypadku, gdy PPF przetwarza dane osobowe w celu wykonania obowiązku prawnego lub w związku z uzasadnionymi interesami PPF

Osoby mogą zgłosić sprzeciw z „przyczyn związanych z ich szczególną sytuacją". W takim przypadku PPF musi zaprzestać przetwarzania danych osobowych, chyba że:

- Możliwe jest wykazanie istnienia ważnych, uzasadnionych prawnie podstaw przetwarzania, nadrzędnych wobec interesów, praw i wolności danej osoby; lub

- Dane są przetwarzane w celu ustalenia, dochodzenia lub obrony roszczeń.

PPF musi poinformować osoby o ich prawie do zgłoszenia sprzeciwu w chwili pierwszego kontaktu oraz w informacjach o polityce prywatności.

Powyższe musi zostać wyraźnie podane do wiadomości osoby i musi być przedstawione jasno i odrębnie od wszelkich innych informacji przekazywanych danej osobie.

ii) W przypadku, gdy PPF przetwarza dane osobowe w celu prowadzenia marketingu bezpośredniego

PPF zobowiązana jest zaprzestać przetwarzania danych osobowych do celów marketingu bezpośredniego w momencie otrzymania sprzeciwu. Nie obowiązują żadne wyjątki ani podstawy do udzielenia odmowy.

PPF zobowiązana jest rozpatrzeć sprzeciw wobec przetwarzania do celów marketingu bezpośredniego w każdym czasie oraz bezpłatnie.

PPF musi poinformować osoby o ich prawie do zgłoszenia sprzeciwu w chwili pierwszego kontaktu oraz w informacjach o polityce prywatności.

Powyższe musi zostać wyraźnie podane do wiadomości osoby i musi być przedstawione jasno i odrębnie od wszelkich innych informacji przekazywanych danej osobie.

2.7.8 Prawa związane ze zautomatyzowanym podejmowaniem decyzji, w tym profilowaniem

Przepisy dotyczące ochrony danych chronią osoby przed ryzykiem podjęcia potencjalnie szkodliwej decyzji bez interwencji ludzkiej.

Osobom przysługuje prawo do niepodlegania danej decyzji, gdy:

- Decyzja została podjęta w oparciu o zautomatyzowane przetwarzanie;

- Decyzja wywołuje skutek prawny lub w podobny sposób znacząco wpływa na daną osobę.

Przykładem powyższego może być sytuacja pracownika, którego wynagrodzenie jest bezpośrednio związane z jego produktywnością, zaś produktywność mierzona jest w sposób w pełni zautomatyzowany.

PPF zobowiązana jest zapewnić, by osoby mogły:

- Uzyskać interwencję ludzką;
- Wyrazić własne stanowisko; oraz
- Uzyskać wyjaśnienie w zakresie decyzji oraz zakwestionować daną decyzję.

Przedmiotowe prawo nie ma zastosowania, jeżeli decyzja:

- Jest niezbędna w celu zawarcia lub wykonania umowy pomiędzy PPF a daną osobą;
- Jest dozwolona przez prawo (np. do celów zapobiegania oszustwom lub unikania podatków); lub
- Opiera się na wyraźnej zgodzie.

Ponadto prawo to nie ma zastosowania, gdy decyzja nie ma prawnego lub podobnego istotnego wpływu na dowolną osobę.

Co jeszcze RODO mówi o profilowaniu?

Przepisy o ochronie danych ograniczają również „profilowanie" osób. Profilowanie to dowolna forma zautomatyzowanego przetwarzania danych, mająca na celu ocenę pewnych czynników osobowych osoby fizycznej, w szczególności analizę lub prognozowanie aspektów dotyczących na przykład jej:

- efektów pracy;
- sytuacji ekonomicznej;
- zdrowia;
- osobistych preferencji;
- wiarygodności; lub
- zachowania.

Przetwarzając dane osobowe do celów profilowania, PPF musi zapewnić odpowiednie zabezpieczenia. Takie zabezpieczenia obejmują co najmniej:

- Przekazanie osobie istotnych informacji o założeniach przetwarzania, a także o jego znaczeniu i przewidywanych konsekwencjach;
- Stosowanie odpowiednich procedur matematycznych lub statystycznych na potrzeby profilowania;
- Wdrożenie odpowiednich środków technicznych i organizacyjnych, by umożliwić skorygowanie nieprawidłowości i zminimalizowanie ryzyka błędów;
- Zabezpieczenie danych osobowych w sposób, który jest proporcjonalny do ryzyka dla interesów i praw osoby, której dane dotyczą, i zapobiega skutkom w postaci dyskryminacji osób fizycznych.

Decyzje zautomatyzowane nie mogą opierać się na przetwarzaniu wrażliwych danych osobowych, chyba że PPF uzyska wyraźną zgodę danej osoby.

2.7.9 Tryb rozpatrywania żądań osób, których dane dotyczą

W przypadku każdego żądania osoby, której dane dotyczą, związanego z prawem dostępu, sprostowania, usunięcia, ograniczenia przetwarzania i sprzeciwu wobec przetwarzania danych

osobowych, a także praw związanych z przenoszeniem danych i zautomatyzowanym podejmowaniem decyzji (w tym profilowaniem) (zob. punkty 2.7.2 do 2.7.8 powyżej), należy przestrzegać następujących wytycznych:

- Informacje należy przekazywać na piśmie oraz, w stosownych przypadkach, za pomocą środków elektronicznych;

- Informacje muszą być przekazywane bez zbędnej zwłoki, a w każdym przypadku w ciągu jednego miesiąca od otrzymania żądania;

- Jeżeli okres jednego miesiąca zostanie przekroczony zważywszy na złożoność i liczbę żądań, okres ten może zostać przedłużony o kolejne dwa miesiące, pod warunkiem że osoba, której dane dotyczą zostanie poinformowana o przedłużeniu i jego przyczynach;

- Jeśli PPF podejmie decyzję o niepodejmowaniu działań w związku z danym żądaniem, musi wyjaśnić przyczynę niepodjęcia działań osobie, której dane dotyczą bez zbędnej zwłoki, a w każdym przypadku w ciągu jednego miesiąca od otrzymania żądania;

- Informacje muszą zostać przekazane osobie, której dane dotyczą bezpłatnie (z wyjątkiem przypadków, gdy żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, np. z powodu jego ustawicznego charakteru).

