

Wybrane zagadnienia z zakresu ochrony danych

Przewodnik dla przedsiębiorców

Niniejsza publikacja powstała w ramach Projektu Partnerskiego Leonardo da Vinci „Podnoszenie świadomości w zakresie ochrony danych wśród przedsiębiorców działających na terytorium UE” (2009-1-PL1-LEO04-05167 1). Projekt ten został sfinansowany przy wsparciu Komisji Europejskiej w ramach programu Uczenie się przez całe życie.

Przewodnik „Wybrane zagadnienia z zakresu ochrony danych. Przewodnik dla przedsiębiorców” stanowi owoc współpracy międzynarodowej pomiędzy ekspertami reprezentującymi trzy organy ochrony danych:

- Biuro Generalnego Inspektora Ochrony Danych Osobowych z Polski
- Biuro Ochrony Danych z Czech
- Rzecznika Ochrony Danych i Wolności Informacji z Węgier.

Niniejsza publikacja odzwierciedla jedynie poglądy autorów. Komisja Europejska nie ponosi odpowiedzialności za wykorzystanie zawartych w niej informacji w jakikolwiek sposób.

Niniejsza publikacja dostępna jest na stronach internetowych partnerskich organów ochrony danych, skąd można pobrać ją dla celów niekomercyjnych.

PRZEDMOWA	4
------------------	----------

1. WSTĘP	5
-----------------	----------

2. PRAWODAWSTWO EUROPEJSKIE I KRAJOWE ORAZ PODSTAWOWE DEFINICJE Z ZAKRESU OCHRONY DANYCH	6
---	----------

2.1. Europejskie i krajowe akty prawne z zakresu ochrony danych	6
--	---

2.2. Definicje związane z prawodawstwem z zakresu ochrony danych	9
---	---

3. ZASADY OCHRONY DANYCH W DZIAŁALNOŚCI GOSPODARCZEJ	17
---	-----------

4 DANE OSOBOWE JAKO PRZEDMIOT DZIAŁALNOŚCI GOSPODARCZEJ	34
--	-----------

4.1. Przetwarzanie danych w cyklu biznesowym	34
--	----

4.2. Przetwarzanie danych osobowych w związku z zatrudnieniem	37
--	----

4.3. Dane osobowe w marketingu i kontaktach z klientami	43
---	----

ORGANY OCHRONY DANYCH UCZESTNICZĄCE W PROJEKCIE	47
--	-----------

PRZEDMOWA

Dwudziesty pierwszy wiek często nazywany jest epoką informacji. Panuje pogląd, że ludzka działalność opiera się na wymianie informacji. Nowoczesna technologia umożliwia zbieranie, ocenę, przekazywanie i przetwarzanie bezprecedensowych ilości danych. Ludzie mają obecnie natychmiastowy dostęp do informacji, które przedtem nie były dostępne. Wraz z możliwościami, proporcjonalnie wzrasta ryzyko naruszania prywatności obywateli i jego niepożądanych konsekwencji. Zaufanie, jakim darzymy technologię informacyjną zależy od poziomu ochrony danych, jaki zapewnia ona swoim użytkownikom.

Celem niniejszej publikacji jest dostarczenie przedsiębiorcom i pracownikom informacji o ochronie danych. Przewodnik ten wyjaśnia, w jaki sposób odpowiedni system ochrony danych pomaga rozwinąć kulturę korporacyjną opartą na odpowiedzialności społecznej. Podnosi także świadomość faktu, że ochrona danych może stanowić olbrzymią przewagę konkurencyjną, szczególnie w pewnych branżach działalności. Niniejsza książeczka pomoże Państwu zapoznać się z podstawowymi zasadami ochrony danych i Państwa obowiązkami prawnymi w tym zakresie.

Wierzymy, że niniejszy przewodnik będzie dla Państwa cenną pomocą.

1. WSTĘP

Rozpoczęcie działalności gospodarczej, w szczególności za granicą, wymaga zaznajomienia się z wieloma przepisami, mającymi znaczący wpływ na codzienną działalność przedsiębiorców. Zaliczają się do nich m.in. przepisy podatkowe, prawo pracy, prawa konsumenta, a także ustawodawstwo w zakresie ochrony danych osobowych i prywatności.

Działalność gospodarcza wiąże się z potrzebą wykorzystania danych osobowych, zatem każdy przedsiębiorca rozpoczynający działalność na terenie Czech, Polski i Węgier musi wypełnić zobowiązania w zakresie ochrony danych. Zobowiązania te dotyczą zarówno osób prowadzących jednoosobową działalność gospodarczą jak i dużych spółek handlowych. Niniejszy przewodnik, opisujący ogólne kwestie dotyczące ochrony danych, adresowany jest do przedsiębiorców zamierzających rozpocząć działalność na rynkach zagranicznych: w Czechach, w Polsce i na Węgrzech.

Poniżej przedstawiony został ogólny przegląd czeskiego, węgierskiego i polskiego prawa krajowego w zakresie przetwarzania danych. Jeśli chcą Państwo otrzymać szczegółowe informacje na ten temat, zalecamy skontaktowanie się z organem ochrony danych w danym państwie członkowskim UE i zapoznanie się z materiałami zamieszczonymi na jego stronie internetowej.

2. PRAWODAWSTWO EUROPEJSKIE I KRAJOWE ORAZ PODSTAWOWE DEFINICJE Z ZAKRESU OCHRONY DANYCH

2.1 Europejskie i krajowe akty prawne z zakresu ochrony danych

W Europie ochrona danych osobowych ma szczególne znaczenie. Jako jedno z praw podstawowych, jest zagwarantowana przez wiele krajowych i międzynarodowych aktów prawnych. Prawo do poszanowania życia prywatnego i rodzinnego gwarantuje art. 8 Europejskiej Konwencji Praw Człowieka. Pierwszym międzynarodowym aktem prawnym regulującym tę kwestię w sposób kompleksowy jest Konwencja Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przyjęta przez Radę Europy 28 stycznia 1981 roku. Na poziomie Unii Europejskiej, aktem takim jest dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Ponadto, prawo do ochrony danych osobowych jest również chronione jako prawo podstawowe na mocy art. 8 Karty Praw Podstawowych Unii Europejskiej i art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej. Poza dyrektywą 95/46/WE, kwestię ochrony danych osobowych regulują również inne akty prawa wspólnotowego. W znaczącym stopniu uzupełniają one przepisy dyrektywy 95/46/WE, która ma charakter ogólny i służy jako punkt odniesienia dla odpowiednich przepisów państw członkowskich.

Dyrektywa 95/46/WE reguluje prawo do ochrony prywatności każdej osoby fizycznej w zakresie przetwarzania danych osobowych, należące do podstawowych praw i wolności osób fizycznych. Dyrektywa ma zastosowanie do przetwarzania danych osobowych prowadzonego w sposób w całości lub w części zautomatyzowany oraz do przetwarzania w sposób niezautomatyzowany danych osobowych stanowiących lub mających stanowić część zbioru danych.

Podstawowym celem dyrektywy 95/46/WE jest zapewnienie najwyższego możliwego poziomu ochrony danych osobowych i ułatwienie swobodnego przepływu danych na terytorium Unii Europejskiej i praktycznie całego Europejskiego Obszaru Gospodarczego.

Przetwarzanie danych osobowych na terenie Wspólnoty winno odbywać się zgodnie z prawem państwa członkowskiego, w którym prowadzi działalność administrator odpowiedzialny za to przetwarzanie. Jeśli jeden administrator prowadzi działalność, w szczególności za pośrednictwem filii, na terytorium kilku państw członkowskich, musi on zapewnić działanie każdej z filii zgodnie z wymogami nałożonymi przez prawo danego państwa członkowskiego.

Państwa członkowskie UE były zobowiązane do wdrożenia przepisów dyrektywy w swoich systemach prawnych, otrzymały jednak pewien margines swobody w jej zastosowaniu, co może prowadzić do różnic w ustawodawstwie krajowym. Przedsiębiorcy prowadzący działalność w poszczególnych krajach powinni mieć świadomość tego faktu. Niniejsza publikacja wskazuje takie różnice pomiędzy prawem polskim, czeskim i węgierskim.



Ustawodawstwo polskie

W Polsce prawo do prywatności i ochrony danych zagwarantowane jest w Konstytucji Rzeczypospolitej Polskiej (patrz art. 47 i 51). Zasady przetwarzania danych i prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych określa ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm., dalej zwana ustawą) oraz akty wykonawcze przyjęte na jej podstawie: rozporządzenia Ministra Spraw Wewnętrznych i Administracji:

1. Rozporządzenie z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) – przyjęte na podstawie art. 39a ustawy – określa:
 - rodzaj i zakres dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych – odpowiednie do zagrożenia i kategorii danych podlegających ochronie;
 - główne wymogi techniczne i organizacyjne, jakie winny spełniać systemy informatyczne i urządzenia wykorzystywane do przetwarzania danych osobowych;
 - wymogi w zakresie zapisywania ujawnienia danych i bezpieczeństwa przetwarzania danych.
2. Rozporządzenie z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536) – przyjęte na podstawie art. 46a ustawy – określa wzór, stanowiący załącznik do niego.
3. Rozporządzenie z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) – przyjęte na podstawie art. 22a ustawy – określa wzór.

System ochrony danych obejmuje również inne przepisy szczególne, np. przepisy Kodeksu Cywilnego o ochronie dóbr osobistych oraz inne przepisy regulujące wykorzystanie danych osobowych.

W Polsce, organem odpowiedzialnym za nadzorowanie zgodności przetwarzania danych z przepisami o ochronie danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych (<http://www.giodo.gov.pl>).



Ustawodawstwo czeskie

W Czechach, ochronę danych osobowych reguluje przede wszystkim ustawa nr 101/2000 Coll. o ochronie danych osobowych i zmianie niektórych ustaw (dalej zwana „ustawą 101”), stanowiąca integralną część czeskiego systemu prawnego na dwa sposoby:

- Jest powiązana z art. 10 i 17 Karty Praw Podstawowych, przyznającej z jednej strony prawo do informacji, z drugiej – prawo do ochrony prywatności. Ustawa 101 rozwiązuje problem sprzecznego charakteru wymienionych wyżej praw. Nie jest jednak jedyną regulacją tego rodzaju – Kodeks Cywilny (ustawa nr 40/1964 Coll. z późniejszymi zmianami) również zawiera przepisy o ochronie tożsamości, w istotny sposób powiązane z pojęciami „przetwarzania danych osobowych” i „osoby, której dane dotyczą” określonymi w ustawie 101.
- Ustawa 101 to ustawa ogólna, regulująca przetwarzanie danych osobowych na terytorium Czech, z wyjątkiem przetwarzania prowadzonego przez osoby fizyczne wyłącznie dla potrzeb osobistych. Ustawa 101 zezwala także na przetwarzanie danych osobowych dla celów szczególnych (zgodnie z dyrektywą 95/46/WE), również w celu wypełnienia przepisanych prawem zadań. Przedsiębiorcy muszą sprawdzić, czy planowana lub prowadzona operacja przetwarzania nie jest objęta

przepisami szczególnymi. Jeśli tak – ustawa 101 ma zastosowanie jako przepis wtórny. Jeśli nie – ma pierwszeństwo przed innymi przepisami.

Ustawę 101 (i ustawodawstwo w zakresie ochrony danych jako takie) podzielić można na trzy części tematyczne:

1. Przepisy regulujące warunki przetwarzania danych osobowych (zawarte w art. 5-19 i w art. 27 ustawy 101), określające podstawy prawne dla przetwarzania danych osobowych (np. zgoda osoby, której dane dotyczą, zobowiązania umowne lub wypełnienie zobowiązań nałożonych przepisami szczególnymi).
2. Przepisy regulujące konsekwencje naruszenia zasad ochrony danych, w tym:
 - środki naprawcze, które mogą mieć postać usunięcia danych, zakończenia nielegalnego przetwarzania itp. (patrz art. 40 ustawy 101), nie stanowią jednak sankcji;
 - kary (patrz Rozdział VII ustawy 101). Sankcje karnoprawne – np. nielegalne przetwarzanie danych osobowych stanowi przestępstwo karne zgodnie z art. 180 Kodeksu Karnego;
 - odszkodowanie, w przypadkach, w których zastosowanie mają przepisy Kodeksu Cywilnego i Kodeksu Handlowego.
3. Przepisy proceduralne, określające metody egzekwowania praw w przypadku naruszenia zasad ochrony danych. Postępowanie, w którym odwołuje się do środków naprawczych, musi być prowadzone przed sądem; sprawy karne muszą być prowadzone przez organy wymiaru sprawiedliwości, w innych przypadkach organem właściwym jest Biuro Ochrony Danych Osobowych – niezależny organ nadzorczy (Rozdział V ustawy 101).

W Czechach organem właściwym do spraw ochrony danych jest Biuro Ochrony Danych Osobowych (<http://www.uoou.cz/>). Poza jego właściwością znajdują się jedynie operacje przetwarzania prowadzone przez służby wywiadowcze. Biuro odpowiada między innymi za rozpatrywanie skarg w sprawie naruszenia zasad ochrony danych (skargę lub wniosek może nieodpłatnie złożyć każdy, również osoby niebędące obywatelami Czech), oferuje także bezpłatne konsultacje.



Ustawodawstwo węgierskie

Na Węgrzech, prawo do ochrony danych osobowych zapewnia Konstytucja. To prawo podstawowe i jego zakres zostały dokładniej określone i uregulowane ustawą LXIII z roku 1992 o ochronie danych osobowych i dostępie do informacji publicznej (dalej zwanej ustawą DP & FOI). Ustawa ta wdrożyła przepisy dyrektywy 95/46/WE w prawie węgierskim. Oprócz ustawy o ochronie danych, istnieje kilka ustaw sektorowych zawierających istotne przepisy z zakresu ochrony danych. Ustawa DP & FOI i ustawy sektorowe były nowelizowane po wejściu w życie. Główne rozdziały ustawy DP&FOI, zawierające podstawowe definicje i najważniejsze zasady ochrony danych, oparte są na dyrektywie 95/46/WE. Ustawa określa kompetencje i uprawnienia Rzecznika Ochrony Danych i reguluje dostęp do informacji publicznej oraz wykorzystanie danych osobowych dla celów naukowych lub statystycznych.

Na Węgrzech ochronę danych nadzoruje niezależny organ – Rzecznik Ochrony Danych i Wolności Informacji (<http://www.adatvedelmibiztos.hu/abi/>).

2.2 Definicje związane z prawodawstwem z zakresu ochrony danych

Definicje związane z prawodawstwem z zakresu ochrony danych oparte są na art. 2 dyrektywy 95/46/WE.

Dane osobowe i osoba, której dane dotyczą

Dane osobowe oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej ("osoby, której dane dotyczą"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość.

Pojęcie danych osobowych jest niezwykle istotne, ponieważ ustawy o ochronie danych mają zastosowanie jedynie do informacji stanowiących dane osobowe. Ochrona innych informacji może być zapewniona innymi przepisami.

Dane osobowe to zestaw danych pozwalający na zidentyfikowanie określonej osoby w takim stopniu, by było możliwe odróżnienie jej od innych osób, których dane dotyczą i kontaktowanie się z nią lub w znacznym stopniu ułatwiający kontakt z tą osobą i wyciąganie wniosków na jej temat na podstawie dostępnych danych. W toku przetwarzania danych są one uznawane za dane osobowe dopóty, dopóki można stwierdzić ich związek z osobą, której dotyczą.

Informacji związanych z osobami prawnymi lub jednostkami organizacyjnymi nieposiadającymi osobowości prawnej nie uznaje się za dane osobowe. Również informacji o osobach zmarłych nie klasyfikuje się jako dane osobowe, chyba, że w określonej sytuacji informacje te dotyczą również osób żyjących.

Przedsiębiorcy zwykle wykorzystują podstawowe informacje o osobach fizycznych, takie jak imiona, nazwiska, adresy, daty urodzenia, numery identyfikacyjne i inne najczęściej wykorzystywane dane, udostępniane w sytuacjach dnia codziennego. Ustawodawstwo w zakresie ochrony danych osobowych nie zawiera pełnego katalogu kategorii danych, gdyż jego stworzenie nie jest możliwe ze względu na złożoność pojęcia danych osobowych.



Nie istnieją szczególne różnice w prawie krajowym.



Nie istnieją szczególne różnice w prawie krajowym.



Na Węgrzech dane osobowe osób zarządzających podmiotami prawnymi wpisanymi do Rejestru Spółek (np. dyrektorów zarządzających lub wspólników rzeczywistych) są publiczne na mocy ustawy V z roku 2006 o upublicznianiu informacji na temat spółek, rejestracji spółek i postępowaniu likwidacyjnym. Wspomniany rejestr publiczny zawiera dane osobowe, np. nazwisko, datę i miejsce urodzenia i nazwisko panieńskie matki dyrektorów zarządzających i menedżerów.

Dane szczególnie chronione

Dane szczególnie chronione to dane ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również dane dotyczące zdrowia i życia seksualnego.

Dane związane z wyrokami, wyrokami sądowymi lub środkami bezpieczeństwa oraz dane dotyczące sankcji administracyjnych lub wyroków w sprawach cywilnych mogą mieć podobny status.