2.7.10 Powiadomienie odbiorców danych osobowych

Ilekroć osoba, której dane dotyczą zwróci się do PPF o sprostowanie, usunięcie lub ograniczenie przetwarzania swoich danych osobowych (patrz punkty 2.7.3 do 2.7.5 powyżej), PPF zobowiązana jest przekazać to żądanie odbiorcom danych osobowych, chyba że jest to niemożliwe lub wymaga niewspółmiernie dużego wysiłku.

Na przykład na żądanie byłego pracownika, który zwrócił się do PPF o usunięcie jego danych osobowych, PPF musi przekazać przedmiotowe żądanie m.in.:

- Wewnętrznemu działowi księgowości PPF, jeżeli dane osobowe są przetwarzane za pomocą oddzielnej księgowej bazy danych; oraz

- Zewnętrznemu dostawcy usług chmurowych świadczącemu usługi kadrowe i / lub usługi płacowe na rzecz PPF.

PPF zobowiązana jest ujawnić listę odbiorców na żądanie osoby, której dane dotyczą.

2.8 <u>Przetwarzanie danych w sposób bezpieczny i poufny (zasada integralności i poufności)</u>

2.8.1 Obowiązek wdrożenia środków bezpieczeństwa

Dane osobowe podlegają obowiązkowi zachowania tajemnicy. Wszelkie nieuprawnione gromadzenie, przetwarzanie lub wykorzystywanie danych przez pracowników jest zabronione. Wszelkie przetwarzanie danych przez pracownika, który nie został upoważniony do ich przetwarzania w ramach swoich prawowitych obowiązków jest nieupoważnione. Pracownicy mogą mieć dostęp do danych osobowych wyłącznie, o ile jest to odpowiednie do rodzaju i zakresu wykonywanych przez nich zadań. Pracownikom zabrania się wykorzystywania danych osobowych do celów prywatnych lub komercyjnych, ujawniania ich osobom nieupoważnionym lub udostępniania ich w jakikolwiek inny sposób.

RODO wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić poziom bezpieczeństwa odpowiedni w odniesieniu do ryzyka wynikającego z przetwarzania (np. przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych). Przedmiotowe środki obejmują na przykład:

- 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.

Obowiązek ten pozostanie w mocy nawet po ustaniu zatrudnienia. Powyższe ma zastosowanie niezależnie od tego, czy dane są przetwarzane elektronicznie, czy w formie papierowej. Przed wprowadzeniem nowych metod przetwarzania danych, w szczególności nowych systemów informatycznych, należy zdefiniować i wdrożyć środki techniczne i organizacyjne w celu ochrony danych osobowych.

Kiedy środki bezpieczeństwa są odpowiednie?

RODO nie zawiera szczegółowych wytycznych dotyczących tego, kiedy środki bezpieczeństwa są odpowiednie.

Przy ustalaniu, czy środki są odpowiednie, należy wziąć pod uwagę następujące kryteria:

- Stan wiedzy technicznej i praktyk w obszarze technologii bezpieczeństwa;
- Koszty wdrożenia przedmiotowych środków;
- Charakter, zakres, kontekst i cele przetwarzania danych

Czym jest naruszenie ochrony danych?

Wszelkie naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób przez PPF lub w jej imieniu. Oznacza to, że naruszenie to coś więcej niż tylko utrata danych osobowych.

2.8.2 Obowiązek zgłaszania naruszeń ochrony danych osobowych

PPF zobowiązana jest zgłosić określone rodzaje naruszenia ochrony danych właściwemu organowi nadzoru ochrony danych, a w niektórych przypadkach także osobom, których naruszenie to dotyczy.

Oto kilka przykładów naruszenia ochrony danych:

- *Utrata lub kradzież danych lub sprzętu, na którym przechowywane są dane.* Na przykład: przed opuszczeniem biura pracownik zgrywa arkusze kalkulacyjne zawierające dane kontaktowe klientów (takie jak nazwiska, adresy e-mail i numery telefonu osób kontaktowych klientów) na pamięć USB. Po przybyciu do domu uświadamia sobie, że zgubił pamięć USB w pociągu.

- *Niewłaściwe kontrole dostępu umożliwiające nieuprawnione użycie.* Na przykład: lokalny dział zasobów ludzkich przechowywał dokumenty zawierające dane pracowników (w tym dane dotyczące wynagrodzeń itp.) na dysku publicznym. Dokumenty te były dostępne dla wszystkich pracowników PPF przez dwa tygodnie. Co najmniej dwóch pracowników PPF uzyskało dostęp do danych, a jeden z nich pobrał kopię, gdy opuszczał firmę.

- *Awaria sprzętu.* Na przykład: serwery jednego z zewnętrznych dostawców usług chmury, z którego usług korzysta PPF, zostały fizycznie zniszczone, w wyniku czego dane kilku pracowników PPF zostały utracone.

- *Błąd ludzki.* Na przykład: zewnętrzny dostawca usług płacowych przez pomyłkę przesłał dokumenty zawierające dane pracowników PPF (w tym dane dotyczące wynagrodzeń itp.) do innego klienta, nie przestrzegając zwykłej procedury przesyłania danych.

- *Atak hakerski na systemy informatyczne spółki lub systemy informatyczne obsługiwane przez zewnętrznego dostawcę usług, który przetwarza dane osobowe w imieniu spółki.* Na przykład: zewnętrzny dostawca usług chmurowych obsługujący bazę danych CRM spółki pada ofiarą ataku hakerskiego na dużą skalę.

- *Spoofing, tj. gdy informacje są uzyskiwane w drodze oszustwa.* Na przykład: pracownik zostaje oszukany klikając w link w wiadomości e-mail typu spam, co powoduje, że cała baza danych CRM zostaje skopiowana na odległość przez hakera.

PPF zobowiązana jest powiadomić właściwy organ nadzoru ochrony danych o naruszeniu, które może spowodować ryzyko w odniesieniu do praw i wolności osób. W przypadku braku podjęcia działań przedmiotowe naruszenie może mieć znaczny szkodliwy wpływ na osoby fizyczne – na przykład prowadzić do dyskryminacji, utraty reputacji, strat finansowych, naruszenia poufności lub wszelkiej innej znacznej szkody gospodarczej lub społecznej.

Należy to ocenić indywidualnie dla każdego przypadku. Na przykład PPF będzie zobowiązana powiadomić właściwy organ nadzoru ochrony danych o utracie danych klienta, w przypadku gdy w wyniku naruszenia możliwa będzie kradzież tożsamości osób fizycznych.

Dodatkowo, w przypadku, gdy istnieje wysokie prawdopodobieństwo, że naruszenie spowoduje wysokie ryzyko w odniesieniu do praw i wolności osób fizycznych, PPF zobowiązana jest powiadomić osoby, na które może to mieć bezpośredni wpływ. „Wysokie ryzyko" oznacza, że próg w zakresie powiadamiania osób fizycznych jest wyższy niż w zakresie powiadamiania właściwego organu nadzoru.

Jak zgłosić naruszenie?

W przypadku powzięcia wiadomości o naruszeniu ochrony danych osobowych, które może mieć wpływ na dane osobowe przetwarzane przez PPF lub w imieniu PPF, należy natychmiast powiadomić przełożonego oraz dział prawny.

PPF musi zgłosić naruszenia ochrony danych osobowych w ściśle określonych ramach czasowych (w ciągu 72 godzin właściwemu organowi nadzoru ochrony danych, zaś osobom, na które naruszenie ma wpływ – bezzwłocznie). W związku z powyższym wszelkie naruszenia danych osobowych, o których powzięte zostaną informacje należy zgłaszać w najszybszym możliwym terminie.

2.9 Przekazywanie danych odbiorcom spoza UE wyłącznie po spełnieniu określonych warunków

2.9.1 Czym jest przekazywanie danych?

Przekazywanie danych obejmuje:

- Przesyłanie danych osobowych z jednego kraju do danej osoby w innym kraju (na przykład: spółka zależna na Węgrzech przesyła dane kadrowe do spółki PPF w Holandii); lub

- Umożliwienie osobie z jednego kraju dostępu do danych osobowych przechowywanych w innym kraju (na przykład: PPF zezwala amerykańskiemu dostawcy usług IT na zdalny dostęp do bazy danych CRM[5] na Węgrzech z USA, w celu przeprowadzenia określonych działań w odniesieniu do danych zawartych w bazie danych CRM).

2.9.2 Przekazywanie danych w EOG

Dane osobowe mogą być swobodnie przekazywane pomiędzy podmiotami mającymi siedzibę w EOG[6]. W związku z powyższym dozwolone jest, by podmiot powiązany (np. w Czechach, Holandii, Polsce lub na Słowacji) przesyłał dane kadrowe do głównej siedziby spółki na Węgrzech (oczywiście pod warunkiem przestrzegania innych zobowiązań w zakresie ochrony danych).

2.9.3 Przekazywanie danych z UE do odbiorcy spoza EOG

Administrator może przekazywać dane osobowe wyłącznie do krajów spoza EOG (**krajów trzecich**), które zapewniają odpowiedni poziom ochrony danych. W celu podjęcia decyzji, czy dany kraj zapewnia odpowiedni poziom ochrony danych, administrator może polegać na decyzjach Komisji Europejskiej. Z zastrzeżeniem pewnych warunków Komisja UE do tej pory uznała Andorę, Argentynę, Kanadę, Wyspy Owcze, Guernsey, Izrael, Wyspę Man, Jersey, Nową Zelandię, Szwajcarię, Urugwaj.[7]

Jeżeli państwo trzecie nie zapewnia odpowiedniego stopnia ochrony danych, administrator nie może przekazywać danych osobowych żadnej osobie mającej siedzibę w tym państwie trzecim (**podmiotowi odbierającemu dane**), chyba że:

- Osoba fizyczna, poinformowana o ewentualnym ryzyku, z którym może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę;

- Przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a organizacją lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą;

- Przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, między administratorem a inną osobą;

- Przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;

- Przekazanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń. Celem niniejszego wyjątku jest ułatwienie przekazania, np. danych osobowych od podmiotu administratora posiadającego siedzibę w EOG podmiotowi administratora posiadającemu siedzibę w USA w przypadku, gdy przekazanie jest niezbędne, aby umożliwić temu drugiemu podmiotowi ustalenie lub dochodzenie roszczenia prawnego lub obronę przed roszczeniem podniesionym przez osobę trzecią. Należy pamiętać, że niniejszy wyjątek należy interpretować ściśle. Wyłączenie to nie może zatem usprawiedliwiać systematycznego przekazywania danych osobowych administratorowi posiadającemu siedzibę w USA jedynie z powodu możliwości wszczęcia postępowania sądowego w przyszłości;

- Przekazanie jest konieczne w celu ochrony żywotnych interesów osoby, której dane dotyczą lub innych osób w przypadku, gdy osoba, której dane dotyczą jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

---

5 Nawet jeśli klienci PPF są osobami prawnymi (a nie osobami fizycznymi), baza danych CRM najprawdopodobniej będzie zawierała dane kontaktowe osób pracujących dla klientów PPF. Przedmiotowe dane kontaktowe będą danymi osobowymi.