Zgodnie z dyrektywą 95/46/WE, ustawy poszczególnych państw członkowskich zawierają odrębny katalog szczególnych kategorii danych, zwanych danymi szczególnie chronionymi. Ze względu na ich charakter, dane te podlegają szczególnej ochronie, ponieważ ich wykorzystanie może prowadzić do poważnego naruszenia praw i wolności obywateli, np. do dyskryminacji. Należy pamiętać, że katalog danych szczególnie chronionych może być różny w różnych państwach.



Pojęcie danych osobowych nie obejmuje informacji o przedsiębiorstwach, w tym o osobach fizycznych prowadzących jednoosobową działalność gospodarczą, jeśli informacje takie identyfikują te osoby w obrocie handlowym i jeśli są one wpisane do rejestru przedsiębiorstw. W ustawie polskiej katalog danych szczególnie chronionych jest bardziej szczegółowy i obejmuje informacje o przynależności do partii politycznych, kodzie genetycznym, uzależnieniach, wyrokach wskazujących, decyzjach nakładających kary i grzywny oraz innych decyzjach wydanych w toku postępowań sądowych lub administracyjnych.



Dane osób fizycznych prowadzących działalność gospodarczą są również uznawane za dane osobowe. Wykorzystanie daty urodzenia jest ściśle ograniczone na mocy ustawy nr 133/2000 Coll. Dane szczególnie chronione obejmują również dane o pochodzeniu etnicznym, o wyrokach skazujących za przestępstwo karne oraz dane genetyczne i biometryczne umożliwiające bezpośrednią identyfikację lub potwierdzenie tożsamości osoby, której dane dotyczą. Stosując ustawę, należy pamiętać o następujących kwestiach:

1. Dane o pochodzeniu etnicznym należy wyraźnie rozróżnić od danych o obywatelstwie. Pojęcia te są często mylone w języku kolokwialnym.
2. Informacje o członkostwie w partiach politycznych traktuje się jako dane szczególnie chronione, ujawniające przekonania polityczne. Trybunał Konstytucyjny orzekł jednak, że informacja o członkostwie w Partii Komunistycznej przed rokiem 1989 nie stanowi danych szczególnie chronionych.
3. Informacje o wyrokach skazujących za przestępstwo karne traktowane są jako dane szczególnie chronione. Nie należy ich zatem traktować podobnie jak informacji o zachowaniu, które można uznać za przestępstwo karne ani jak danych o innych sankcjach, np. grzywnach. Za dane szczególnie chronione uznawane nie są natomiast informacje o braku wyroków skazujących za przestępstwa karne, np. dane o niekaralności zaczerpnięte z rejestru przestępstw, ani informacje o odstąpieniu od wymierzenia kary za czyn noszący znamiona przestępstwa, np. ze względu na niepełnoletniość sprawcy.
4. Co do zasady, dane biometryczne uznać można za dane o mierzalnych i obiektywnie klasyfikowalnych cechach ciała ludzkiego. Ustawa 101 dodaje jednak jeszcze jedno

kryterium – możliwość bezpośredniej identyfikacji lub potwierdzenia tożsamości osoby, której dane dotyczą. Ogólnie rzecz ujmując, długość stopy danej osoby nie jest uznawana za daną biometryczną, natomiast odcisk jej palca – owszem.



Dane o osobach fizycznych prowadzących działalność gospodarczą również uznaje się za dane osobowe. Pojęcie danych osobowych obejmuje także członkostwo osoby, której dane dotyczą w organizacjach reprezentujących interesy, przedstawicielstwach i organizacjach adwokackich z obszaru – co bardzo istotne – prawa pracy i zatrudnienia. Ustawodawca poszerzył również zakres danych szczególnie chronionych związanych z przestępstwami karnymi. Zaliczają się do nich wszelkie dane osobowe, które zostały utworzone (podczas postępowań w sprawach karnych lub przed rozpoczęciem takich postępowań, w związku z przestępstwem karnym) przez organy uprawnione do prowadzenia postępowań w sprawach karnych lub badania przestępstw karnych bądź przez organy karne i które mogą zostać powiązane z osobą, której dane dotyczą, a także dane osobowe dotyczące poprzednich wyroków w sprawach karnych.

Przetwarzanie danych osobowych

Przetwarzanie danych osobowych („przetwarzanie”) oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie.

Pojęcie to jest bardzo istotne dla przedsiębiorców, ponieważ potrzebują oni odpowiedniej podstawy prawnej dla każdej operacji przetwarzania danych.

Przetwarzanie może być prowadzone raz lub kilka razy, w sposób identyczny lub kompatybilny technologicznie. Bardzo istotny jest fakt, że pojedyncza (jednorazowa) operacja wykonana na danych, np. ich ujawnienie, jest traktowana jako ich przetwarzanie.

Najczęściej wykonywane operacje uznawane za przetwarzanie danych to fotografowanie, zapisywanie dźwięku lub obrazu oraz zapisywanie cech fizycznych umożliwiających identyfikację osoby (np. odcisków palców, próbek DNA i obrazu siatkówki). Przechowywanie danych również traktuje się jako ich przetwarzanie.



Nie istnieją szczególne różnice w prawie krajowym.



Przetwarzanie jest rozumiane jako operacja lub zestaw operacji wykonywane w sposób systematyczny. W związku z tym, za przetwarzanie uznaje się jedynie określony rodzaj operacji, wykonywanej wielokrotnie, w sposób identyczny lub kompatybilny z technologicznego punktu widzenia. Nie można wykluczyć, że zestaw operacji zostanie wykonany jedynie raz bądź że zostanie wykonana tylko jedna operacja z całego zestawu. Decydujące znaczenie ma zamiar

powtarzania lub kontynuowania tych operacji w danych okolicznościach. Zamiar ten może być udokumentowany w postaci opisów organizacji pracy, elementów sprzętu i oprogramowania itp. Pojęcie „przetwarzanie danych osobowych” może na przykład oznaczać „prowadzenie określonego rejestru, zbioru lub katalogu”. Jednorazowe przetwarzanie danych osobowych (pojedyncza publikacja lub przekazanie) nie jest objęte Ustawą 101.



Każda operacja wykonana na danych, również pojedyncza (jednorazowa), np. ich ujawnienie, jest traktowana jako ich przetwarzanie.

Szczególną formą przetwarzania jest techniczne przetwarzanie danych. Polega ono na wykonywaniu zadań technicznych związanych z operacjami przetwarzania danych, niezależnie od zastosowanych metod i środków i od miejsca ich zastosowania.

Zbiór danych

Zbiór danych („zbiór”) oznacza każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, scentralizowanych, zdecentralizowanych lub rozproszonych funkcjonalnie lub geograficznie.

Możliwość wyszukiwania na podstawie dowolnego kryterium osobowego (imię, nazwisko, data urodzenia, numer identyfikacyjny) lub nieosobowego (data wprowadzenia danych do zbioru) świadczy o uporządkowanym charakterze zestawu danych i pozwala na zaklasyfikowanie go jako zbiór danych. W przypadku przedsiębiorców typowymi zbiorami danych są np. akta osobowe pracowników, stworzone w związku z ich zatrudnieniem i z wykonywaną przez nich pracą, oraz zbiory danych konsumentów. Zbiory mogą być prowadzone zarówno w systemach informatycznych jak i w formie papierowej.

Administrator

Administrator danych oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe.

Administrator decyduje o celach i środkach przetwarzania danych. Jest odpowiedzialny za przetwarzanie danych osobowych i za kontrolę nad tym przetwarzaniem. Administratorami mogą być organy władzy publicznej i samorządowej, podmioty gospodarcze lub osoby fizyczne prowadzące działalność gospodarczą, jeśli decydują one o celach i środkach przetwarzania.



Administratorem może być każda osoba fizyczna i prawna oraz organizacja pozbawiona osobowości prawnej.



Administratorem jest każda osoba fizyczna lub prawna określająca cel i środki przetwarzania danych, wykonująca operacje przetwarzania i odpowiedzialna za to przetwarzanie.



Administratorem jest każda osoba fizyczna lub prawna, bądź organizacja pozbawiona osobowości prawnej, która określa cel przetwarzania, podejmuje decyzje dotyczące przetwarzania (w tym dotyczące zastosowanych do niego środków) i wdraża takie decyzje lub zleca ich wdrażanie technicznemu przetwarzającemu, któremu zleciła przetwarzanie.

W toku zatrudnienia można wprowadzić rozróżnienie pomiędzy administratorem danych a innymi osobami administrującymi danymi. Administratorem jest firma lub osoba zatrudniająca osobę, której dane dotyczą. Pracodawca działający w ramach administratora czyli firmy, np. dyrektor, ma prawo zapoznać się z danymi osobowymi pracownika.

Przetwarzający

Przetwarzający oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych.

Administrator nie musi samodzielnie wykonywać wszystkich czynności związanych z przetwarzaniem danych osobowych. Może upoważnić inny podmiot do prowadzenia przetwarzania, w całości lub w części. Przetwarzający nie staje się administratorem danych, których przetwarzanie mu powierzono. Fakt, że podmiot, któremu zlecono przetwarzanie danych, nie staje się ich administratorem, pociąga za sobą określone konsekwencje. Zobowiązania nałożone przez ustawodawstwo na administratora, np. obowiązek rejestracji, nie mają zastosowania do tego podmiotu, spoczywa na nim jednak obowiązek zabezpieczenia danych.



Ustawa wymaga sporządzenia umowy powierzenia przetwarzania danych innemu podmiotowi w formie pisemnej i dokładnego określenia w niej zakresu i celu przetwarzania danych. Jeśli chodzi o zgodność z wymogami w zakresie zabezpieczania danych, przetwarzający ponosi taką samą odpowiedzialność jak administrator. Ponadto, podmiot, któremu powierzono przetwarzanie danych odpowiada przed administratorem za działania niezgodne z zawartą z nim umową. Generalny Inspektor Ochrony Danych Osobowych odpowiada za nadzorowanie zgodności przetwarzania danych przez podmiot, któremu je powierzono z przepisami o ochronie danych osobowych. Nadzór jest prowadzony zgodnie z zasadami określonymi w art. 14-19 ustawy o ochronie danych osobowych (art. 31 ust. 5 wspomnianej ustawy).



W przypadku braku podstaw prawnych dla upoważnienia, administrator i przetwarzający zawierają umowę o przetwarzanie danych osobowych zgodnie z art. 6 ustawy o ochronie danych. Umowa taka musi zostać sporządzona na piśmie i wyraźnie określać w szczególności zakres, cel i czas trwania, a także gwarantować zastosowanie przez przetwarzającego

technicznych i organizacyjnych zabezpieczeń danych.

Jeśli przetwarzający odkryje, że administrator nie dopełnia wymogów określonych prawem, ma obowiązek niezwłocznie zgłosić taką sytuację i przerwać przetwarzanie. Jeśli tego zaniecha, może wspólnie i solidarnie z administratorem odpowiadać za wszelkie szkody, jakich doznała osoba, której dane dotyczą.

Jeśli przetwarzanie podlega obowiązkowi rejestracji, obowiązek zgłoszenia do organu ochrony danych spoczywa na administratorze.



Nie istnieją szczególne różnice w prawie krajowym.

Osoba trzecia

Osoba trzecia oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędący osobą, której dane dotyczą, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego upoważnione są do przetwarzania danych.

Pojęcie osoby trzeciej jest niezwykle istotne dla działalności przedsiębiorców, ponieważ przekazywanie danych osobom trzecim pociąga za sobą liczne zobowiązania, takie jak istnienie odpowiednich podstaw prawnych lub obowiązku ochrony danych przed dostępem stron trzecich, jeśli nie istnieją dla niego takie podstawy. Należy pamiętać, że jako osobę trzecią traktuje się nie samego administratora, a osoby, które upoważnił on do przetwarzania danych bądź przetwarzającego. Nie wszystkie przepisy krajowe regulują tę kwestię, jednak z definicji administratora, osoby upoważnionej do przetwarzania danych lub przetwarzającego da się pośrednio wywnioskować definicję osoby trzeciej.



Nie istnieją szczególne różnice w prawie krajowym.



Nie istnieją szczególne różnice w prawie krajowym.



Zatrudnienie tworzy stosunek prawny pomiędzy pracodawcą a pracownikiem. Poza pracodawcą, występującym w charakterze administratora danych, i innymi osobami upoważnionymi do kontroli danych w toku zatrudnienia, wszystkich innych uczestników można traktować jako osoby trzecie na mocy ustawy o ochronie danych i Kodeksu Pracy. Przekazywanie danych osobom trzecim może odbywać się z opóźnieniem, ponieważ nie istnieją dla niego żadne przesłanki prawne, w związku z czym wszyscy pracownicy, których dane dotyczą muszą zgodzić się na taką operację.

Odbierający dane

Odbierający dane oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, któremu ujawniane są dane, będący lub niebędący osobą trzecią; jednakże władze, które mogą otrzymywać dane w ramach konkretnego dochodzenia, nie są uważane za odbiorcę.

W celu zapewnienia możliwości kontrolowania danych osobowych przez osoby, których dane dotyczą, przedsiębiorca zobowiązany jest poinformować te osoby o znanych sobie odbiorcach danych, które przetwarza.



Odbierający dane oznacza każdą osobę, której przekazywane są dane, z wyjątkiem:

- a) osoby, której dane dotyczą,
- b) osoby upoważnionej do prowadzenia przetwarzania danych,
- c) przedstawiciela administratora prowadzącego działalność w państwie trzecim, wykorzystującego środki przetwarzania danych,
- d) podmiotu określonego w art. 31,
- e) władz państwowych lub samorządowych, którym ujawniono dane w związku z prowadzonym postępowaniem.



Odbierający dane oznacza każdy podmiot, któremu przekazywane są dane. Nie jest to podmiot, który przetwarza dane dla celów inspekcji, nadzoru i regulacji związanych z pełnieniem funkcji publicznej.



Ustawa o ochronie danych zawiera odniesienia do tego pojęcia, nie definiuje go jednak. Odbierającym dane jest zwykle administrator. Nie jest to status nowy. Należy odróżnić administratora od odbierającego dane.

Zgoda osoby, której dane dotyczą

Zgoda osoby, której dane dotyczą oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych.

Jest to dobrowolne, konkretne i świadome oświadczenie woli osoby, której dane dotyczą, przez które wyraża ona w wyraźny sposób zgodę na przetwarzanie, w całości lub w części, swoich danych osobowych. Zgoda taka może zostać wycofana. Zgoda na wykorzystanie danych szczególnie chronionych wymaga formy pisemnej.



Zgoda nie może zostać domniemana na podstawie oświadczenia woli dotyczącego innej kwestii. Oświadczenie woli musi zostać wyodrębnione.



Zgodę osoby, której dane dotyczą określa się jako dobrowolne, świadome oświadczenie woli osoby, której dane dotyczą. Zgoda taka obejmuje akceptację przez osobę, której dane dotyczą, przetwarzania jej danych osobowych. Choć ustawa o ochronie danych nie wymaga formy pisemnej, nakłada wymóg możliwości weryfikacji zgody przez okres przetwarzania danych.



W każdym przypadku należy zdecydować, czy przepisy Kodeksu Pracy bądź zgoda stanowią przesłankę dopuszczalności przetwarzania danych. Istnieje jedynie kilka przepisów sektorowych w tej kwestii. Zgoda osoby, której dane dotyczą, wydaje się lepszym zabezpieczeniem prawnym w związku z faktem, że w wielu przypadkach przesłanki prawne można zakwestionować.

3. ZASADY OCHRONY DANYCH W DZIAŁALNOŚCI GOSPODARCZEJ

Podstawowe zobowiązania w zakresie przetwarzania danych

Administrator musi być w stanie wykazać, że spełnione zostały odpowiednie przesłanki prawne dla przetwarzania danych, musi również spełnić obowiązek informacyjny oraz zapewnić jakość przetwarzanych danych. Jest również zobowiązany do poszanowania praw osób, których dane dotyczą, odpowiedniego zabezpieczenia danych oraz zgłoszenia prowadzonych zbiorów danych do rejestracji przez krajowy organ ochrony danych.

Legalność przetwarzania danych

Każda operacja przetwarzania danych musi mieć odpowiednią podstawę prawną. Przez „podstawę prawną” rozumiemy zezwolenie na przetwarzanie danych w określonym zakresie. Przykładem podstawy prawnej są zgoda i wymóg prawny. W niektórych krajach podstawy prawne określone są w sposób bardziej szczegółowy.

Co do zasady, przetwarzanie danych szczególnie chronionych jest zakazane. Jednak w niektórych przypadkach administrator może wykorzystywać takie dane, jeśli zdoła udowodnić, że ma do czynienia z przypadkiem wyjątkowym, określonym w krajowych przepisach o ochronie danych.



Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. W tym przypadku za prawnie usprawiedliwione cele uważa się marketing bezpośredni własnych produktów i usług administratora lub dochodzenie roszczeń wynikających z działalności gospodarczej.

Przesłanki te są rozdzielne. Aby wykorzystanie danych można było uznać za legalne, wystarczy spełnienie jednej z nich, nie wszystkich łącznie, zatem jeśli nie da się zrealizować uprawnienia lub spełnić obowiązku wynikającego z przepisu prawa bez wykorzystania danych, nie jest wymagana dodatkowa zgoda na ich wykorzystanie, nie ma też potrzeby udowadniania, że przetwarzanie prowadzone jest dla dobra publicznego lub jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów. Pojęcie zgody na wykorzystanie danych w celu wykonania przepisów prawa jest mylące, sugeruje bowiem, że zgoda taka może zostać wycofana, jeśli przekazywanie danych jest niezbędne dla celów, dla których zostały zebrane dane.