6 EOG obejmuje państwa członkowskie UE, Islandię, Liechtenstein i Norwegię.

7 Aktualna lista tak zwanych „decyzji stwierdzających odpowiedni stopień ochrony" znajduje się na stronie internetowej Komisji UE.

- Przekazanie jest dokonywane z rejestru, który zgodnie z lokalnym prawem (tj. obowiązującym w Czechach, na Węgrzech, w Holandii, w Polsce, w Słowacji, w Szwecji, we Włoszech, w Niemczech) lub prawem unijnym ma służyć za źródło informacji dla ogółu obywateli (i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes związany z dostępem do rejestru);

- Administrator i podmiot odbierający dane (działający z kolei w charakterze administratora lub podmiotu przetwarzającego w odniesieniu do przekazywanych danych osobowych) zawarli umowę zapewniającą wystarczające zabezpieczenia umowne. W dniu 4 czerwca 2021 r. Komisja wydała zmodernizowane standardowe klauzule umowne na mocy RODO dotyczące przekazywania danych od administratorów lub podmiotów przetwarzających w UE/EOG (lub w inny sposób podlegających RODO) do administratorów lub podmiotów przetwarzających mających siedzibę poza UE/EOG (i niepodlegających RODO). Kopia standardowych klauzul dostępna jest na stronie internetowej Komisji Europejskiej.

- W ramach grupy korporacyjnej wykorzystywać można również jednostronne zobowiązania (tak zwane **wiążące reguły korporacyjne**). Wiążące reguły korporacyjne to zestaw wiążących reguł, które można wdrożyć, aby umożliwić wielonarodowym grupom przesyłanie danych osobowych, które są przez nie kontrolowane z EOG do ich podmiotów powiązanych spoza EOG, zgodnie z krajowymi i unijnymi przepisami o ochronie danych. Wiążące reguły korporacyjne nie obejmują przekazywania danych osobowych poza grupę korporacyjną.

Istnieją również inne wyłączenia. Są one jednak mniej istotne dla PPF.

3. ROZLICZALNOŚĆ

3.1 Zasada rozliczalności

RODO wymaga, aby przedsiębiorstwa stały się organizacjami, które można rozliczyć za ochronę prywatności. Oznacza to, że do odpowiedzialności PPF należy nie tylko zachowanie zgodności z przepisami RODO, ale również możliwość stałego wykazania zachowania tej zgodności.

W jaki sposób można wykazać zachowanie zgodności? RODO wymaga od przedsiębiorstw wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zgodności i wykazania jej zachowania:

- Przyjęcia wewnętrznych polityk dotyczących ochrony danych (np. polityki prywatności HR)

- Organizacji szkoleń dotyczących ochrony danych dla członków personelu, którzy przetwarzają dane osobowe

- Przeprowadzania audytów wewnętrznych czynności przetwarzania

- Utrzymywania stosownej dokumentacji dotyczącej czynności przetwarzania

- W stosownych i wymaganych przypadkach, wyznaczenia inspektora ochrony danych

- Wdrożenia środków zgodnych z zasadą uwzględnienia ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Środki te mogą obejmować:

    - minimalizację danych;

    - pseudonimizację;

    - przejrzystość; oraz

    - tworzenie i stałe udoskonalanie zabezpieczeń.

- Stosowanie ocen skutków dla ochrony danych w stosownych i wymaganych przypadkach.

Poniżej przedstawione są dalsze informacje dotyczące niektórych z wyżej wskazanych środków.

3.2 Prowadzenie rejestru czynności przetwarzania

PPF jest zobowiązana do prowadzenia wewnętrznego rejestru czynności przetwarzania danych.

Wewnętrzny rejestr musi zawierać następujące informacje:

- Nazwę i szczegółowe informacje dotyczące PPF (oraz, w stosownych przypadkach, innych administratorów) oraz inspektora ochrony danych.

- Różne cele, dla których PPF przetwarza dane osobowe.

- Opis kategorii osób i kategorii danych osobowych przetwarzanych przez PPF.

- Kategorie odbiorców, którym PPF udostępnia dane osobowe (np. zewnętrzni dostawcy usług informatycznych, zewnętrzni dostawcy usług związanych z zasobami ludzkimi (headhunterzy, firmy prowadzące działalność w zakresie wyszukiwania i selekcji pracowników itp.)).

- Szczegóły dotyczące przekazywania danych do państw trzecich, w tym dokumentacja dotycząca wdrożonych mechanizmów zabezpieczających przekazywanie danych (np. stosowanie standardowych klauzul).

- Okresy przechowywania danych.

- Opis technicznych i organizacyjnych środków bezpieczeństwa na potrzeby ochrony danych.

PPF może być zobowiązana do udostępnienia przedmiotowego rejestru właściwemu organowi nadzoru ochrony danych w celach związanych z prowadzeniem dochodzenia.

3.3 Zasada uwzględniania ochrony danych w fazie projektowania oraz zasada domyślnej ochrony danych

Zasada uwzględniania ochrony danych w fazie projektowania oznacza, że na każdym etapie opracowywania nowego systemu lub procesu, który będzie wykorzystywał dane osobowe (oraz podczas całego cyklu przetwarzania danych), należy uwzględnić odpowiednie zabezpieczenia prywatności (takie jak pseudonimizacja i minimalizacja danych).

Aby określić, co jest „odpowiednie”, należy wziąć pod uwagę następujące kryteria:

- Stan wiedzy technicznej;

- Koszty wdrożenia przedmiotowych zabezpieczeń;

- Charakter, zakres, kontekst i cele przetwarzania danych. Na przykład, gdy nowy system ma przetwarzać dane osobowe na dużą skalę, zabezpieczenia prywatności będą musiały być bardziej rygorystyczne i gwarantujące lepszą ochronę, niż gdyby przetwarzanie miało bardziej ograniczony zakres.

- Ryzyka dla osób, które mogą wynikać z przetwarzania. Na przykład, gdy nowy system ma przetwarzać wrażliwe dane osobowe dotyczące osoby fizycznej, zabezpieczenia prywatności będą musiały być bardziej rygorystyczne i gwarantujące lepszą ochronę, niż gdyby przetwarzanie danych w ramach nowego systemu było mniej inwazyjne.

Zasada domyślnej ochrony danych oznacza, że gdy system daje użytkownikowi wybór co do przetwarzania jego danych, a osoba ta nie podejmuje żadnych działań w celu wyrażenia preferencji,

domyślnie system będzie przetwarzać dane osobowe w sposób najmniej naruszający prywatność. Obowiązek ten dotyczy ilości danych osobowych gromadzonych za pośrednictwem systemu, zakresu ich przetwarzania, okresu ich przechowywania i ich dostępności.

3.4 Oceny skutków dla ochrony danych

Ocena skutków dla ochrony danych (**DPIA**) (znana również jako ocena wpływu na prywatność lub PIA) to narzędzie, które może pomóc PPF w określeniu najbardziej skutecznego sposobu spełnienia wymogów w zakresie ochrony danych i spełnienia oczekiwań osób fizycznych w zakresie ochrony prywatności. Skuteczna DPIA pozwoli PPF zidentyfikować i rozwiązać problemy na wczesnym etapie, ograniczyć związane z nimi koszty oraz zaradzić naruszeniu dobrego imienia, które mogłoby w innym przypadku wystąpić.

PPF musi przeprowadzić DPIA, gdy:

- Korzysta z nowych technologii; oraz
- Istnieje prawdopodobieństwo, że przetwarzanie spowoduje wysokie ryzyko w odniesieniu do praw i wolności osób fizycznych. Oto kilka przykładów przetwarzania danych, które wiąże się z wysokim ryzykiem:
    - Systematyczna i szczegółowa ocena osób, która jest oparta na zautomatyzowanym przetwarzaniu i jest wykorzystywana do podejmowania decyzji wywołujących skutek prawny (lub w podobny sposób znacząco wpływających na osobę fizyczną);
    - Przetwarzanie wrażliwych danych osobowych na dużą skalę (np. danych medycznych lub danych osobowych związanych z wyrokami skazującymi za przestępstwa lub przestępstwami);
    - Systematyczny monitoring obszarów publicznych, prowadzony na dużą skalę (CCTV).

Każda DPIA musi zawierać:

- Opis operacji przetwarzania i celów, w tym w stosownych przypadkach, prawnie uzasadnionych interesów realizowanych przez administratora danych;
- Ocenę niezbędności i proporcjonalności przetwarzania w odniesieniu do celu;
- Ocenę ryzyka dla osób fizycznych; oraz
- Środki stosowane w celu zaradzenia ryzyku dla osób fizycznych, w tym środki bezpieczeństwa, oraz w celu wykazania zgodności z przepisami dotyczącymi ochrony danych.

4. CO SIĘ DZIEJE W PRZYPADKU BRAKU ZACHOWANIA ZGODNOŚCI?

Od 25 maja 2018 roku poziom kar pieniężnych jest znacznie wyższy. Będzie obowiązywać dwupoziomowy system administracyjnych kar pieniężnych, który będzie miał zastosowanie zarówno w stosunku do administratorów, jak i podmiotów przetwarzających.

Niektóre naruszenia (na przykład przepisów w zakresie prowadzenia dokumentacji dotyczącej przetwarzania - patrz punkt 3.2) podlegają karom pieniężnym do 10.000.000 EUR lub do 2% całkowitego rocznego światowego obrotu uzyskanego przez PPF w poprzednim roku obrotowym, przy czym zastosowanie ma kwota wyższa.

Inne naruszenia (na przykład naruszenia warunków przetwarzania/warunków uzyskania zgody) podlegają wyższym karom pieniężnym do 20.000.000 EUR lub do 4% całkowitego rocznego światowego obrotu uzyskanego przez PPF w poprzednim roku obrotowym, przy czym zastosowanie ma kwota wyższa.

Jeśli chodzi o inne rodzaje egzekwowania przepisów przez organy ochrony danych, jest to również kwestia, która obecnie znacznie różni się w poszczególnych państwach członkowskich UE w świetle obowiązujących przepisów o ochronie danych. Organy ochrony danych mają uprawnienia do interwencji, do których należą m.in. wydawanie opinii przed prowadzeniem przetwarzania, a także nakaz blokowania, usuwania i niszczenia danych. Organy ochrony danych mogą również przeprowadzać kontrole i wnosić oskarżenia o naruszenie przepisów RODO. Uprawnienia w zakresie egzekwowania prawa będą zasadniczo zharmonizowane w ramach RODO (chociaż egzekwowanie prawa karnego powierzono państwom członkowskim UE). Obejmują one uprawnienia do wydawania ostrzeżeń, nagan i poleceń administratorom danych i podmiotom przetwarzającym; nakładania tymczasowych i ostatecznych zakazów przetwarzania; zawieszania zagranicznych przepływów danych; oraz do nakazywania sprostowania lub usunięcia danych osobowych.

Sądy mogą nakazać:

- Konfiskatę wszelkich nośników zawierających dane osobowe, które zostały przetworzone;
- Sąd może nakazać PPF usunięcie wszelkich danych osobowych, w stosunku do których nastąpiło naruszenie lub może zabronić PPF przetwarzania wszelkich takich danych osobowych;
- Odpowiedzialność cywilna za szkody spowodowane naruszeniem obowiązków w zakresie ochrony danych.

Media mogą również publikować wszelkie przypadki braku zachowania zgodności z przepisami w zakresie ochrony danych, które mogą mieć znaczenie dla opinii publicznej.

5. APPROVAL, REVIEW PERIOD, MONITORING

This Policy has been reviewed, discussed and approved by PPF's Executive Committee. The Policy should be reviewed and updated regularly but at least annually.