Wykorzystanie danych szczególnie chronionych jest co do zasady zabronione na mocy art. 27

(1) ustawy. Administrator może jednak wykorzystać takie dane, jeśli udowodni, że zaistniała jedna z wyjątkowych sytuacji określonych w art. 27 (2) ustawy.

Przetwarzanie danych szczególnie chronionych jest dopuszczalne m.in. jeśli osoba, której dane dotyczą, wyrazi na to zgodę na piśmie lub jeśli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony. Przetwarzanie danych szczególnie chronionych jest również dozwolone jeśli jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora; jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie; jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych.



Główną podstawę prawną dla legalności przetwarzania danych stanowi zgoda osoby, której dane dotyczą. Ustawa 101 określa zestaw wymogów, jakie należy spełnić ubiegając się o taką zgodę. Należy mieć to na uwadze, gdyż zgoda bywa nadużywana i stosowana jako narzędzie naruszające inne instrumenty ochrony danych osobowych.

Zgoda musi być wyraźna. Osoba, której dane dotyczą udziela zgody na rzecz administratora. Przetwarzanie danych osobowych nie może mieć miejsca bez dopełnienia tej czynności prawnej, a zgoda jako taka nie miałaby bez niej żadnego sensu. W związku z powyższym, zgodę można interpretować jako propozycję zawarcia pewnej umowy lub część bardziej złożonej umowy. W żadnym wypadku nie należy jej postrzegać jako odrębny, jednostronny akt.

Administrator może przetwarzać dane bez uzyskania zgody:

- jeśli prowadzi przetwarzanie niezbędne dla spełnienia spoczywających na nim obowiązków prawnych;
- jeśli przetwarzanie jest niezbędne dla realizacji umowy, której stroną jest osoba, której dane dotyczą lub rozpoczęcia negocjacji zmierzających do zawarcia lub zmiany umowy na żądanie osoby, której dane dotyczą;
- jeśli jest to niezbędne dla ochrony istotnych interesów życiowych osoby, której dane dotyczą. W takim przypadku, należy uzyskać zgodę osoby, której dane dotyczą bez zbędnej zwłoki. W przypadku nieotrzymania zgody, administrator zobowiązany jest zakończyć przetwarzanie i usunąć dane;
- w odniesieniu do danych osobowych, które zostały legalnie opublikowane zgodnie z przepisami szczególnymi, jednak bez uszczerbku dla prawa do ochrony życia prywatnego i osobistego osoby, której dane dotyczą;
- jeśli jest to niezbędne dla ochrony praw i uzasadnionych interesów administratora, odbiorcy lub innych zainteresowanych osób, jednak bez uszczerbku dla prawa do ochrony życia prywatnego i osobistego osoby, której dane dotyczą;
- jeśli przetwarza dane osobowe osoby publicznej, urzędnika administracji publicznej lub pracownika, ujawniając informacje o ich działalności publicznej lub administracyjnej, funkcji bądź stanowisku;
- jeśli przetwarzanie prowadzone jest wyłącznie dla celów archiwalnych, zgodnie z przepisami szczególnymi.

Podstawy prawne dla przetwarzania danych szczególnie chronionych określa art. 9 ustawy 101.



Zgodnie z główną zasadą węgierskiej ustawy o ochronie danych, dane osobowe można przetwarzać jedynie na podstawie ustawy uchwalonej przez parlament lub zgody osoby, której dane dotyczą. W przypadku danych szczególnie chronionych, zgoda na ich przetwarzanie musi zostać udzielona na piśmie.

Zgodnie z art. 2 pkt. 6 ustawy DP&FOI, zgoda oznacza dobrowolne, konkretne i świadome oświadczenie woli osoby, której dane dotyczą, którym jednoznacznie deklaruje ona zgodę na przetwarzanie, w całości lub w części, dotyczących jej danych osobowych.

Ustawa nie określa zakresu danych osobowych, które mogą być przetwarzane przez pracodawcę. Zgodnie z art. 77 ustawy XXII z roku 1992 Kodeks Pracy „(1) Pracownika można prosić o złożenie oświadczenia, wypełnienie kwestionariusza lub wykonanie testu zdolności jedynie jeśli nie narusza to jego praw osobistych, a dostarcza informacji uznawanych za istotne dla celów nawiązania stosunku pracy”. Pracodawca uprawniony jest do przetwarzania danych na mocy ustaw określających szczegółowo zakres danych i może przetwarzać jedynie objęte nim dane (np. dane związane z ubezpieczeniami społecznymi, podatkami, obowiązkiem uiszczenia odpowiednich składek itp.).

Ważne:

- Przed rozpoczęciem przetwarzania zawsze należy upewnić się, że spełniają Państwo przynajmniej jedną z przesłanek legalności określonych w ustawie o ochronie danych obowiązującej w danym kraju. W zależności od krajów, do podobnych operacji przetwarzania danych mogą odnosić się różne przesłanki legalności.
- Jeśli niezbędna jest zgoda, administrator musi wyraźnie sformułować klauzule zgody i oddzielić je od innych oświadczeń woli składanych przez osoby, których dane dotyczą.
- Co do zasady, zbieranie danych szczególnie chronionych jest zabronione. Jeśli jednak takie dane muszą zostać zebrane dla potrzeb działalności gospodarczej, można to zrobić pod warunkiem otrzymania pisemnej zgody osoby, której dane dotyczą lub spełnienia innej przesłanki legalności.
- Zgoda musi być dobrowolna, konkretna i świadoma.

Jakość danych

Jakość danych zapewniają następujące zasady:

1. Zasada celowości

Zasada ta, zwana także **zasadą ograniczenia celu**, stanowi, że dane należy zbierać jedynie dla określonych, legalnych celów i nie przetwarzać ich niezgodnie z tymi celami. Oznacza to, że:

- strona zbierająca dane nie może pominąć lub ukryć celu przetwarzania,
- cel ten nie może być określony w sposób niejasny,
- cel winien zostać podany osobie zainteresowanej przed zebraniem danych osobowych,
- niedozwolone jest uzależnianie zawarcia umowy od uzyskania zgody na przetwarzanie danych dla zupełnie innych celów (np. marketingu produktów i usług stron trzecich).

Przetwarzanie danych dla celów innych niż ten, dla którego zostały zebrane, jest jednak dozwolone, jeśli nie narusza praw i wolności osoby, której dane dotyczą i jest prowadzone:

- dla celów naukowych, historycznych lub statystycznych, a w Polsce również dydaktycznych,
- w sposób spełniający przesłanki legalności.

2. Zasada dokładności

Administrator ma obowiązek zapewnić, że dane są dokładne, kompletne i aktualne. W tym celu podczas przetwarzania danych kontroler winien:

- za każdym razem oceniać wiarygodność źródła danych,
- opracować sposób weryfikacji dokładności danych (w zależności od tego, czy dane są „zwykłe” czy szczególnie chronione) i stworzyć kodeks postępowania w sytuacjach, w których dane okażą się niedokładne,
- informować innych administratorów, którym przekazał dane o wszelkich dokonanych w nich uaktualnieniach bądź poprawkach.

Zbieranie danych z nieznanymi źródłami, które nie gwarantują ich dokładności, uważa się za pogwałcenie tej zasady. Przetwarzanie danych niedokładnych, niekompletnych lub nieaktualnych często jest niemożliwe z przyczyn technicznych (np. ze względu na budowę aplikacji informatycznych wykorzystywanych do przetwarzania danych osobowych).

3. Zasada proporcjonalności/odpowiedniości

Zgodnie z zasadą odpowiedniości, dane muszą być odpowiednie i nienadmierne w stosunku do celu, dla którego są przetwarzane. Administrator może przetwarzać dane jedynie takiego rodzaju i o takiej treści, jakie są niezbędne dla celów, dla których dane zostały zebrane. Odpowiedniość danych należy ocenić najpóźniej w momencie ich zbierania, administrator ma zatem obowiązek jej zweryfikowania. Zakres danych osobowych odpowiednich dla celu przetwarzania należy ocenić za każdym razem z perspektywy danego stosunku prawnego, w związku z którym administrator przetwarza dane osobowe. W kontekście umów, należy uwzględnić ich charakter i wagę. Zdarza się, że ustawodawca wyraźnie określa zakres danych odpowiednich w stosunku do celów przetwarzania w odpowiednich przepisach.

4. Zasada ograniczenia czasu

Administrator jest prawnie zobowiązany do przechowywania danych w postaci umożliwiającej identyfikację osób, których dane dotyczą tak długo, jak długo jest to konieczne dla spełnienia celu, dla którego dane są przetwarzane. Po osiągnięciu tego celu (np. wykonaniu umowy, zakończeniu okresu przechowywania danych wskazanego w przepisach) dane należy usunąć, zanonimizować lub przekazać podmiotowi upoważnionemu z mocy prawa do ich przejęcia od administratora (np. archiwum państwowemu).

Ważne:

- Przetwarzanie rozpoczyna się wraz ze zbieraniem danych. Zbieranie danych stanowi operację przetwarzania.
- Należy zbierać wyłącznie dane ściśle związane z celem prowadzonej przez Państwa działalności gospodarczej.
- Nie wolno zbierać danych „na wszelki wypadek”, do przyszłego wykorzystania. Składowanie danych jest niedozwolone.
- Zabronione jest uzależnianie zawarcia umowy od uzyskania zgody na przetwarzanie danych dla innych celów (np. marketingu towarów i usług stron trzecich).
- Nie wolno wykorzystywać danych osobowych uzyskanych z nieznanymi lub niepewnymi źródłami, nie gwarantujących dokładności. Zawsze należy upewnić się, że zebrane dane są dokładne, kompletne i, o ile to możliwe, aktualne. Muszą zatem Państwo opracować sposób weryfikacji dokładności danych i stworzyć kodeks postępowania w sytuacjach, w których dane okażą się niedokładne.
- Należy nieustannie monitorować zawartość zbiorów danych, pamiętając o usuwaniu nadmiernych danych.
- Nie wolno przechowywać danych dłużej niż jest to konieczne dla osiągnięcia celu, dla którego zostały zebrane.
- Po osiągnięciu celu przetwarzania (np. po wykonaniu umowy), zebrane dane winny być usunięte, zanonimizowane lub przekazane podmiotowi upoważnionemu z mocy prawa do ich przejęcia od administratora.

Obowiązek informacyjny administratora wobec osoby, której dane dotyczą i dostęp osoby, której dane dotyczą do danych

Przed zebraniem danych, administrator winien udzielić osobie, której dane dotyczą określonych informacji. Ich zakres zależy od tego, czy dane zostały zebrane bezpośrednio od osoby, której dane dotyczą, czy z innych źródeł.

Zgodnie z przepisami dyrektywy 95/46/WE, administrator ma obowiązek przedstawienia osobie, której dane dotyczą i od której gromadzone są dane, co najmniej następujących informacji, z wyjątkiem przypadku, kiedy informacje takie już posiada:

- (a) tożsamości administratora danych i ewentualnie jego przedstawiciela;
- (b) celów przetwarzania danych, do których dane są przeznaczone;
- (c) wszelkich dalszych informacji, jak np.:
 - odbiorcy lub kategorie odbierających dane,
 - tego, czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz ewentualne konsekwencje nieudzielenia odpowiedzi,
 - istnienie prawa wglądu do swoich danych oraz ich sprostowania,

o ile takie dalsze informacje są potrzebne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą.

W przypadku gdy dane uzyskiwane są z innych źródeł niż osoba, której dane dotyczą, administrator danych jest zobowiązany od początku gromadzenia danych osobowych lub w przypadku ujawnienia danych osobie trzeciej, nie później niż do momentu, gdy dane są ujawniane po raz pierwszy, dostarczyć osobie, której dane dotyczą, co najmniej następujące informacje, z wyjątkiem przypadku, kiedy posiada już ona takie informacje:

- tożsamość administratora i ewentualnie jego przedstawiciela;
- cele przetwarzania danych;
- wszelkie dalsze informacje, jak np.:
- kategorie potrzebnych danych,
- odbiorcy lub kategorie odbierających dane,
- istnienie prawa wglądu do swoich danych oraz ich sprostowania,

o ile takie dalsze informacje są konieczne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą.

Obowiązek informacyjny nie zachodzi w gdy, szczególnie w przypadku przetwarzania danych do celów statystycznych, historycznych lub naukowych, dostarczenie takich informacji wymagałoby niewspółmiernie dużego wysiłku lub jeżeli gromadzenie lub ujawnianie informacji jest wyraźnie przewidziane przez prawo. W takich przypadkach państwa członkowskie zapewniają odpowiednie środki zabezpieczające.

W takim przypadku, na administratorze spoczywa obowiązek poinformowania osoby, której dane dotyczą o zasadach wykorzystania danych, niezależnie od tego, czy osoba ta wnioskuje o podanie takich informacji. Na każdym kolejnym etapie przetwarzania danych informacje powinny być podawane na wniosek osoby, której dane dotyczą.

Od chwili rozpoczęcia przetwarzania danych, każda osoba, której dane dotyczą ma prawo dostępu do danych bez ograniczeń, w odpowiednich odstępach czasu oraz bez nadmiernego opóźnienia lub kosztów, w celu otrzymania:

- potwierdzenia, czy dotyczące jej dane są przetwarzane oraz co najmniej informacji o celach przetwarzania danych, kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane,

- wyrażonej w zrozumiałej formie informacji o danych przechodzących przetwarzanie oraz posiadanych informacji o ich źródłach,
- wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego.

Ponadto, osoba, której dane dotyczą może zażądać, odpowiednio do przypadku, sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z przepisami dyrektywy, szczególnie ze względu na niekompletność lub niedokładność danych.

Należy podkreślić, że zakres informacji udzielanych przez administratora i sposób ich udzielania na żądanie osoby, której dane dotyczą mogą różnić się w zależności od kraju.



Obowiązek informacyjny regulują art. 24 i 25 ustawy o ochronie danych osobowych.

Jeśli dane zbierane są od osoby, której dane dotyczą, administrator ma obowiązek udzielić informacji w zakresie wskazanym w dyrektywie 95/46/WE w momencie ich zbierania. Obowiązek ten nie powstaje, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub, podobnie jak w dyrektywie 95/46/WE, osoba, której dane dotyczą, posiada informacje, o których mowa w art. 24.1 ustawy.

W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator winien wypełnić obowiązek informacyjny określony w art. 25.1 ustawy i poza informacjami wskazanymi w dyrektywie 95/46/WE, udzielić osobie, której dane dotyczą informacji o źródle danych, prawie dostępu do treści swoich danych oraz ich poprawiania i uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 ustawy o ochronie danych osobowych: prawie do wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację i prawie wniesienia sprzeciwu wobec przetwarzania jej danych dla celów marketingowych i przekazywania ich innym administratorom. Bardzo istotne jest wypełnienie obowiązku informacyjnego niezwłocznie po zapisaniu zebranych danych w sposób umożliwiający ich dalsze przetwarzanie.

Wyjątki od tego obowiązku wymienione są w art. 25.2 ustawy, zgodnie z którym udzielanie informacji nie jest konieczne, jeżeli:

- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
- dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania,
- dane są przetwarzane przez podmiot publiczny lub podmiot niepubliczny realizujący zadania publiczne na podstawie przepisów prawa,
- osoba, której dane dotyczą, posiada już te informacje.

Prawo dostępu należy wykonać w ciągu 30 dni od daty złożenia wniosku przez osobę, której dane dotyczą, w zakresie określonym w art. 32.1, pkt. 1-5a. Na wniosek osoby, której dane dotyczą, informacji udziela się na piśmie. Jeśli prawo dostępu wykonywane jest rzadziej niż raz na 6 miesięcy, nie jest za to pobierana opłata.

Informacji nie udziela się jeśli spowodowałoby to:

1. ujawnienie wiadomości zawierających informacje niejawne,
2. zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
3. zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
4. istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.



1. Przy wykonywaniu obowiązku wynikającego z art. 11(1) ustawy 101 (zgodnego z art. 10 dyrektywy 95/46/WE) fakt, że przedmiotowe dane osobowe są już znane może stanowić okoliczność wyjątkową. W takim przypadku obowiązek informacyjny może zostać wykonany np. poprzez klauzulę zgody na przetwarzanie danych. Inne wyjątki zgodne z art. 10 i 11 wymienionej dyrektywy wymienione są w art. 11(3) ustawy 101. W przeciwieństwie do niego, art. 11(4) nakłada wyraźny obowiązek informowania o przetwarzaniu na mocy art. 5(2)(e) i art. 9(h) (przetwarzanie danych osobowych w celu ochrony praw, zgodnie z art. 7(f) i art. 8(2)(e) dyrektywy 95/46/WE).

2. Administratorzy mają prawo, w związku z dostępem do danych osobowych na mocy art. 12(3) ustawy 101, pobierać opłaty za udzielenie informacji osobie, której dane dotyczą. Opłata nie może przewyższać kosztów udzielenia informacji. Obowiązek informacyjny może w imieniu administratora spełnić przetwarzający.