In the event of violation of the Policy, PPF shall use all means to eliminate them and take the necessary legal and other disciplinary steps, which are allowed by the respective legal systems.

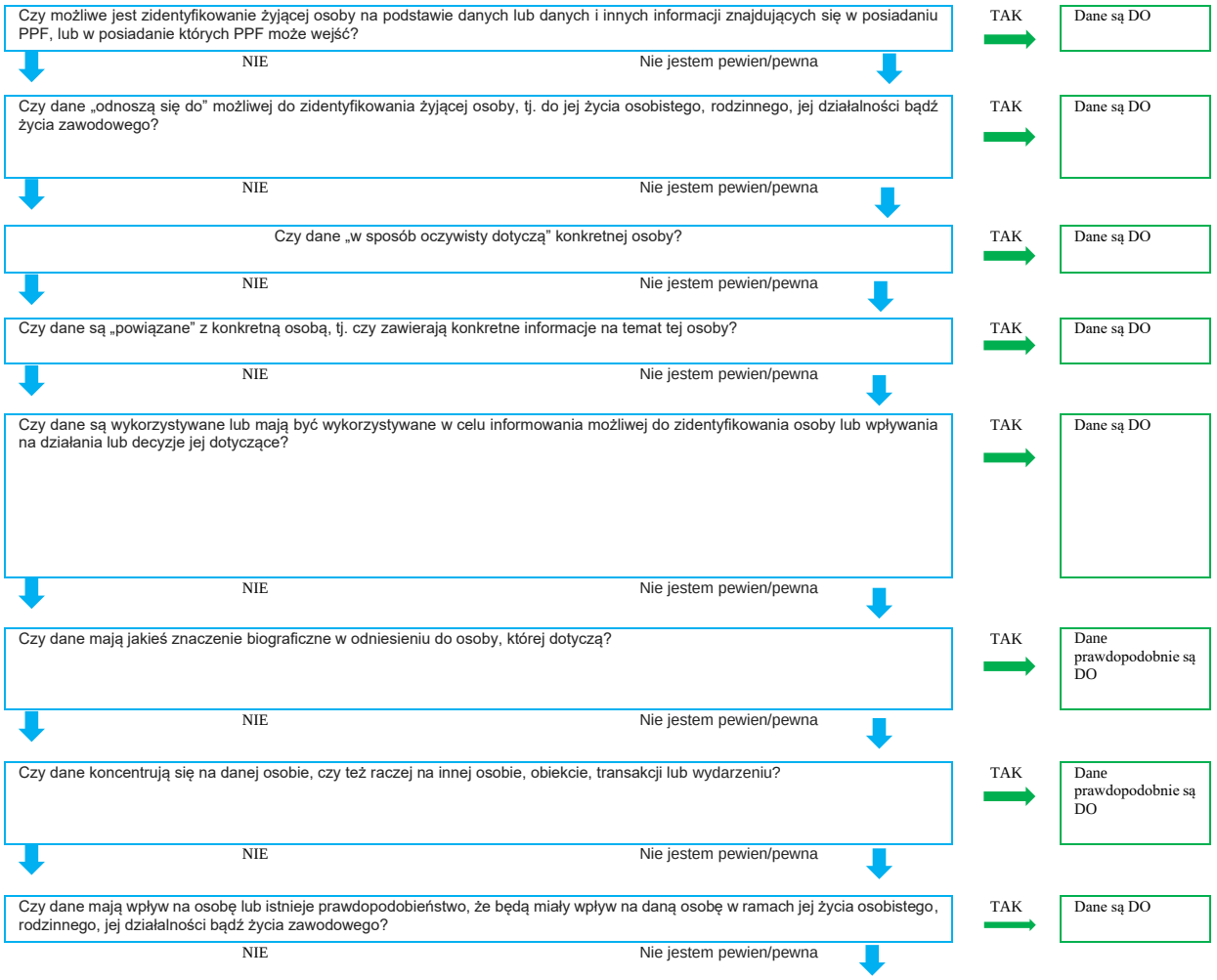
GERALD KÜHR
CEO

MARIEKE HOORNEMAN
CHIEF PEOPLE OFFICER

STÉPHANE RE
CFO

TORSTEN JACOBS
COO

ZAŁĄCZNIK 1 - SCHEMAT - CZYM SĄ DANE OSOBOWE (DO)?



Znaczenie terminu „odnoszą się do": dane, które identyfikują daną osobę nawet bez podania jej imienia i nazwiska mogą być danymi osobowymi w przypadku, gdy są przetwarzane w celu uzyskania bądź zarejestrowania informacji o tej osobie bądź w przypadku, gdy przetwarzanie tych informacji ma na tę osobę wpływ.

Przykładami danych, które „w sposób oczywisty dotyczą" konkretnej osoby są historia medyczna danej osoby, informacje o karalności lub dokumentacja dotycząca jej wyników w pracy.

Przykład: jeśli pracownik zajmuje stanowisko, które w spółce jest zajmowane tylko przez jedną osobę, informacje dotyczące wynagrodzenia związanego z tym stanowiskiem będą traktowane jako dane osobowe „powiązane" z tym pracownikiem.

Przykład: informacje na temat wartości rynkowej danego domu mogą być wykorzystywane w celach statystycznych na potrzeby określania tendencji w zakresie wartości domów na danym obszarze. Dom nie zostaje wybrany nie dlatego, że administrator nie chce uzyskać informacji o jego mieszkańcach, lecz ze względu na fakt, iż jest to dom wolnostojący z czterema sypialniami w średniej wielkości miejscowości. W momencie, gdy dane dotyczące domu:

- zostaną powiązane z daną osobą fizyczną w celu uzyskania konkretnych informacji o tej osobie (np. jej adresu); bądź
- zostaną wykorzystane przy rozważaniach na temat tej osoby bądź przy podejmowaniu decyzji na jej temat (nawet bez powiązania ich z imieniem i nazwiskiem tej osoby np. ilość prądu zużywana w domu zostanie wykorzystana na potrzeby określenia kwoty rachunku, którą właściciel domu jest zobowiązany do uiszczenia);

wówczas dane te będą stanowić dane osobowe.

Przykład: kiedy członek kierownictwa uczestniczy w posiedzeniu zarządu, jego nazwisko i stanowisko będą stanowiły dane osobowe dotyczące jego osoby. Nie oznacza to jednak, że wszystkie informacje zawarte w protokole z tego posiedzenia są danymi osobowymi każdego z uczestników.

Przykład: w przypadku, gdy prowadzona jest dyskusja, czy dana osoba byłaby odpowiednia, by wziąć udział w danym kursie lub objąć dane stanowisko (z uwzględnieniem jej kwalifikacji, osobowości i/lub wyników osiąganych w pracy), zapis przedmiotowej dyskusji będzie stanowił dane osobowe tej osoby.

ZAŁĄCZNIK 2 - DALSZE WYTYCZNE DOTYCZĄCE WARUNKÓW PRZETWARZANIA

Podstawy prawne przetwarzania danych osobowych (innych niż wrażliwe dane osobowe)	*Dalsze wskazówki*
Zgoda osoby fizycznej	Zgoda musi być dobrowolnym, konkretnym, świadomym i jednoznacznym wskazaniem woli danej osoby fizycznej. Innymi słowy, zgoda wymaga pewnej formy wyraźnej czynności potwierdzającej. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie oznaczają zgody. Zgoda musi być możliwa do zweryfikowania. Oznacza to, że należy prowadzić pewną formę dokumentacji dotyczącej sposobu i daty udzielenia zgody. Należy uzyskać oświadczenie o wyrażeniu zgody w formie pisemnej lub elektronicznej do celów prowadzenia dokumentacji. Nawiązując stosunek pracy, dane osobowe kandydatów mogą być przetwarzane za ich zgodą. Jeżeli PPF odrzuci kandydata, jego/jej dane należy usunąć z zachowaniem wymaganego okresu przechowywania, chyba że kandydat wyrazi zgodę na pozostawienie jego danych w aktach na potrzeby przyszłego procesu rekrutacyjnego. Jeśli w trakcie procedury aplikowania o pracę konieczne będzie uzyskanie informacji o kandydacie od osoby trzeciej, należy przestrzegać wymogów wynikających z odpowiednich przepisów prawa krajowego. W razie wątpliwości należy uzyskać zgodę kandydata. Osoby fizyczne mają prawo do cofnięcia zgody w dowolnym momencie. Należy pamiętać, że możliwe jest oparcie się na podstawach prawnych alternatywnych w stosunku do zgody - na przykład, gdy przetwarzanie jest niezbędne do celów związanych z prawnie uzasadnionymi interesami PPF lub osób trzecich.

Podstawy prawne przetwarzania danych osobowych (innych niż wrażliwe dane osobowe)	*Dalsze wskazówki*
Przetwarzanie jest niezbędne w celu wykonania umowy z osobą fizyczną lub podjęcia kroków w celu zawarcia umowy	Obejmuje to wyłącznie przetwarzanie, które jest bezwzględnie niezbędne w celu wykonania umowy. Fakt, że przetwarzanie danych jest związane z umową lub przewidziane w warunkach umowy niekoniecznie oznacza, że przetwarzanie jest bezwzględnie niezbędne w celu wykonania umowy. W związku z powyższym zgodnie z praktyczną zasadą należy zadać sobie pytanie: czy PPF może wykonać umowę bez przetwarzania danych? Jeśli odpowiedź brzmi „tak", przetwarzanie nie jest niezbędne w celu wykonania umowy. W ramach stosunku pracy PPF może przetwarzać dane osobowe, jeśli jest to konieczne do zawarcia, realizacji i rozwiązania umowy o pracę. Na przykład PPF musi posiadać numery rachunków bankowych swoich pracowników, aby móc wywiązywać się ze swoich zobowiązań wynikających z umów o pracę, które zawarła z pracownikami. Innymi słowy, PPF nie może wykonywać swoich zobowiązań wynikających z umów o pracę bez przetwarzania numerów rachunków bankowych pracowników. W ramach istniejącego stosunku pracy przetwarzanie danych musi zawsze odnosić się do celu umowy o pracę, jeżeli nie ma zastosowania żadna z okoliczności stanowiąca podstawę uprawnionego przetwarzania danych. PPF może przetwarzać dane osobowe odpowiednich potencjalnych klientów, obecnych klientów i partnerów w celu zawarcia, wykonania i rozwiązania umowy. Przed zawarciem umowy - na etapie jej zawierania - PPF może przetwarzać dane osobowe na potrzeby przygotowania ofert lub zamówień lub w celu spełnienia innych żądań potencjalnego klienta związanych z zawarciem umowy. PPF może kontaktować się z potencjalnymi klientami w trakcie procesu przygotowania umowy, wykorzystując dostarczone przez nich informacje. PPF zobowiązana jest do przestrzegania wszelkich ograniczeń wymaganych przez potencjalnych klientów. Do przetwarzania danych osobowych związanych ze stosunkiem pracy, które pierwotnie nie wchodziły w zakres realizacji umowy o pracę wymagane jest upoważnienie prawne.