Zgodnie z art. 6 ustawy DP&FOI, przed zebraniem danych należy poinformować osobę, której dane dotyczą o tym, czy ich podanie jest obowiązkowe czy dobrowolne. W przypadku obowiązku podania danych należy również wskazać podstawę prawną dla ich przetwarzania. Osobie, której dane dotyczą należy udzielić jednoznacznych, szczegółowych informacji o wszystkich aspektach związanych z przetwarzaniem jej danych, w szczególności o celach i podstawach prawnych przetwarzania, osobie upoważnionej do dokonania przetwarzania i przetwarzania technicznego, czasie trwania przetwarzania oraz osobach mających dostęp do danych. Należy również podać informacje o prawach i środkach zaradczych przysługujących osobom, których dane dotyczą w związku z przetwarzaniem. Informacje o przetwarzaniu danych uważa się za podane, jeśli przepisy prawa nakazują zebranie danych z istniejącego zbioru poprzez ich przekazanie lub zestawienie. Jeśli poinformowanie każdej osoby, której dane dotyczą jest niemożliwe lub pociągnęłoby za sobą nadmierne wydatki, w szczególności w przypadku przetwarzania danych dla celów statystycznych lub naukowych (w tym do badań historycznych) informacji można udzielić poprzez podanie do publicznej wiadomości faktu zbierania danych, zainteresowanych osób, których dane dotyczą, celu zbierania danych, czasu trwania zbierania danych i dostępności danych.

Art. 12 ustawy DP&FOI stanowi, że administrator ma obowiązek poinformować osobę, której dane dotyczą, na jej wniosek, o danych przetwarzanych przez administratora lub przetwarzanych technicznie przez przetwarzającego, o celu przetwarzania danych, jego podstawach prawnych i czasie trwania, o nazwie, adresie siedziby i działaniach przetwarzającego związanych z przetwarzaniem danych oraz o tym, kto i w jakim celu otrzymał lub otrzyma dane. Okres przechowywania informacji o przekazaniu danych i związanego z nim obowiązku informacyjnego może być ograniczony przepisami o przetwarzaniu danych. Okres ten nie może być krótszy niż pięć lat dla danych osobowych i dwadzieścia lat dla danych szczególnych. Administrator winien udzielić informacji na piśmie, w zrozumiałym sposób, w jak najkrótszym czasie, nie później jednak niż w ciągu 30 dni od daty złożenia wniosku. Wspomniane informacje są udzielane bezpłatnie, chyba że osoba wnioskująca o udzielenie informacji złożyła już podobny wniosek w danym roku kalendarzowym. W innych przypadkach można zażądać zwrotu wydatków. Pobrana w związku z tym kwota może podlegać zwrotowi, jeśli dane były przetwarzane nielegalnie lub wniosek o udzielenie informacji doprowadził do poprawienia danych.

Prawa osób, których dane dotyczą mogą być ograniczone ustawowo ze względów bezpieczeństwa wewnętrznego i zewnętrznego państwa, np. ze względów obrony i bezpieczeństwa narodowego

oraz zapobiegania i wykrywania przestępczości, ze względu na interes gospodarczy lub finansowy Unii Europejskiej, w celu zapobieżenia ujawnieniu (każdorazowo objętych nadzorem i kontrolą) wykroczeń o charakterze zawodowym, dyscyplinarnym lub etycznym bądź naruszeń prawa pracy lub przepisów w zakresie bezpieczeństwa i higieny pracy oraz dla ochrony praw osób, których dane dotyczą lub innych osób (art. 16 ustawy DP&FOI).

Ważne:

- Należy bezpośrednio poinformować osobę, której dane dotyczą, że zamierają Państwo zbierać jej dane przed rozpoczęciem ich zbierania. Informacje muszą zostać udzielone indywidualnie i nie mogą mieć innej postaci, np. ogłoszenia czy noty zawartej np. w treści regulacji, jeśli osoba zainteresowana nie ma możliwości bezpośredniego zaznajomienia się z treścią takiej dokumentacji.
- Nie istnieje określona forma, w jakiej należy powiadomić osobę, której dane dotyczą o rozpoczęciu zbierania danych (można to zrobić osobiście, pisemnie, telefonicznie itp.), zaleca się jednak wykorzystanie drogi formalnej (np. formy pisemnej). Należy pamiętać, że w przypadku ewentualnego sporu dotyczącego wypełnienia obowiązku informacyjnego, administrator zobowiązany będzie dostarczyć dowodów, że obowiązek ten został spełniony.
- Należy zawsze udostępniać zebrane informacje osobie, której dane dotyczą.
- Osoba, której dane dotyczą ma prawo dostępu do informacji, ich poprawiania, usuwania oraz żądania zaprzestania ich dalszego przetwarzania.
- Jeśli nie uzyskali Państwo informacji bezpośrednio od osoby, której dane dotyczą (np. jeśli kupili Państwo zbiór danych od innej firmy), powinni Państwo niezwłocznie poinformować osobę, której dane dotyczą o przetwarzaniu danych i źródle informacji. Nie wolno Państwu podejmować żadnej działalności marketingowej nie informując osób, których dane uzyskali Państwo w sposób pośredni i nie dając im możliwości wyrażenia sprzeciwu wobec przetwarzania ich danych dla celów marketingowych.

Bezpieczeństwo danych

Jednym z podstawowych obowiązków administratora jest zapewnienie bezpieczeństwa danych, tj. wdrożenie odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem lub przypadkową utratą, zmianą, nieuprawnionym ujawnieniem lub dostępem, w szczególności w przypadkach, w których przetwarzanie obejmuje przekazywanie danych przez sieć, oraz przed wszystkimi innymi bezprawnymi formami przetwarzania. Zastosowane środki muszą być odpowiednie do zagrożenia i do kategorii danych oraz odzwierciedlać stan wiedzy w tej dziedzinie. Zapewnienie bezpieczeństwa danych to proces o charakterze ciągłym, który obejmuje analizę ryzyka i powinien również uwzględniać zmienne okoliczności wpływające na poziom i charakter istniejących zagrożeń.

Obowiązek zabezpieczenia danych spoczywa na każdym administratorze (niezależnie od jego wielkości) i każdym podmiocie, któremu zlecono przetwarzanie danych.

Zabezpieczanie danych oznacza nie tylko wdrożenie środków organizacyjnych, takich jak przygotowanie specjalnej dokumentacji opisującej przetwarzanie danych i ich ochronę czy powołanie administratora bezpieczeństwa informacji, ale także zastosowanie ściśle określonych środków technicznych.

Zastosowanie środków bezpieczeństwa może być związane z potrzebą wprowadzenia uznanych standardów bezpieczeństwa lub bezpośredniego zastosowania przepisów o ochronie danych, które mogą zawierać szczegółowe wymogi w tym zakresie.

Środki bezpieczeństwa powinny zależeć od środowiska, w którym przetwarzane są dane. W przypadku sieci informatycznych, bezpieczeństwo danych osobowych można uznać za tożsame z bezpieczeństwem informacji, oznaczającym zapewnienie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i wiarygodności. Terminy te mają następujące znaczenie:

- Poufność** – zapewnienie, że informacje nie będą udostępniane ani ujawniane nieuprawnionym osobom, podmiotom lub procesom,
- Integralność** – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieuprawniony,
- Dostępność** – zapewnienie dostępności i możliwości wykorzystania na żądanie, w określonym terminie, przez uprawniony podmiot,
- Rozliczalność** – zapewnienie możliwości przypisania działań danego podmiotu w sposób jednoznaczny wyłącznie temu podmiotowi,
- Autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest taka sama jak deklarowana (autentyczność odnosi się do użytkowników, procesów, systemów i informacji),
- Niezaprzeczalność** – brak możliwości zaprzeczenia zaangażowaniu, w całości lub w części, w wymianę danych przez jeden z podmiotów uczestniczących w tej wymianie,
- Niezawodność** – zapewnienie spójności oraz planowanych działań i efektów.

Należy podkreślić, że zapewnienie, a następnie wykazanie określonych cech często wymaga zastosowania określonych środków i spełnienia jednocześnie wielu warunków.



Administrator zobowiązany jest między innymi do:

- wyznaczenia administratora bezpieczeństwa informacji nadzorującego przetwarzanie (zaleca się, aby osoba ta miała wiedzę z zakresu ochrony danych osobowych niezbędną dla efektywnego pełnienia swojej funkcji), chyba, że administrator sam wykonuje te czynności;
- prowadzenia dokumentacji opisującej metodę przetwarzania danych oraz wprowadzone środki techniczne i organizacyjne. Dokumentacja ta powinna zawierać politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym;
- zapewnienia nadzoru nad danymi, nad tym, kto i kiedy wprowadził dane do zbioru i do kogo są one przekazywane. Sposób sprawowania takiego nadzoru określa administrator, uwzględniając zastosowane środki techniczne i organizacyjne.
- wydawania upoważnień osobom mającym dostęp do danych osobowych.

Obowiązek wydawania upoważnień oparty jest na art. 37 ustawy. Biorąc pod uwagę cele ewidencyjne i konieczność prowadzenia rejestru upoważnień, powinny one być sporządzone w formie pisemnej i zawierać imię (nazwisko), imię i nazwisko osoby udzielającej upoważnienia do przetwarzania danych, datę wydania i datę wygaśnięcia. Powinny być również określone zakres danych, do których dana osoba ma dostęp i nazwa zbioru danych. Rejestr osób upoważnionych powinien zawierać następujące informacje: imię i nazwisko osoby upoważnionej, datę udzielenia upoważnienia, datę wygaśnięcia oraz zakres upoważnienia do przetwarzania danych i identyfikator, jeśli dane przetwarzane są w systemie informatycznym. Osoby upoważnione do przetwarzania danych mają obowiązek zachować je w tajemnicy. Szczegółowe warunki zabezpieczania danych osobowych określone są w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Rozporządzenie to określa również środki bezpieczeństwa, jakie winny być

zastosowane do ochrony danych. Wybór tych środków zależy od poziomu bezpieczeństwa danych w systemie informatycznym zastosowanym dla danego zbioru danych.



Art. 13 ustawy 101, wykraczający poza ramy dyrektywy 95/46/WE, nakłada na administratora i przetwarzających obowiązek uwzględnienia pewnych zagrożeń i przyjęcia dalszych, szczególnych środków. Ma on zastosowanie przede wszystkim do następujących obowiązków:

1. Opracowania i udokumentowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.
2. Spełnienia, w przypadku zautomatyzowanego przetwarzania danych, następujących wymogów:
 - zapewnienia, że systemy służące do zautomatyzowanego przetwarzania danych osobowych wykorzystywane są jedynie przez osoby uprawnione;
 - zapewnienia, że osoby fizyczne uprawnione do wykorzystywania systemów zautomatyzowanego przetwarzania danych osobowych mają dostęp jedynie do danych odpowiadających zakresowi ich upoważnienia, na podstawie szczegółowych upoważnień dla użytkowników wydawanych wyłącznie takim osobom;
 - sporządzania elektronicznych zapisów umożliwiających ustalenie i weryfikację kiedy, przez kogo i z jakich powodów dane osobowe zostały zapisane lub przetworzone w inny sposób oraz
 - zapobieżenia nieuprawnionemu dostępowi do nośników danych.

Przepisy art. 17(2) i 17(3) dyrektywy, dotyczące relacji pomiędzy administratorami a przetwarzającymi, uwzględnione zostały w art. 6 ustawy 101, ustanawiającym możliwość zawarcia pomiędzy nimi umowy. Obowiązki przetwarzającego regulują różne przepisy ustawy 101, konkretnie jej art. 7 i 8. Art. 16 dyrektywy 95/46/WE został wdrożony w art. 14 i 15 ustawy 101.



Art. 10 ustawy DP&FOI zawiera zasady bezpieczeństwa danych określające wymogi w zakresie przetwarzania. Zapewnienie bezpieczeństwa danych i zastosowanie wszelkich środków technicznych i organizacyjnych oraz opracowanie procedur niezbędnych dla zapewnienia zgodności z ustawą oraz innymi zasadami ochrony danych i poufności należą do obowiązków administratora lub przetwarzającego. Dane muszą być chronione w szczególności przed nieuprawnionym dostępem, zmienianiem, przekazywaniem, upublicznianiem, usunięciem lub zniszczeniem oraz przed przypadkowym zniszczeniem lub uszkodzeniem. Jeśli dane osobowe przekazywane są przez sieć lub za pomocą innych urządzeń technologii informacyjnej, administrator, przetwarzający techniczny oraz operator urządzeń telekomunikacyjnych lub technologii informacyjnej winni zastosować szczególne środki ochrony w celu zapewnienia ochrony technicznej danych osobowych. Art. 31/A ustawy DP&FOI określa przypadki, w których obowiązkowe jest wyznaczenie administratora bezpieczeństwa informacji lub opracowanie zasad ochrony i bezpieczeństwa danych. Artykuł ten stanowi, że należy wyznaczyć wewnętrznego administratora bezpieczeństwa informacji, absolwenta studiów prawniczych, administracyjnych lub informatycznych bądź posiadającego równoważne z ich ukończeniem kwalifikacje, działającego w ramach organizacji administratora lub przetwarzającego i odpowiedzialnego bezpośrednio przed kierownikiem następujących podmiotów:

- administratorów lub przetwarzających prowadzących przetwarzanie lub przetwarzanie techniczne zbiorów danych władz państwowych lub krajowych zbiorów danych o pracownikach lub przestępstwach;
- organizacji finansowych oraz

- dostawców usług telekomunikacyjnych i użyteczności publicznej.

Wewnętrznym administratorem bezpieczeństwa informacji może być pracownik administratora lub osoba wyznaczona do sprawowania tej funkcji.

Wewnętrzny administrator bezpieczeństwa informacji:

- a) uczestniczy lub pomaga w podejmowaniu decyzji związanych z przetwarzaniem danych i egzekwowaniem praw osób, których dane dotyczą;
- b) monitoruje zgodność z ustawą i innymi przepisami prawnymi w zakresie przetwarzania danych oraz z wewnętrznymi zasadami ochrony i bezpieczeństwa informacji i wymogami w zakresie bezpieczeństwa danych;
- c) bada przedłożone mu raporty i wzywa administratora lub przetwarzającego do przerwania wszelkich stwierdzonych przez siebie nielegalnych operacji przetwarzania danych;
- d) opracowuje wewnętrzne zasady ochrony i bezpieczeństwa danych;
- e) prowadzi wewnętrzny rejestr ochrony danych oraz
- f) zapewnia szkolenie pracowników w zakresie ochrony danych.

Administratorzy zobowiązani do wyznaczenia wewnętrznego administratora bezpieczeństwa informacji winni wdrożyć zasady bezpieczeństwa i ochrony danych. Zasady ochrony danych to wiążące wewnętrzne zasady obowiązujące w obrębie organizacji, opisujące szczegółowo przetwarzanie danych i promujące zastosowanie przepisów w zakresie ochrony danych i wykonywanie praw przez osoby, których dane dotyczą. Ustawa DP&FOI nie określa treści zasad ochrony danych w tym kontekście. Trudno byłoby także stworzyć jednolite zasady ochrony danych ze względu na zmienność działań w zakresie przetwarzania danych. Najistotniejsze kwestie do rozstrzygnięcia można jednak streścić w następujący sposób:

- zaadaptowanie zasad określonych w ustawie DP&FOI do indywidualnych potrzeb;
- wspieranie ochrony danych w organizacji;
- zdefiniowanie prawa dostępu;
- zdefiniowanie mechanizmu kontroli;
- wyznaczenie odpowiedzialności w jasny sposób;
- określenie poszczególnych zestawów przetwarzanych danych.

Oznacza to, że zasady ochrony danych stanowią wiążące wewnętrzne instrukcje wydane przez szefa danej organizacji.

Pojęcie to ma duże znaczenie w praktyce rzeczników ochrony danych. Było stosowane, kiedy zachodziły wątpliwości co do prawnej dopuszczalności przetwarzania danych. Na przykład informacje podawane osobie, której dane dotyczą muszą być szczegółowe, a jeśli są niejasne lub niedokładne, osoba, której dane dotyczą może niewłaściwie je zrozumieć. W związku z powyższym uznaje się, że administrator danych naruszył wymóg pozyskiwania i przetwarzania danych w sposób rzetelny i legalny, wchodzący w zakres zasady bezpieczeństwa danych.

Ważne:

- Stosując zabezpieczenia należy wziąć pod uwagę istniejące zagrożenia i charakter przetwarzanych danych.
- Dostęp do danych mogą mieć jedynie osoby odpowiednio upoważnione przez administratora. W poszczególnych krajach mogą istnieć szczególne wymogi określające formę upoważnienia.
- Administrator winien opracować specjalną dokumentację wewnętrzną mającą na celu opisanie procedur przetwarzania danych, wskazującą działania, jakie należy podjąć oraz określającą zasady i reguły postępowania, jakie należy zastosować w celu odpowiedniego zabezpieczenia danych osobowych. Dokumentacja ta powinna przełożyć się na codzienną działalność administratora.
- Administrator winien również określić metodę kontroli stosowaną w celu

- nadzorowania przetwarzania danych, w szczególności tego, jakie dane, gdzie i przez kogo zostały wprowadzone do zbioru i komu zostały przekazane.
- Administrator i wszystkie osoby upoważnione do przetwarzania danych zobowiązane są zachować w tajemnicy dane i metodę ich zabezpieczania.