Podstawy prawne przetwarzania danych osobowych (innych niż wrażliwe dane osobowe)	*Dalsze wskazówki*
	Upoważnieniem prawnym mogą być wymogi prawne, regulaminy zbiorowe uzgodnione z przedstawicielami pracowników, zgoda pracownika lub prawnie uzasadniony interes spółki.
Przetwarzanie jest konieczne ze względu na prawny obowiązek, który ma zastosowanie w stosunku do PPF (inny niż zobowiązania wynikające z umowy).	Niniejszy przykład dotyczy wyłącznie jasnych i konkretnych zobowiązań prawnych wynikających z prawa unijnego, prawa lokalnego (w Czechach, na Węgrzech, w Holandii, Polsce, w Słowacji, w Szwecji, we Włoszech, w Niemczech) lub prawa innego państwa członkowskiego UE. W przypadku niewiążących wytycznych (na przykład organów regulacyjnych) lub obcego (na przykład amerykańskiego) zobowiązania prawnego, należy rozważyć, czy PPF może opierać się na podstawie prawnej w postaci prawnie uzasadnionego interesu.
Przetwarzanie jest konieczne w celu ochrony żywotnych interesów osoby fizycznej.	Powyższy warunek dotyczy wyłącznie przypadków zagrożenia życia, na przykład, gdy historia medyczna danej osoby jest ujawniana szpitalowi, w którym osoba ta przebywa po ciężkim wypadku przy pracy.
Przetwarzanie jest konieczne w związku z uzasadnionymi interesami PPF (lub dowolnej osoby trzeciej, której ujawniane są dane), wobec których charakteru nadrzędnego nie mają interesy lub prawa podstawowe osób, których dane są przetwarzane.	Jeżeli PPF nie będzie w stanie polegać na żadnej z powyższych podstaw prawnych przetwarzania danych (zgoda, wykonanie umowy, zobowiązanie prawne itp.), należy rozważyć, czy PPF może polegać na podstawie prawnej w postaci prawnie uzasadnionego interesu. Uzasadnione prawnie interesy zazwyczaj mają charakter prawny (np. windykacja zaległych należności) lub komercyjny (np. unikanie naruszeń umowy). Należy zapoznać się z Załącznikiem 3 do niniejszej Polityki Ochrony Danych, który zawiera listę kontrolną, aby ustalić, czy możliwe jest oparcie się na tej podstawie prawnej w celu przetwarzania.

ZAŁĄCZNIK 3 - KIEDY MOŻNA OPIERAĆ SIĘ NA PODSTAWIE PRAWNEJ W POSTACI UZASADNIONEGO INTERESU?

Poniższe kroki mogą pomóc ocenić, czy PPF może opierać się na podstawie prawnej w postaci uzasadnionego interesu:

⇨ **Krok 1** – należy sprawdzić, czy interes jest:

- Zgodny z prawem unijnym, prawem lokalnym (w Czechach, na Węgrzech, w Holandii, Polsce, w Słowacji, w Szwecji, we Włoszech, w Niemczech) lub prawem innego państwa członkowskiego UE; oraz
- Wystarczająco jasno wyartykułowany, by umożliwić przeprowadzenie testu bilansującego z uwzględnieniem interesów i podstawowych praw osoby fizycznej (tj. wystarczająco konkretny); oraz
- Interesem rzeczywistym i aktualnym (tzn. nieopartym na domysłach).

⇨ **Krok 2** – należy rozważyć, czy istnieją inne, mniej inwazyjne sposoby osiągnięcia tego samego celu i interesu.

⇨ **Krok 3** – należy ocenić, czy podstawowe prawa lub interesy osób fizycznych nie są nadrzędne wobec interesu administratora. Podczas przeprowadzania przedmiotowej oceny należy wziąć pod uwagę następujące elementy:

- Ewentualne ujemne strony dla PPF (i/lub osób trzecich), gdyby przetwarzanie danych nie było prowadzone
- Charakter danych, których przetwarzanie jest planowane (dane wrażliwe? dane „zwykłe”?)
- Status osoby fizycznej (małoletni, pracownik, klient itp.)
- Sposób przetwarzania danych (na dużą skalę, eksploracja danych, zaawansowana analityka, profilowanie, ujawnianie wielu osobom lub publikacja danych)
- Rozsądne oczekiwania osoby fizycznej
- Porównanie wpływu przetwarzania na osobę fizyczną z oczekiwaną korzyścią płynącą z przetwarzania dla PPF

⇨ **Krok 4** – jeśli interes PPF nie jest przeważający wobec interesu osoby fizycznej, należy zastosować odpowiednie dodatkowe zabezpieczenia, by skorygować równowagę interesów. Przedmiotowe zabezpieczenia mogą obejmować na przykład:

- Minimalizację danych (np. ścisłe ograniczenia w gromadzeniu danych lub natychmiastowe usunięcie danych po ich wykorzystaniu)

- Środki techniczne i organizacyjne zapewniające, że dane nie mogą być wykorzystywane w celu podejmowania innych czynności w odniesieniu do osób, których dotyczą („funkcjonalne oddzielenie")

- Szerokie zastosowanie technik anonimizacji, agregacji danych, technologii gwarantujących zwiększoną ochronę prywatności, uwzględnienie ochrony danych w fazie projektowania

- Zwiększenie przejrzystości (tj. podanie szczegółowych informacji na temat sposobu, w jaki PPF będzie przetwarzać dane; wyjaśnienie powodów, dla których PPF uważa, że interesy danej osoby nie są nadrzędne w stosunku do interesów PPF)

- Zapewnienie bezwarunkowego prawa do wyrażenia sprzeciwu (*opt-out*) wobec przetwarzania, jeżeli prawo do sprzeciwu nie jest przewidziane przepisami obowiązującego prawa o ochronie danych

Details for revisions and policy updates

Policy name:	Group Data Protection Policy
Version number:	V3
Effective date of this version:	1 November 2024
Authorized by:	PPF Executive Committee
Scope:	All companies of PPF Group and their employees
Policy Review Cycle:	Annually from effective date
Docket Responsibility of Review Cycle:	Legal Counsel

Revision history:	
Date: 1 August 2018 Approved by:	Creation of V1 of Group Data Protection Policy PPF Executive Committee
Date: 1 August 2023 Approved by:	Coming into effect of V2 of Group Data Protection Policy PPF Executive Committee
Date: 1 November 2024 Approved by:	Amendment to Chief People Officer (V3) PPF Executive Committee