Obowiązek zgłoszenia do rejestracji

Administrator ma obowiązek zgłoszenia zbioru danych do rejestracji przez organ ochrony danych kraju, w którym firma prowadzi działalność. Obowiązek ten istnieje we wszystkich państwach partnerskich, jednak sposób jego spełniania może być różny w różnych krajach.

Istnieją pewne wyjątki od ogólnego obowiązku zgłaszania zbiorów do rejestracji. Zostały one wymienione w przepisach krajowych w zakresie ochrony danych.

Przed zgłoszeniem zbioru danych do rejestracji, każdy administrator powinien sprawdzić, czy prowadzony przez niego zbiór danych nie jest zwolniony z obowiązku zgłaszania do rejestracji na podstawie tych przepisów.

Należy pamiętać, że rejestracja nie jest jedynym obowiązkiem administratora.



Zgodnie z art. 40 ustawy, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Ochrony Danych Osobowych. Wyjątki od tej reguły wymienione są w art. 43.1 ustawy. Przed zgłoszeniem zbioru do rejestracji, każdy administrator winien sprawdzić, czy prowadzony przez niego zbiór danych nie jest zwolniony z obowiązku rejestracji na podstawie tego przepisu.

Metoda zgłaszania.

Zbiór danych należy zgłaszać do rejestracji za pomocą formularza, którego wzór opublikowany został w przepisach wykonawczych do ustawy.

Wszelkie zmiany informacji zgłoszonych uprzednio do rejestracji należy zgłosić w ciągu 30 dni od daty ich wprowadzenia. Jeśli zatem ulegną zmianie warunki prowadzenia zbioru danych, zmianę taką należy zgłosić Generalnemu Inspektorowi Ochrony Danych Osobowych. Zgłoszeniu podlega również informacja o zaprzestaniu przetwarzania danych osobowych.

Możliwe jest wezwanie strony do przedstawienia innych dokumentów mogących mieć istotne znaczenie (wypisu z Krajowego Rejestru Sądowego, dokumentu polityki bezpieczeństwa, instrukcji zarządzania systemem informatycznym) w związku z postępowaniem administracyjnym prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych w celu rejestracji zbioru. Zgłoszenie zbioru danych do rejestracji i uaktualnienia może zostać dokonane pocztą, osobiście lub za pomocą elektronicznej platformy komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych, platformy e-gido, dostępnej na stronie www.gido.gov.pl.

System e-gido pozwala na zgłaszanie zbiorów danych do rejestracji i ich uaktualnianie przez Internet. W takim przypadku, formularz zgłoszenia wypełnia się za pomocą aplikacji zainstalowanej na stronie www.gido.gov.pl. Zapewnia ona wnioskodawcy przydatne wskazówki i informacje dotyczące prawidłowego wypełniania formularzy. Po wypełnieniu, zgłoszenie może zostać przesłane drogą elektroniczną przez podmioty posiadające podpis elektroniczny. Formularz wypełniony w internecie można również wydrukować i wysłać w sposób tradycyjny.

Zaświadczenie o rejestracji zbioru danych.

Administrator „zwykłych” rejestrowanych danych może rozpocząć ich przetwarzanie po zgłoszeniu zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Zaświadczenie o rejestracji zbioru danych wydaje się na wniosek administratora.

Administrator może rozpocząć zbieranie danych szczególnie chronionych dopiero po rejestracji zbioru danych. Generalny Inspektor Ochrony Danych Osobowych zobowiązany jest wydać zaświadczenie niezwłocznie po rejestracji zbioru danych.

Przykłady zwolnienia z obowiązku zgłaszania zbiorów danych do rejestracji:

- Rejestracja danych pracowników i osób ubiegających się o pracę
Zwolnienie z obowiązku rejestracji zgodnie z art. 43.1(4) ustawy dotyczy zbiorów danych przetwarzanych w związku z zatrudnieniem u administratora (np. zbiorów danych obecnych i dawnych pracowników oraz osób ubiegających się o pracę) czy świadczeniem mu usług na podstawie umów cywilnoprawnych (np. umowy zlecenia lub umowy o dzieło). Takie zbiory nie muszą być zgłaszane do rejestracji.
- Rejestracja zbiorów przetwarzanych w zakresie drobnych bieżących spraw życia codziennego
Obowiązek rejestracji zbioru nie powstaje, jeśli zawarte w nim dane są powszechnie dostępne (art. 43.1(9)) lub przetwarzane w zakresie drobnych bieżących spraw życia codziennego (art. 43.1(11)).
Przetwarzanie danych w celu utrzymywania kontaktu z osobą reprezentującą dany podmiot lub w zakresie niezbędnym dla osiągnięcia tego celu ma za zadanie poprawienie funkcjonowania administratora danych, zatem dane przetwarzane w takim zbiorze można traktować jako dane przetwarzane w zakresie drobnych bieżących spraw życia codziennego.

Zgłoszenie do rejestracji jest nieodpłatne.

Zarejestrowane zbiory danych figurują w krajowym rejestrze zbiorów danych dostępnym w internecie.



Administratorzy mają obowiązek zgłoszenia do OPDP planowanego lub prowadzonego przetwarzania danych osobowych. Zgłoszenie odbywa się w drodze procedury formalnej (pisemnie lub elektronicznie), zgodnie z art.16(2) ustawy 101.

Nie każda operacja przetwarzania podlega obowiązkowi zgłoszenia. Wyjątki wymienione są w art. 18 ustawy 101. W poszczególnych sytuacjach wymienionych w tym artykule, administratorzy winni spełnić szczególny obowiązek informacyjny, tj. zapewnić dostępność wymaganych danych w sposób zdalny lub w innej odpowiedniej formie.

Zasady rejestracji określa ustawa 101. Nie jest ona uregulowana ustawodawstwem o postępowaniu administracyjnym.

Po złożeniu formularza rejestracyjnego w OPDP, jego treść jest sprawdzana pod względem kompletności i w razie potrzeby wzywa się administratora do przekazania dodatkowych informacji w określonym terminie. Jeśli administrator nie dopełni tego obowiązku, zgłoszenie uznaje się za niebyłe.

Jeśli jakiegokolwiek informacje zawarte w zgłoszeniu budzą obawy o możliwe naruszenie prawa podczas przetwarzania, OPDP ma prawo wszcząć postępowanie zgodnie z Kodeksem Administracyjnym. Naturalnie, kontrolerzy mogą dojść do wniosku, że nie ma zagrożenia naruszeniem prawa – w takim przypadku postępowanie jest przerywane. Jeśli zadecydują inaczej, OPDP nakazuje zaprzestanie operacji przetwarzania. Postępowanie takie jest bardzo podobne do procedury kontroli wstępnej opisanej w ustawie 101 (w rozumieniu art. 20 dyrektywy 95/46/WE). Jeśli cel przetwarzania przestaje istnieć, OPDP może zdecydować (z własnej inicjatywy lub na wniosek administratora) o odwołaniu rejestracji. OPDP może także anulować rejestrację w przypadku naruszenia prawa przez administratora. Jeśli administrator planuje zaprzestanie działalności, ma obowiązek poinformować OPDP o tym, jak zamierza postąpić z uprzednio

przetwarzanymi danymi, które zostały zgłoszone i zarejestrowane przez OPDP.

Zgłoszenie i rejestracja są nieodpłatne.

OPDP wykorzystuje zgłoszenia do prowadzenia rejestru operacji przetwarzania, dostępnego publicznie na stronie internetowej OPDP. Informacje o odwołanych rejestracjach są regularnie publikowane w Oficjalnym Dzienniku OPDP. Jedynie informacje dotyczące metod przetwarzania i środków zabezpieczenia danych nie są publicznie dostępne.



Art. 28 ustawy DP&FOI stanowi, że przed rozpoczęciem działalności, administrator przetwarzający dane osobowe winien zgłosić do rejestracji Rzecznikowi Ochrony Danych: cel przetwarzania danych; kategorie danych i podstawy prawne dla ich przetwarzania; zakres osób, których dane dotyczą; źródło danych; kategorie i odbiorców przekazywanych danych oraz podstawy prawne dla przekazywania; limity czasowe dla usunięcia pewnych rodzajów danych; nazwę i adres (siedziby) administratora danych i przetwarzającego, miejsce przetwarzania lub przetwarzania technicznego oraz działania przetwarzającego związane z przetwarzaniem danych. Rzecznik Ochrony Danych wpisuje przetwarzanie do publicznego rejestru.

Rejestr ten nie jest rejestrem upoważnień, wpisanie do niego nie daje prawa do rozpoczęcia przetwarzania. Niedopełnienie obowiązku zgłoszenia lub nieprawidłowe zgłoszenie może stanowić podstawę do wszczęcia postępowania przez Rzecznika Ochrony Danych.

Administratorzy mają obowiązek zgłoszenia przetwarzania, z wyjątkiem kategorii przetwarzania wymienionych w art. 30 ustawy DP&FOI. Zgłoszeniu nie podlegają dane osób zatrudnionych. Wyjątek ten ma zastosowanie również do relacji podobnych do stosunku pracy oraz do innych stosunków prawnych. Przed rozpoczęciem działalności przedsiębiorstwa muszą jednak zgłosić inne kategorie przetwarzania danych, niewymienione jako wyjątki w ustawie DP&FOI, na przykład przetwarzanie danych dla celów marketingu bezpośredniego.

Zgłoszenie jest nieodpłatne i może zostać przeprowadzone drogą elektroniczną, jednak jego wydrukowaną, podpisaną kopię należy przesłać do Rzecznika Ochrony Danych, ponieważ zgłoszenie traktowane jest jako oświadczenie.

Ważne:

- W każdym z krajów partnerskich obowiązek zgłoszenia do rejestracji należy do podstawowych obowiązków administratorów danych.
- W poszczególnych państwach członkowskich UE mogą istnieć różnice w zakresie zgłaszania zbiorów danych do rejestracji. W związku z tym, przed rozpoczęciem działalności gospodarczej w innym państwie członkowskim UE należy zawsze zapoznać się z odpowiednimi przepisami prawnymi dotyczącymi obowiązku rejestracji.
- Poszczególne państwa członkowskie mogą stosować wyjątki od obowiązku rejestracji zbiorów danych – na przykład w przypadku zbiorów danych pracowników. Lista wyjątków może być różna w zależności od kraju.
- Niedopełnienie obowiązku zgłoszenia zbioru danych do rejestracji wynikającego z obowiązujących przepisów może wiązać się z odpowiedzialnością cywilną i karną za naruszenie przepisów o ochronie danych.
- Zmiany w informacjach podlegających zgłoszeniu i usunięcie zbioru wymagają zgłoszenia w określonym terminie.
- Zalecane jest spełnienie obowiązku zgłoszenia przez Internet. W tym celu należy odwiedzić stronę internetową danego organu ochrony danych, aby sprawdzić taką możliwość.
- Zarówno zgłoszenie jak i uaktualnienie zbioru danych muszą odbywać się w oficjalnym języku danego kraju.

Przekazywanie danych do państw trzecich

Przekazywanie danych pomiędzy przedsiębiorcami w Polsce, Czechach i na Węgrzech oraz przekazywanie danych podmiotom w innych państwach członkowskich EOG (państwach członkowskich UE oraz Islandii, Lichtensteinie i Norwegii) traktowane jest jak każde inne przetwarzanie w obrębie każdego z państw partnerskich i nie powoduje powstania dodatkowych zobowiązań.

Istnieją dodatkowe wymogi związane z przekazywaniem danych do państw trzecich (nienależących do EOG). Poza tymi dodatkowymi wymogami, należy wypełnić wszystkie zobowiązania wynikające z przepisów prawa w zakresie ochrony danych.

Co do zasady, dane mogą być przekazywane jedynie odbiorcom z państw trzecich zapewniających odpowiedni poziom ochrony danych osobowych. Bardzo często są to kraje, w odniesieniu do których Komisja Europejska wydała specjalne decyzje stwierdzające, że zapewniają one odpowiedni poziom ochrony danych.

Poszczególne ustawy o ochronie danych zawierają szczegółowe zasady przekazywania danych do państw trzecich, w szczególności w przypadku krajów niezapewniających odpowiedniego poziomu ochrony. Przepisy takie określają szczegółowo postawy prawne dla przekazywania danych i mogą wymagać uzyskania specjalnego upoważnienia (zezwoleń) od właściwego organu ochrony danych. Jeśli kraj, do którego przekazywane są dane, nie zapewnia odpowiedniego poziomu ochrony, należy poinformować o tym, tj. o zagrożeniu ewentualnymi naruszeniami zasad przetwarzania danych, osobę, której dane dotyczą.

Bardzo często administrator musi zagwarantować zapewnienie przez odbiorcę danych odpowiedniego poziomu ochrony danych osobowych i praw osób, których dane dotyczą.

Administratorzy i przetwarzający działający w państwach trzecich mogą zagwarantować odpowiednią ochronę na kilka sposobów:

- a) Stosując zestaw standardowych przepisów przyjętych przez Komisję Europejską, zwanych „Wzorcowymi Klauzulami Umownymi”.

Klauzule te dają podstawę prawną dla przekazywania danych z państw członkowskich UE do państw trzecich. Istnieją dwie grupy klauzul – jedna ma zastosowanie do przekazywania danych administratorom prowadzącym działalność w państwie trzecim, druga reguluje przekazywanie danych przetwarzającym.

Z uwagi na złożony charakter tej kwestii, zaleca się konsultację z krajowym organem ochrony danych.

- b) Stosując klauzule umowne ad hoc.

Poza zastosowaniem Wzorcowych Klauzul Umownych Unii Europejskiej, administratorzy i przetwarzający dane w państwach trzecich oraz organizacje przekazujące dane mogą także ustalić warunki przekazywania danych i zawrzeć w tej sprawie umowę. Umowa taka musi zapewniać odpowiedni poziom ochrony danych osobowych podczas przetwarzania danych przez administratora lub przetwarzającego.

- c) Stosując Wiążące Reguły Korporacyjne (BCR).

Wiążące Reguły Korporacyjne są zwykle opracowywane i stosowane przez firmy międzynarodowe w celu uregulowania przepływu danych pomiędzy ich oddziałami mieszczącymi się w różnych krajach (również poza UE). BCR pozwalają firmom międzynarodowym uregulować wymianę danych pomiędzy wieloma podmiotami za pomocą jednego dokumentu w zakresie ochrony danych, tak aby podmioty uczestniczące w wymianie danych nie musiały zawierać umów z innymi biorącymi w niej udział podmiotami.



Przekazywanie danych do państw trzecich niezapewniających odpowiedniego poziomu ochrony danych osobowych może mieć miejsce jedynie w przypadku, gdy:

- osoba, której dane dotyczą udzieliła pisemnej zgody na przekazywanie jej danych do państw trzecich,
- jest dozwolone na mocy ratyfikowanej umowy międzynarodowej lub przepisu prawa,
- jest niezbędne do wykonania umowy pomiędzy osobą, której dane dotyczą i administratorem lub odbywa się na wniosek osoby, której dane dotyczą,
- jest niezbędne dla realizacji umowy zawartej w interesie osoby, której dane dotyczą pomiędzy administratorem a innym podmiotem,
- jest niezbędne lub wymagane ze względów interesu publicznego lub dla dochodzenia roszczeń,
- jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą,
- dotyczy danych powszechnie dostępnych.

Zgodnie z prawem polskim, przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą (art. 48 ustawy). Należy podkreślić, że przekazywanie danych do państwa trzeciego niezapewniającego odpowiedniego poziomu ochrony możliwe jest jedynie po uzyskaniu pozytywnej decyzji Generalnego Inspektora Ochrony Danych Osobowych – oznacza to, że przekazywanie danych osobowych przed wydaniem takiej decyzji jest nielegalne. Rozpatrując wniosek o zgodę, Generalny Inspektor musi ocenić, czy administrator zapewnia odpowiedni poziom ochrony prywatności, praw i wolności osoby, której dane dotyczą. Każda sprawa rozpatrywana jest indywidualnie, w oparciu o okoliczności faktyczne.



Przed przekazaniem danych za granicę, administratorzy muszą uzyskać zezwolenie OPDP. Zezwolenie (upoważnienie) takie nie jest niezbędne, jeśli swobodny przepływ danych zapewniają umowa międzynarodowa lub decyzja organu UE. W związku z powyższym, za państwa zapewniające odpowiedni poziom ochrony uznaje się te, które ratyfikowały Konwencję 108 Rady Europy i przyjęły odpowiednie przepisy w zakresie ochrony danych osobowych. Administratorzy mający siedzibę poza terytorium UE, którzy przetwarzają dane na terytorium Czech, zobowiązani są wyznaczyć i upoważnić przetwarzającego mającego siedzibę w Czechach. Informacje o sposobie uzyskania zgody na przekazywanie danych za granicę można znaleźć na stronie internetowej OPDP, pod adresem <http://www.uoou.cz/>.



Zgodnie z art. 9 ust. (1) ustawy LXIII z roku 1992 o ochronie danych osobowych i dostępie do informacji publicznej (zwanej dalej ustawą o ochronie danych), dane osobowe nie mogą być przekazywane administratorom lub przetwarzającym w państwach trzecich, chyba że osoba, której dane dotyczą wyraziła na to wyraźną zgodę lub jest to przewidziane ustawą, a podczas przetwarzania przekazanych danych przez administratora lub przetwarzającego zapewniony jest odpowiedni poziom ochrony danych osobowych w państwie trzecim. Nie jest wymagane uzyskanie zezwolenia od organu ochrony danych.

W praktyce, zasady te oznaczają konieczność uzyskania zgody osoby, której dane dotyczą, ponieważ nie ma obecnie żadnej ustawy przewidującej przekazywanie danych w ramach stosunku pracy.

Należy zauważyć, że jeśli osoba, której dane dotyczą udzieliła wyraźnej zgody na przekazanie

jej danych, warunek odpowiedniego poziomu ochrony w państwie trzecim nie ma zastosowania, choć rzecz jasna zaleca się sprawdzenie, czy warunek ten został spełniony. Zgodnie z istniejącą praktyką w zakresie ochrony danych, jeśli dane mają zostać przekazane do kraju niezapewniającego odpowiedniego poziomu ochrony, należy poinformować o tym, tj. o zagrożeniu ewentualnymi naruszeniami zasad przetwarzania danych, osobę, której dane dotyczą. Jedynie po uzyskaniu takiej informacji osoba, której dane dotyczą może udzielić wyraźnej zgody, wymaganej przepisami prawa. Jeśli nie otrzymała ona takich informacji, nie może stwierdzić, w jaki sposób przetwarzanie danych może wpłynąć na jej prawa.

Często pojawia się pytanie, czy zgoda osoby, której dane dotyczą jest potrzebna również w przypadku przekazywania danych do krajów EOG, które uznaje się za przekazywanie danych w obrębie terytorium Węgier. Jako że, zgodnie z art. 8, zgoda osoby, której dane dotyczą jest niezbędna dla przekazywania danych (tj. przetwarzania danych przez administratora) nawet w obrębie terytorium Węgier, zgoda taka jest niezbędna również w przypadku przekazywania danych do krajów EOG. Jeśli jednak dane nie są przekazywane do kraju EOG w celu ich przetwarzania przez administratora, a jedynie przez przetwarzającego, wystarczy poinformować o tym osobę, której dane dotyczą. W takim przypadku, zgoda osoby, której dane dotyczą nie jest wymagana, ponieważ nie jest również niezbędna na Węgrzech w przypadku przekazywania danych w celu ich przetwarzania przez przetwarzającego. Jeśli jednak dane nie są przekazywane do kraju EOG, a do innego państwa trzeciego, należy uzyskać zgodę osoby, której dane dotyczą, ponieważ wspomniany powyżej art. 9 ust. (1) wyraźnie mówi o przekazywaniu w celu przetwarzania danych przez przetwarzającego. Jak wskazano powyżej, zgodnie z ustawą o ochronie danych zapewnienie odpowiedniego poziomu ochrony danych nie jest warunkiem koniecznym legalności przekazywania danych jeśli osoba, której dane dotyczą udzieli na nie zgody. Osoba lub organizacja przekazująca dane i ich odbiorca (tj. eksporter i importer danych) mogą jednak zawrzeć umowę w celu zapewnienia odpowiedniego poziomu ochrony, wykorzystując wiążące reguły korporacyjne lub pakiety wzorcowych klauzul umownych określone w decyzjach Komisji Europejskiej. Należy jednak podkreślić, że istnienie takiej umowy nie stanowi podstawy prawnej dla przekazywania danych – może jedynie zapewnić określony poziom ochrony. Jak zatem stwierdzono, co do zasady konieczne jest uzyskanie zgody osoby, której dane dotyczą.

Ważne:

- Przekazywanie danych do Polski, Czech i Węgier oraz do innych państw należących do Europejskiego Obszaru Gospodarczego traktowane jest jako przekazywanie krajowe i nie wymaga żadnych dodatkowych gwarancji.
- Przekazywanie danych do państw trzecich pociąga za sobą konieczność spełnienia dodatkowych wymogów i co do zasady jest możliwe, jeśli dane państwo zapewnia odpowiedni poziom ochrony danych osobowych.
- Przed planowanym przekazaniem danych należy dokładnie sprawdzić warunki określone w prawie krajowym poszczególnych państw, np. czy wymagana jest zgoda organu ochrony danych.
- Spełnienie wymogów w zakresie przekazywania danych do państw trzecich nie stanowi przesłanki legalności przetwarzania danych osobowych.
- Dane mogą być przekazywane do państw trzecich jedynie dla celów operacji przetwarzania dozwolonych przepisami prawa w poszczególnych państwach partnerskich.
- Jeśli do przekazania danych niezbędne jest upoważnienie, odpowiedni wniosek musi zostać napisany w oficjalnym języku danego kraju i spełniać wszelkie wymogi formalne określone w prawie krajowym.

4. DANE OSOBOWE JAKO PRZEDMIOT DZIAŁALNOŚCI GOSPODARCZEJ

4.1 Przetwarzanie danych w cyklu biznesowym

Rozpoczęcie działalności gospodarczej pociąga za sobą upublicznienie rozmaitych informacji dotyczących przedsiębiorcy i pracowników, należy zatem zwracać szczególną uwagę na wszelkie działania związane ze zbieraniem i dalszym przetwarzaniem danych osobowych w każdym obszarze działalności firmy i na każdym poziomie jej wewnętrznej hierarchii.

Rejestracja spółki

Przedsiębiorcy rozważający rozpoczęcie lub rozszerzenie działalności na inne państwo członkowskie UE powinni zaznajomić się z przepisami szczególnymi dotyczącymi rejestracji działalności gospodarczej. Rozpoczynając działalność, przedsiębiorcy muszą zarejestrować ją w rejestrach publicznych, w tym w rejestrze przedsiębiorców, urzędzie statystycznym, urzędzie ubezpieczeń społecznych, urzędzie podatkowym itp. Zakres podawanych informacji zależy od formy, w jakiej prowadzona będzie działalność gospodarcza. Przedsiębiorcy mogą również być zobowiązani do podania identyfikujących ich informacji handlowych.



Przedsiębiorcy zamierzający prowadzić działalność jednoosobową lub wspólnie z innymi przedsiębiorcami na mocy umowy spółki powinni zgłosić to do Centralnej Ewidencji i Informacji o Działalności Gospodarczej na oficjalnym formularzu on-line, listem poleconym lub osobiście w wybranym urzędzie gminy. Do 1 lipca 2011 r. takie wnioski zgłaszano odpowiedniemu prezydentowi miasta, burmistrzowi lub wójtowi, prowadzącemu ewidencję działalności gospodarczej. Zgodnie z art. 7a ustawy o działalności gospodarczej, dane wpisane już do ewidencji są jawne i nie podlegają ochronie danych. We wniosku o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej tak jak wcześniej do ewidencji działalności gospodarczej, należy zawrzeć informacje dotyczące przedsiębiorcy ściśle związane z prowadzoną przez niego działalnością, które zostały określone odpowiednimi przepisami.

Warto wspomnieć o art. 37.1 ustawy o swobodzie działalności gospodarczej, która weszła w życie 1 lipca 2011 roku. Artykuł ten umożliwia ujawnianie danych i informacji o przedsiębiorcach będących osobami fizycznymi w rozumieniu art. 25.1, poza ich numerem PESEL i adresem zamieszkania, jeśli jest on tożsamy z miejscem prowadzenia działalności. Numer PESEL nie służy do identyfikacji przedsiębiorcy, a osoby fizycznej. Ustawodawca chciał zezwolić na ujawnienie informacji związanych jedynie z działalnością gospodarczą prowadzoną przez przedsiębiorcę wpisanego do ewidencji, nie z jego życiem prywatnym. Dane i informacje udostępnione przez Centralną Ewidencję i Informację o Działalności Gospodarczej są jawne. Każdy ma prawo dostępu do danych i informacji udostępnianych przez CEIDG. Dane i informacje są udostępniane na stronie internetowej.



W związku z założeniem i prowadzeniem spółki, dane osobowe przedsiębiorców są przechowywane w dwóch publicznych rejestrach utworzonych na mocy Kodeksu Handlowego (ustawa nr 513/1991 Coll.) i ustawy o licencjach handlowych (nr 455/1991 Coll.): Rejestrze Spółek (Obchodní rejstřík) i Rejestrze Handlowym (Živnostenský rejstřík).

W Rejestrze Spółek znajdują się następujące informacje: imię, nazwisko, adres domowy i numer identyfikacyjny (lub data urodzenia, jeśli nie nadano takiego numeru) przedsiębiorcy będącego organem statutowym osoby prawnej. Można również zbierać te same dane o członkach organu statutowego osoby prawnej bądź o innych przedsiębiorcach w przypadkach wymienionych w Kodeksie Handlowym. Rejestr Spółek jest publicznie dostępny. Rejestr Handlowy również jest publiczny, z wyłączeniem numerów identyfikacyjnych i informacji o grzywnach nałożonych na przedsiębiorców w związku z prowadzeniem przez nich działalności gospodarczej.



Działalność gospodarcza prowadzona jest głównie przez organizacje (spółki) i podmioty niebędące osobami prawnymi. Spółki są zakładane i rejestrowane za pośrednictwem osób fizycznych, których dane identyfikacyjne powinny pochodzić z wiarygodnego źródła (np. dokumentu tożsamości). Na pierwszym etapie zakładania działalności gospodarczej najistotniejszą kwestią jest przedstawienie dokładnych danych identyfikacyjnych zainteresowanych osób fizycznych.

Niektóre dane osobowe właścicieli i przedstawicieli spółek są publicznie dostępne zarówno na etapie zakładania działalności gospodarczej, jak i podczas jej prowadzenia. Podstawową cechą węgierskiego rejestru spółek (cégnyilvántartás) jest jego publiczny charakter. Nazwiska, adresy zamieszkania i numery identyfikacji podatkowej przedstawicieli spółek wpisanych do rejestru spółek są publicznie dostępne.

Rozpoczęcie działalności gospodarczej

Rozpoczęcie działalności gospodarczej wiąże się z koniecznością wypełnienia rozmaitych zobowiązań wynikających z przepisów o ochronie danych osobowych, w zależności od zakresu przetwarzania danych prowadzonego w ramach takiej działalności i od daty rozpoczęcia operacji przetwarzania. Przedsiębiorca rozpoczynający działalność niewątpliwie powinien przeanalizować, dla jakich celów i w jakim zakresie będą przetwarzane dane osobowe oraz zapewnić wypełnienie wymogów określonych w rozdziale 2, w szczególności legalności, odpowiedniości, wypełnienia obowiązku informacyjnego, bezpieczeństwa danych i – jeśli istnieje taki wymóg – zgłoszenia zbiorów danych osobowych do rejestracji.

Z praktycznego punktu widzenia, w momencie rozpoczynania działalności kluczowe znaczenie ma sporządzenie dokumentacji przetwarzania danych i zgłoszenie prowadzonych zbiorów danych do rejestracji przed rozpoczęciem ich przetwarzania. Jeśli planowane jest zbieranie danych osobowych, należy opracować formularz o odpowiedniej treści.

Likwidacja spółki/zakończenie działalności

W przypadku likwidacji lub upadłości przedsiębiorcy, możliwe jest przetwarzanie informacji identyfikujących tego przedsiębiorcę lub jego przedstawicieli. Zasady takiego przetwarzania zostały określone w odrębnych przepisach, regulujących postępowanie upadłościowe i naprawcze. W tym kontekście należy pamiętać, że przedsiębiorcy mogą również być wpisywani do rozmaitych rejestrów dłużników na mocy odrębnych przepisów.

Likwidacja spółki nie zwalnia przedsiębiorcy lub osób prowadzących przetwarzanie z obowiązków wynikających z przepisów o ochronie danych osobowych. W szczególności należy pamiętać o zachowaniu zgodności z zasadami celowości i legalności danych osobowych przetwarzanych przez taki podmiot.

Po zakończeniu działalności gospodarczej, istnieje obowiązek przechowywania różnych rodzajów dokumentacji przez określony czas.



Zgodnie z art. 51.1 ustawy o narodowym zasobie archiwalnym i archiwach, w przypadku likwidacji lub upadłości pracodawcy, ma on obowiązek wskazać podmiot prowadzący działalność gospodarczą w zakresie przechowywania dokumentacji, do którego przekaże swoją dokumentację w celu dalszego przechowywania, oraz zapewnić niezbędne fundusze do końca 50-letniego okresu przechowywania dokumentacji, rozpoczynającego się 1) w dniu zakończenia pracy dla danego pracodawcy – w przypadku dokumentacji personalnej; 2) w dniu sporządzenia – w przypadku dokumentacji płacowej. W przypadku, gdy sąd rejestrowy stwierdzi – na wniosek pracodawcy wpisanego do Krajowego Rejestru Sądowego lub ewidencji działalności gospodarczej – że niemożliwe jest zapewnienie środków na pokrycie kosztów dalszego przechowywania, dokumentację przejmuje archiwum państwowe, ustanowione w tym celu przez Ministra Kultury i Dziedzictwa Narodowego. Przed wydaniem decyzji w takiej sprawie, sąd winien skonsultować się z naczelnikiem urzędu podatkowego właściwego dla siedziby pracodawcy w kwestii sytuacji finansowej pracodawcy.



W związku z upadłością, możliwe jest przetwarzanie danych osobowych zadłużonych przedsiębiorców w rejestrze upadłości (prowadzonym zgodnie z ustawą o upadłości – nr 182/2006 Coll.), który jest publicznie dostępny, z wyjątkiem danych określonych w ustawie o upadłości. Jeśli dłużnik jest osobą fizyczną, jego imię, nazwisko, adres domowy i numer identyfikacyjny (lub, jeśli nie został nadany, data urodzenia) są wpisywane na listę dłużników. Jeśli jest osobą prywatną z zarejestrowaną siedzibą, działającą na mocy przepisów szczególnych, na listę dłużników wpisuje się również siedzibę. Jeśli dłużnik jest przedsiębiorcą, na listę wpisuje się również informacje identyfikujące jego firmę oraz jej siedzibę (jeśli jej adres jest różny od adresu domowego) i numer identyfikacyjny.

We wszystkich wyżej wymienionych przypadkach, przetwarzanie danych jest kwalifikowane na mocy czeskiej ustawy o ochronie danych jako przetwarzanie bez zgody osoby, której dane dotyczą, na podstawie faktu, że jest ono niezbędne dla wypełnienia zobowiązań prawnych administratora.

W przypadku zakończenia działalności gospodarczej, dane osobowe klientów można potraktować na dwa sposoby – zlikwidować (usunąć) je lub, zgodnie z obowiązującymi przepisami, przekazać je innemu podmiotowi.



Zgodnie z ustawą, w przypadku likwidacji akta pracowników należy przekazać administratorowi – osobie powołanej do prowadzenia takich akt.

4.2 Przetwarzanie danych osobowych w związku z zatrudnieniem

Przetwarzanie danych pracowników w okresie zatrudnienia

Pracodawca zobowiązany jest do przetwarzania danych osobowych pracowników w sposób i w okresie niezbędnym dla celów zarządzania zasobami ludzkimi. Szczegółowy zakres danych, które mogą być przetwarzane przez pracodawcę regulują szczególne przepisy prawne poszczególnych krajów. Zakres ten obejmuje obszary ubezpieczenia społecznego i zdrowotnego oraz, w większości krajów, podatki.

Podczas przetwarzania danych pracowników, pracodawcy muszą mieć świadomość ich prawa do ochrony prywatności w miejscu pracy. Chociaż należy uwzględnić potrzebę kontroli pracy pracowników i wykorzystania przez nich zasobów firmy, pracodawcy powinni pamiętać, że pracownikom również przysługują określone prawa.

W niniejszym rozdziale skoncentrujemy się na zakresie technik i metod nadzoru, które mogą zostać zastosowane przez pracodawców zgodnie z przepisami o ochronie danych. Wykorzystanie rozmaitych technik nadzoru może być uzasadnione szczególnym charakterem pracy i działalności gospodarczej, jednak pracodawca ma obowiązek poinformowania pracowników o mechanizmach kontroli wykorzystywanych w spółce i sposobie ich zastosowania.



Podstawę prawną dla przetwarzania danych osobowych pracowników przez pracodawcę stanowi ustawa z dnia 26 czerwca 1974 roku Kodeks Pracy i przepisy wykonawcze do niego, w szczególności rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika.

Informacje o pracowniku, takie jak jego imię i nazwisko czy służbowy adres e-mail, są ściśle związane z wykonywaną przez niego pracą i jej wykonywaniem. Informacje takie mogą zatem zostać podane do publicznej wiadomości przez pracodawcę, również bez zgody pracownika. Zasada ta została potwierdzona przez Sąd Najwyższy w wyroku z dnia 19 listopada 2003 r., sygnatura akt I PK 590/02, stwierdzającym, że „Nazwisko (i imię) jest skierowanym na zewnątrz znakiem rozpoznawczym osoby fizycznej i ujawnienie go w celu jej identyfikacji nie może być zasadniczo uznane za bezprawne, o ile nie łączy się z naruszeniem innego dobra osobistego, np. czci, prywatności lub godności osobistej. Ujawnienie przez pracodawcę nazwiska (imienia) pracownika bez jego zgody nie stanowi bezprawnego naruszenia dobra osobistego, jeżeli jest usprawiedliwione zadaniami i obowiązkami pracodawcy związanymi z prowadzeniem zakładu, jest niezbędne i nie narusza praw oraz wolności pracownika”. W swoim wyroku Sąd Najwyższy wskazał również, że „najistotniejszym składnikiem zakładu pracy (przedsiębiorstwa) są ludzie, a funkcjonowanie zakładu wiąże się nierozłącznie z kontaktami zewnętrznymi – z kontrahentami, klientami(...) Dlatego pracodawca nie może być pozbawiony możliwości ujawniania nazwisk pracowników, zajmujących określone stanowiska w ramach instytucji. Przeciwnie stanowisko prowadziłoby do sparaliżowania lub poważnego ograniczenia możliwości działania pracodawcy, bez żadnego rozsądnego uzasadnienia w ochronie interesów i praw pracownika. (...) Imiona i nazwiska pracowników widnieją na drzwiach w zakładach pracy, umieszcza się je na pieczętkach imiennych, pismach sporządzanych w związku z pracą, prezentuje w informatorach o instytucjach i przedsiębiorstwach, co oznacza że zgodnie z powszechną praktyką są one zasadniczo jawne”.

Pracodawca może wymagać również innych informacji lub dokumentów w celu sprawdzenia uprawnienia danej osoby do otrzymywania zasiłków z funduszu świadczeń pracowniczych. Zgodnie z art. 8.1 tej ustawy, przyznawanie ulgowych usług i świadczeń oraz wysokość dopłat

z Funduszu uzależnia się od sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu. zasady i warunki korzystania z usług i świadczeń finansowanych z Funduszu, z uwzględnieniem ust. 1, oraz zasady przeznaczania środków Funduszu na poszczególne cele i rodzaje działalności socjalnej określa pracodawca w regulaminie (art. 8.2). Wspomniane powyżej przepisy nie wskazują dokładnie, jakich informacji pracodawca może zażądać od pracownika w celu przyznania mu zasiłków socjalnych z funduszu świadczeń pracowniczych. W związku z tym, zgodnie z zasadami ogólnymi, w celu przyznania zasiłków z funduszu socjalnego pracodawca może wymagać jedynie takich informacji o pracowniku, jakie są odpowiednie (niezbędne) dla tego celu. Biorąc pod uwagę, że ustawodawca zapewnił jedynie ogólne wytyczne związane z danymi osobowymi, jakich pracodawca może wymagać od pracownika w celu przyznania mu zasiłków z funduszu socjalnego, kwestia ta powinna być szczegółowo uregulowana w regulaminie pracodawcy.

Jeśli chodzi o możliwość monitorowania pracowników, np. sprawdzania sposobu korzystania przez nich z Internetu, sprawdzania ich korespondencji e-mailowej itp., mechanizmom takim muszą towarzyszyć zasady regulujące wykorzystanie tych technologii przez pracowników oraz wcześniejsze powiadomienie pracowników o wprowadzeniu określonych środków.

Zabronione są praktyki związane z kontrolowaniem czasu pracy przy użyciu czytników biometrycznych.



W przypadku zatrudnienia stałego, pracodawca ma prawo, a nawet obowiązek, przetwarzania pewnych danych o pracownikach w sposób, przez okres i z zachowaniem jakości określonej w szczególnych przepisach prawnych lub w sposób niezbędny dla celów zarządzania zasobami ludzkimi w zakresie określonym przez ustawę o ochronie danych i art. 316(4) Kodeksu Pracy.

Z punktu widzenia szczególnych przepisów prawa, w przypadku przetwarzania danych prowadzonego na podstawie przepisów art. (5)(2)(a) i (9)(d) ustawy o ochronie danych, należy podkreślić, że zakres danych, jakie pracodawcy mogą przetwarzać dla celów szczególnych, jest bardzo szeroki. W związku z powyższym, oraz z faktem, że przepisy szczególne są często nowelizowane, podawanie ich pełnej listy nie miałoby sensu.

Istnieją jednak szczególnie istotne przepisy prawa, zobowiązujące pracodawców do przetwarzania danych osobowych dla określonych w nich celów. Są to:

- a) Ustawa nr 262/2006 Coll. Kodeks Pracy, z późniejszymi zmianami – np. art. 96 (rejestracja godzin pracy, nadgodziny, praca nocna, dyżury), art. 105 (informacje o obrażeniach odniesionych w miejscu pracy i chorobach zawodowych),
- b) Ustawa nr 187/2006 Coll. o ubezpieczeniach zdrowotnych, z późniejszymi zmianami,
- c) Ustawa nr 582/1991 Coll. o organizacji i zastosowaniu ubezpieczeń społecznych, z późniejszymi zmianami,
- d) Ustawa nr 48/1997 Coll. o publicznym ubezpieczeniu zdrowotnym, z późniejszymi zmianami,
- e) Ustawa nr 117/1995 Coll. o państwowych zasiłkach społecznych, z późniejszymi zmianami,
- f) Ustawa nr 592/1992 Coll. o składkach na ogólne ubezpieczenie zdrowotne, z późniejszymi zmianami,
- g) Ustawa nr 586/1992 Coll. o podatku dochodowym, z późniejszymi zmianami,
- h) Ustawa nr 337/1992 Coll. o zarządzaniu podatkami i opłatami, z późniejszymi zmianami, oraz ustawa nr 280/2009 Coll. Ordynacja Podatkowa.

Powyższe przepisy odnoszą się przede wszystkim do podatków i ubezpieczeń zdrowotnych. Istnieją również szczególne przepisy zawodowe, uprawniające pracodawców do przetwarzania danych osobowych, np. ustawa nr 49/1997 Coll. o lotnictwie cywilnym i nowelizowana

ustawa nr 455/1991 Coll. o handlu (ustawa o licencjach handlowych), ustawa nr 61/2000 Coll. o żegludze morskiej, a także przepisy wykonawcze do niej, czy ustawa 114/1995 Coll. o żegludze śródlądowej, z późniejszymi zmianami.

Przepisy te określają w ogólny sposób okres przechowywania danych przez pracodawców. Jeśli okres ten nie zostanie określony, pracodawcy mogą przechowywać dane do końca okresu przedawnienia, subiektywnego bądź obiektywnego, określonego w art. 333 Kodeksu Pracy. Dane mogą być przechowywane w różnych celach, np. jako dokumentacja na wypadek zaistnienia sporów bądź jako dowód do przedstawienia władzom, że zostały wypełnione określone zobowiązania.

W kontekście zatrudnienia istotne są przepisy art. 312 Kodeksu Pracy w sprawie akt pracowników. Zgodnie z tą ustawą „Pracodawca ma prawo przechowywać akta osobowe pracowników. Akta osobowe mogą zawierać wyłącznie dokumenty niezbędne dla wykonywania pracy w ramach stosunku pracy. Jedynie wysocy rangą pracownicy, przełożeni pracownika, mają prawo do przeglądania akt. Pracownicy Organu Inspekcji Pracy, Organu Zatrudnienia, sądów, prokuratury, policji, Narodowego Biura Bezpieczeństwa i służb wywiadowczych mają prawo dostępu do akt osobowych oraz sporządzania z nich wypisów i kopii na koszt swego pracodawcy”.

Akta osobowe mogą być także przechowywane na podstawie art. 5.2(a) i art. 9(d) ustawy o ochronie danych.

Pracodawcy mają również prawo umieszczać w aktach osobowych np. wzmianki o naruszeniach przepisów prawa pracy związanych z pracą wykonywaną przez pracownika (art. 52(g) Kodeksu Pracy). Art. 316 ust. 1-3 Kodeksu Pracy stanowi, że pracownikom nie wolno wykorzystywać narzędzi pracy i produkcji należących do pracodawcy, w tym urządzeń informatycznych i telekomunikacyjnych, dla własnych potrzeb bez zgody pracodawcy. Pracodawcy mają prawo w odpowiedni sposób nadzorować przestrzeganie tej zasady (art. 316.1 Kodeksu Pracy). Ponadto, „pracodawcom nie wolno wkraczać w sferę prywatną pracowników bez istotnego powodu związanego ze szczególnym charakterem działalności pracodawcy, w miejscach pracy oraz częściach wspólnych siedziby pracodawcy, poprzez ukryte lub jawne monitorowanie pracowników, przechwytywanie i nagrywanie ich rozmów telefonicznych, czytanie ich poczty elektronicznej bądź sprawdzanie przesyłek adresowanych do pracowników” (art. 316.2 Kodeksu Pracy). Jednak „jeśli pracodawcy mają istotny powód wynikający ze szczególnego charakteru swojej działalności, uzasadniający zastosowanie mechanizmów kontrolnych zgodnie z art. 2, mają obowiązek bezpośrednio poinformować pracowników o zakresie i sposobie prowadzenia monitoringu” (art. 316.3 Kodeksu Pracy). Poza obowiązkiem informacyjnym, pracodawcy winni wypełnić obowiązki wynikające z ustawy o ochronie danych, jeśli ma ona zastosowanie do ich działalności.



Jakiego rodzaju dane o stosunku pracy można przetwarzać? Zgodnie z praktyką Rzecznika Ochrony Danych, zastosowanie art. 77 Kodeksu Pracy podczas trwania stosunku pracy jest niezgodne z Konstytucją. Kodeks Pracy nie reguluje tej kwestii, zatem w okresie trwania stosunku pracy można przetwarzać nowe dane osobowe jedynie jeśli osoba, której dane dotyczą wyraziła na to zgodę, zgodnie z art. 3. (3) ustawy DP&FOI.

Istotne są również przypadki, w których pracodawca może kontrolować pracę wykonywaną przez pracownika i wykorzystanie przez niego sprzętu w miejscu pracy.

1. *Systemy nadzoru.* Istnieją dwie podstawy dla wykorzystania systemów nadzoru w miejscu pracy. Pierwszą z nich jest ochrona sprzętu o dużej wartości – np. możliwe jest zastosowanie kamery w magazynie. Druga to obserwowanie i sprawdzanie intensywności

pracy pracowników. Zgodnie z praktyką Rzecznika Ochrony Danych, druga podstawa nie upoważnia do instalacji systemu nadzoru, chyba, że obraz z kamery nie jest nagrywany. Taki rodzaj systemu nadzoru narusza prawo do prywatności obserwowanych osób.

2. *Wykorzystanie skrzynki e-mailowej.* Pracodawcy nie wolno bezpośrednio sprawdzać skrzynek e-mailowych pracowników, nawet jeśli są one wykorzystywane jedynie dla celów zawodowych, a pracodawca uzyska zgodę pracownika. Wynika to z faktu, że w skrzynce mogą znajdować się listy chronione prawem ze względu na przynależność do sfery prywatnej. Jeśli pracodawca chce sprawdzić treść listów, może poprosić pracownika o ich pokazanie, a pracownik ma prawo nie ujawniać prywatnej korespondencji.
Z drugiej strony, pracodawca ma prawo zapoznać się bezpośrednio z treścią listów pisanych przez pracownika. Były Rzecznik Ochrony Danych uzasadniał to faktem, że pracownik nie ma wpływu na treść listów przychodzących, a jedynie na wychodzące.
3. *Wykorzystanie Internetu.* Pracodawcy często chcą kontrolować wykorzystanie Internetu. Rzecznik Ochrony Danych podkreślił znaczenie zasady minimalizacji danych w takim przypadku: jeśli pracodawca chce ograniczyć wykorzystanie Internetu jedynie do celów oficjalnych, powinien ograniczyć dostęp jedynie do stron internetowych potrzebnych do pracy. Jeśli nie jest to możliwe, może prowadzić rejestr odwiedzanych stron.
4. *Komputer.* Należy rozróżnić status prawny komputera jako przedmiotu i danych przechowywanych na komputerze. Oznacza to, że pracodawca nie ma prawa dostępu do danych przechowywanych na komputerze dla potrzeb zawodowych – chyba, że dane są przechowywane z naruszeniem przepisów prawa pracy.
5. *Telefon.* Wykorzystanie telefonów może generować wysokie koszty, a ich wykorzystanie do celów prywatnych tworzy obowiązek podatkowy. Z tego względu pracodawcy często chcą sprawdzać wykorzystanie telefonu. Zgodnie z praktyką Rzecznika Ochrony Danych, nielegalne jest tworzenie list rozmów prowadzonych przez pracownika oraz podsłuchiwanie lub nagrywanie ich bez zgody pracownika.
6. *Lokalizacja GPS, informacje o telefonach komórkowych.* Jednym z podstawowych obowiązków pracownika jest obecność w miejscu i czasie wskazanym przez pracodawcę. Z tego względu oraz ze względów organizacji pracy, pracownicy często sprawdzają lokalizację pracowników przez GPS lub informacje o telefonach komórkowych. Według Rzecznika Ochrony Danych, narzędzia te mogą być wykorzystywane jedynie jeśli jest to uzasadnione ze względów logistycznych, a celów kontroli nie można osiągnąć w sposób bardziej efektywny za pomocą innych narzędzi. Narzędzia te mogą być wykorzystywane jedynie w godzinach pracy.
7. *Informacje z rejestrów pracy.* Pracownicy często proszą o dostęp do rejestrów pracy, np. do rejestru godzin pracy, i spotykają się z odmową ze strony pracodawcy. Zgodnie z art. 12 ustawy DP&FOI, odmowa taka jest bezprawna, chyba, że dopuszcza ją inna ustawa, i narusza prawo pracownika do samostanowienia informacyjnego.

Przetwarzanie danych osobowych w związku z zatrudnieniem

Procedury rekrutacyjne są uregulowane przepisami prawa krajowego w każdym państwie członkowskim UE. Poniżej zaprezentowane zostały wybrane kwestie z tego zakresu, w kontekście zbierania i przetwarzania danych osobowych.

Każdy kraj wprowadził przepisy prawa pracy, określające szczegółowo zakres danych, jakie mogą być przetwarzane w tym celu. Zakres danych wymagany od osób ubiegających się o pracę zależy od rodzaju stanowiska i ewentualnych przepisów szczególnych, jeśli mają one zastosowanie.



Zakres danych osobowych, jakie pracodawca może zbierać od pracowników i osób ubiegających się o pracę, reguluje art. 22¹ ustawy z dnia 26 czerwca 1974 roku Kodeks Pracy (Dziennik Ustaw z 1998 r. nr 21, pozycja 94 z późniejszymi zmianami). Przepis został dodany na mocy § 1 pkt. 7 ustawy z dnia 14 listopada 2003 r. o zmianie ustawy Kodeks Pracy i innych ustaw (Dziennik Ustaw nr 213, poz. 2081) i obowiązuje od 1 stycznia 2004 r.

Zgodnie z art. 22¹ § 1 Kodeksu Pracy, pracodawca ma prawo żądać od osoby ubiegającej się o pracę następujących danych: imię (imiona) i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania (adres korespondencyjny), informacje dotyczące edukacji i historii zatrudnienia. Zakres danych, jakich pracodawca może żądać od pracownika, jest nieco szerszy. Ustęp 2 wyżej wymienionego przepisu uprawnia pracodawcę do żądania innych danych osobowych pracownika – poza danymi wymienionymi w § 1 są to imiona, nazwiska i daty urodzenia dzieci, jeśli takie dane są potrzebne do przyznania pracownikowi specjalnych uprawnień wynikających z prawa pracy oraz numeru identyfikacyjnego PESEL pracownika, nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL). Ponadto, pracodawca ma prawo uzyskać od pracownika dane inne niż wymienione powyżej, jeśli obowiązek podania takich danych wynika z innych przepisów prawa (§ 4 wyżej wymienionego przepisu).

Zgodnie z art. 22¹ § 3 Kodeksu Pracy, udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa w § 1 i 2.

Należy podkreślić, że złożenie takiego oświadczenia przez pracownika bądź osobę ubiegającą się o pracę nie może być traktowane jako zgoda na przetwarzanie danych osobowych osób określonych w art. 23.1.1 ustawy o ochronie danych osobowych. Zgoda taka jest wtórna, ponieważ przetwarzanie danych osobowych przez pracodawcę w zakresie opisanym powyżej prowadzone jest na podstawie szczególnych przepisów prawa, spełnia zatem przesłankę określoną w art. 23.1.2 ustawy o ochronie danych osobowych.



Kodeks Pracy (ustawa nr 262/2006 Coll.) określa pewne limity przetwarzania danych. Na pracodawcach spoczywa obowiązek prawny przetwarzania określonych danych o obecnych, przeszłych i przyszłych pracownikach dla różnych celów, w tym podatkowych oraz podczas płatności składek na ubezpieczenie społeczne i zdrowotne.

Przed wszystkim należy mieć świadomość, że zatrudnienie jest niczym innym jak stosunkiem umownym, w którym strony są formalnie równe.

W praktyce, pozycja podmiotów stosunku pracy nie jest równa. Do pewnego stopnia wyrównują to uregulowania prawne sprzyjające osobom ubiegającym się o pracę, jako stronie słabszej. Na tym etapie, (przyszły) pracodawca może zażądać od osoby ubiegającej się o pracę danych osobowych związanych bezpośrednio z zawarciem umowy o pracę.

Nie jest możliwe stworzenie listy danych spełniających powyższe kryteria, ponieważ ich treść zależy od wielu czynników, takich jak charakter wykonywanej pracy itp. W przypadku, gdyby z jakiegoś powodu nie doszło do zawarcia stosunku pracy, pracodawca winien zwrócić osobie ubiegającej się o pracę wszelkie przekazane przez nią dokumenty i dane. Pracodawcom wolno kontynuować zbieranie danych jedynie jeśli osoba ubiegająca się o pracę udzieliła na to zgody mając na uwadze ewentualne przyszłe działania związane z jej zatrudnieniem (lub w innym celu).



Należy sprawdzić legalność pytań zadawanych podczas procedury rekrutacyjnej, ponieważ pomiędzy kandydatem a osobą pytającą panuje stosunek podporządkowania. W takim przypadku, kandydat ma ograniczoną możliwość odmowy udzielenia odpowiedzi. Zgodnie z art. 77 ustawy XXII z roku 1992 Kodeks Pracy, pracownika można prosić o złożenie oświadczenia, wypełnienie kwestionariusza lub wykonanie testu zdolności jedynie jeśli nie narusza to jego praw osobistych, a dostarcza informacji uznawanych za istotne dla celów nawiązania stosunku pracy. Od pracowników nie wolno wymagać poddania się testowi ciężowemu lub przedstawienia jego wyników, o ile nie jest to prawnie przepisane w celu ustalenia kwalifikacji pracownika na dane stanowisko.

Jeśli pracownik sądzi, że zadawane mu pytania nie są związane ze stosunkiem pracy lub że jego prawa osobiste są ograniczane lub naruszane bez powodu, ma prawo uzyskać informacje o danym pytaniu i związanym z nim przetwarzaniu danych i może zadawać na ten temat pytania osobie prowadzącej rozmowę. Pracownik ma prawo odmówić udzielenia odpowiedzi na pytania niezwiązane z określonym celem zgodnie z ustawą DP&FOI i art. 77 Kodeksu Pracy. Zgodnie z zasadą ograniczenia celu przetwarzania danych, osoba, która otrzymała curriculum vitae od pracownika nie może przekazać go osobie trzeciej, ani nawet poinformować nikogo o fakcie złożenia CV, o ile osoba, której dane dotyczą nie udzieliła na to wyraźnej zgody.

Podczas procedur rekrutacyjnych wykorzystuje się rozmaite narzędzia w celu oceny zdolności kandydata. Najczęściej stosowane nielegalne metody związane są z oceną osobowości kandydata, w całości lub w części, za pomocą testów psychologicznych i poligrafu.

Rzecznik Ochrony Danych w wielu opiniach wyraźnie stwierdził, że zastosowanie poligrafu jest nielegalne. Testy psychologiczne uznaje się za nielegalne jeśli podczas ich prowadzenia naruszane są prawa osoby, której dane dotyczą. Przed wypełnieniem kwestionariusza psychologicznego, osoba, której dane dotyczą musi zostać poinformowana, na jakie pytania odpowie rozwiązując test i jaki jest cel tego rodzaju przetwarzania danych. Należy również podać nazwisko osoby analizującej test, ponieważ jedynie ona ma prawo poznać odpowiedzi. Po przeanalizowaniu testu mierzącego całość osobowości, należy przekazać wyniki osobie, której dane dotyczą. Osoba ta ma prawo zdecydować, czy wyniki mogą zostać przekazane osobie prowadzącej procedurę rekrutacyjną. W przypadku prostszych pytań, sprawdzających np. zdolności pracownika, nie jest konieczne uzyskanie zgody osoby zainteresowanej, a wyniki można przekazać bezpośrednio pracodawcy.

Zakończenie stosunku pracy

Pracodawca powinien przestrzegać kilku zasad zapewniających poszanowanie prywatności byłego pracownika. Oto najważniejsze z nich:

- należy usunąć skrzynki e-mailowe po zakończeniu zatrudnienia (dobrą praktyką jest odsyłanie wiadomości przesłanych do usuniętej skrzynki z powrotem do nadawcy, wraz z informacją o usunięciu skrzynki),
- pracownik ma prawo do informacji o tym, jak długo, przez kogo i w jakim celu jego dane osobowe będą przetwarzane po zakończeniu zatrudnienia,
- należy usunąć dane kontaktowe pracownika ze strony internetowej pracodawcy.

Okres przechowywania danych pracownika w celu udokumentowania roszczeń pracodawcy ma długość równą okresowi przedawnienia roszczeń. Okres przechowywania dla celów ubezpieczeń społecznych jest dłuższy i może wynosić do 50 lat.



Pracodawca zobowiązany jest do przechowywania akt pracowników przez okres 50 lat dla celów ubezpieczeń społecznych.



Co do zasady, okres przechowywania danych wynosi 3 lata, dla celów podatkowych – 10 lat.



Na Węgrzech okres przechowywania danych pracowników wynosi 3 lata.

4.3 Dane osobowe w marketingu i kontaktach z klientami

Baza danych klientów

Przepisy prawa nie określają szczegółowo, jakie dane należy zebrać od klientów w celu wykonania umowy pomiędzy przedsiębiorcą a klientem, informacje takie nie powinny wykraczać poza dane niezbędne do identyfikacji klienta i do wykonania umowy. Zakres takich informacji może różnić się w zależności od rodzaju i charakteru usług świadczonych przez przedsiębiorcę, istnieją jednak rodzaje umów, w przypadku których przepisy wyraźnie określają zakres potrzebnych danych.

Zawierając umowę, przedsiębiorcy zbierają dane osobowe klientów objęte przepisami o danych osobowych. Jednocześnie tworzone są zbiory danych zawierające dane z umów konsumenckich, w szczególności umów sprzedaży towarów, umów najmu, umów ubezpieczenia, umów o prowadzenie rachunków bankowych, umów o dostawę elektryczności, wody i gazu oraz umów o świadczenie publicznie dostępnych usług telekomunikacyjnych.

Przedsiębiorcy mogą przetwarzać dane zebrane w związku z umowami zawartymi z klientami w celu realizacji tych umów i marketingu swoich produktów i usług.



Przetwarzanie danych identyfikujących strony umowy jest szczególnie istotne w momencie zawierania i wykonywania takiej umowy i co do zasady nie wymaga zgody klienta. Podstawowe informacje obejmują imię, nazwisko, adres zamieszkania oraz zazwyczaj numer dokumentu tożsamości i numer identyfikacyjny PESEL. Należy jednak zawsze pamiętać, aby zbierać dane jedynie w zakresie niezbędnym dla wykonania umowy i unikać zbierania nadmiernych ilości danych.

Przepisy bardzo często wskazują, jakie dane mogą być zbierane, np. w odniesieniu do abonentów usług telekomunikacyjnych. Dostawcy publicznie dostępnych usług komunikacyjnych mają prawo przetwarzać następujące dane użytkowników będących osobami fizycznymi: 1) imię i nazwisko; 2) imiona rodziców; 3) data i miejsce urodzenia; 4) adres stałego zamieszkania; 5) numer identyfikacyjny PESEL – w przypadku obywateli Rzeczypospolitej Polskiej; 6) nazwa, seria i numer dokumentu tożsamości, a w przypadku obywatela niebędącego obywatelem państwa członkowskiego ani Konfederacji Szwajcarskiej – numer paszportu lub karty pobytu; 7) dane zawarte w dokumentach potwierdzających zdolność wypełnienia zobowiązań wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikających z umowy o świadczenie usług telekomunikacyjnych. Poza danymi określonymi powyżej, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika związane ze świadczoną usługą, w szczególności Numer Identyfikacji Podatkowej, numer rachunku

bankowego lub karty płatniczej, adres korespondencyjny użytkownika, jeśli jest różny od jego adresu zamieszkania oraz adres poczty elektronicznej i numery telefonów kontaktowych.



Zakres danych osobowych niezbędnych dla zawarcia pisemnej umowy pomiędzy firmą a jej klientem oraz jej wykonania można ustalić w sposób praktyczny odpowiadając na następujące proste pytania: kto, komu, co i za ile, gdzie i kiedy. Umowy są zwykle zawierane na podstawie przepisów Kodeksu Cywilnego i Kodeksu Handlowego, a w niektórych przypadkach – innych przepisów szczególnych. Prawo nie określa zakresu danych osobowych niezbędnych dla identyfikacji stron dla większości rodzajów umów. Zgodnie z Kodeksem Cywilnym, podczas zawierania umów wszystkie strony zobowiązane są do usunięcia wszelkich elementów, jakie mogłyby prowadzić do powstania sporów. Oczywiście jest, że dokładność danych osobowych stanowi podstawową przesłankę dla unikania sporów, szczególnie w przypadku umów ustnych. W celu identyfikacji klienta jako strony umowy, najczęściej wykorzystuje się następujące informacje: imię, nazwisko, adres domowy i w razie potrzeby data urodzenia. Zakres ten można uznać za wystarczający dla wszystkich rodzajów umów pisemnych, z wyjątkiem umów, w przypadku których przepisy wyraźnie wymagają wykorzystania numerów identyfikacyjnych – jak w przypadku umów ubezpieczenia lub umów o świadczenie publicznie dostępnych usług komunikacji elektronicznej. Jeśli ich wykorzystanie nie jest wyraźnie wymagane przepisami, numery identyfikacyjne mogą być wykorzystywane jedynie za zgodą właścicieli. W zależności od rodzaju zawieranej umowy, wykorzystanie numerów dokumentów tożsamości klientów może zostać uznane za spełniające kryterium ograniczenia celu – na przykład w przypadku umów z hotelami.

Warto wyjaśnić, kiedy wpisywanie danych osobowych do umowy uznaje się za przetwarzanie danych. Pojedyncza umowa w formie fizycznej nie może być traktowana jako przetwarzanie danych osobowych strony w rozumieniu ustawy o ochronie danych. Jednak systematycznie zawierane umowy z klientami, np. o sprzedaż towarów lub świadczenie usług, traktuje się jako przetwarzanie danych osobowych. Rodzaj umowy również ma znaczenie dla operacji przetwarzania danych klienta wykonywanych podczas realizacji umowy. Na przykład, zbiory danych zawierające umowy konsumenckie, w szczególności umowy sprzedaży, umowy najmu, umowy ubezpieczenia itp. wiążą się z przetwarzaniem danych osobowych.

Jeśli dane osobowe klientów przetwarzane są w celu zawarcia i wykonania umowy w odpowiednim zakresie, jedynie w celu dostawy i fakturowania produktów i usług, zgoda osoby, której dane dotyczą nie jest konieczna – wyjątek ten został ustanowiony w art. 5.2(b) ustawy o ochronie danych.



Nie istnieją szczególne różnice w prawie krajowym.

Działalność marketingowa

Oferując produkty i usługi, przedsiębiorcy wykorzystują techniki marketingowe, np. materiały marketingowe, które wysyłają do obecnych i potencjalnych klientów.

Marketing bezpośredni w państwach członkowskich UE regulują rozmaite przepisy. W szczególności, różne zasady mogą odnosić się do przesyłania materiałów marketingowych pocztą tradycyjną lub drogą elektroniczną. Wykorzystanie danych osobowych może być dozwolone, pod pewnymi warunkami, bez uprzedniej zgody klienta – w takim przypadku, zwanym zasadą „opt-out”, klient musi mieć możliwość rezygnacji z usług oferowanych przez daną firmę (w tym adresowanych do niego działań marketingowych) i może zażądać zaprzestania przetwarzania swoich danych. W niektórych przypadkach wymagana jest zgoda.

Marketing bezpośredni prowadzony drogą elektroniczną musi spełniać wymogi w zakresie ograniczeń przesyłania niezamawianych wiadomości (spamu handlowego). Co do zasady, przesyłanie wiadomości handlowych (np. reklam) przez Internet powinno być dozwolone jedynie po wyrażeniu zgody przez osobę, której dane dotyczą (zasada „opt-in”).



Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych określa, kiedy firmy mogą przysyłać oferty marketingowe swoim klientom. Mogą to robić:

1. bez ich zgody – w przypadku marketingu własnych produktów i usług. Podstawę prawną dla wykorzystania danych osobowych stanowi wypełnienie prawnie usprawiedliwionego celu administratora (lub firmy), o którym mowa a art. 23.1.5 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem, prawnie usprawiedliwionym celem administratora jest marketing bezpośredni jego własnych produktów lub usług. Dane mogą być zatem wykorzystywane w tym celu, jeśli nie narusza to praw i wolności osoby, której dane dotyczą.
2. za ich zgodą – w przypadku marketingu produktów lub usług innego podmiotu. Nie istnieją przepisy, które zezwalałyby na przysyłanie oferty marketingowej innego podmiotu ze względu na prawnie usprawiedliwiony cel administratora. Nawet zawarcie umowy marketingu wzajemnego przez oba podmioty nie stanowi wystarczającej podstawy dla stwierdzenia, że przysyłanie oferty marketingowej firmy współpracującej stanowi prawnie usprawiedliwiony cel administratora.

Na przykład, jeśli operator telekomunikacyjny, który zawarł z bankiem umowę o współpracy w celu marketingu produktów, chciałby przesłać swoim klientom informacje o korzystnej pożyczce bankowej, musiałby w tym celu uzyskać ich zgodę. Informacja o korzystnej pożyczce stanowi informację marketingową banku, nie operatora telekomunikacyjnego, zatem operator telekomunikacyjny musi uzyskać zgodę klientów, aby móc przysyłać im oferty marketingowe banku. W przypadku, gdy przedsiębiorca zakupi bazę danych klientów w celu marketingu własnych produktów i usług, ma obowiązek uprzedniego poinformowania o tym osób, których dane dotyczą. Zgodnie z art. 25.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, źródle danych, prawie dostępu do treści swoich danych oraz ich poprawiania i uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8: prawie do wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację (pkt. 7) i prawie wniesienia sprzeciwu wobec przetwarzania jej danych (pkt. 8). Wypełnienie obowiązku informacyjnego wiąże się z podaniem osobie, której dane dotyczą pewnych informacji niezbędnych do wykonania przez nią jej praw, np. wspomnianego powyżej prawa sprzeciwu wobec przetwarzania jej danych, czy ewentualnego wniesienia skargi przeciwko administratorowi.

Niedopełnienie obowiązku informacyjnego określonego w art. 25 ustawy podlega odpowiedzialności karnej, ponieważ zgodnie z art. 54 tej ustawy kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Warto wspomnieć o wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 22 stycznia 2004 r. (sygnatura akt II SA 2665/2002), stwierdzającego: „Firma, która nabyła zbiór danych osobowych od innego administratora danych, powinna powiadomić klientów, że posiada ich dane, oraz dać im czas, aby mieli szansę wnieść sprzeciw na ich przetwarzanie w celach marketingowych. Niedotrzymanie tych warunków łamie przepisy o ochronie danych osobowych”. Osoba, której dane dotyczą może wnieść sprzeciw wobec przetwarzania swoich danych w przypadku,

gdy administrator danych przetwarza jej dane dla celów marketingowych zgodnie z art. 23.1.5 ustawy, stanowiącym, że przetwarzanie danych dozwolone jest m.in. jeżeli jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Administrator danych winien zaprzestać dalszego przetwarzania danych osoby, której dane dotyczą w przypadku wniesienia przez nią sprzeciwu wobec takiego przetwarzania. Zgodnie z art. 32.3 ustawy, w razie wniesienia sprzeciwu, dalsze przetwarzanie jest niedopuszczalne. Administrator może jednak przetwarzać dalej imię i nazwisko danej osoby, jej adres oraz numer serii dokumentu tożsamości lub numer identyfikacyjny PESEL w celu uniknięcia ponownego wykorzystania danych dla celów, wobec których osoba, której dane dotyczą wniosła sprzeciw. Prawo każdej osoby do zgłoszenia sprzeciwu wiąże się ze spoczywającym na administratorze danych obowiązkiem zastosowania takich środków technicznych i organizacyjnych, które umożliwią natychmiastowe zapisanie takiego sprzeciwu wobec dalszego przetwarzania. Jeśli chodzi o przesyłanie niezamówionych wiadomości e-mail, zgodnie z przepisami ustawy o świadczeniu usług drogą elektroniczną, regulującej obowiązki dostawców usług uczestniczących w świadczeniu usług drogą elektroniczną i ochronę danych osobowych użytkowników poczty elektronicznej, zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej (art. 10.1 wyżej wymienionej ustawy). Zgodnie z art. 10.2 ustawy, informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny. Art. 4.1 ustawy stanowi, że jeżeli ustawa wymaga uzyskania zgody usługobiorcy, to zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści i może być odwołana w każdym czasie. Art. 10.3 ustawy wskazuje jednak, że przesyłanie niezamówionej informacji handlowej stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r., nr 153, poz. 1503, z późniejszymi zmianami). W takim przypadku osoba, do której skierowane są takie informacje może zwrócić się do rzecznika ochrony konsumentów odpowiedniego dla swojego miejsca zamieszkania.



Zgodnie z ustawodawstwem czeskim, organ ochrony danych jest uprawniony do nadzorowania zgodności z art. 10 ustawy o pewnych usługach społeczeństwa informacyjnego (nr 480/2004 Coll.) dotyczącej pewnych usług i obowiązku informacyjnego związanego z informacjami handlowymi. Niestety, ustawa obejmuje jedynie podmioty podlegające prawu czeskiemu, a większość spamu przesyłana jest z zagranicy. Wymienione powyżej przepisy nie odnoszą się do bezpośrednich rozmów telefonicznych. Zgodnie z ustawą nr 127/2005 Coll. o komunikacji elektronicznej, niedozwolone jest przesyłanie wiadomości marketingowych lub innych podobnych produktów i usług osobom, które wskazały w publicznych książkach telefonicznych, wydanych na mocy tej ustawy, że nie życzą sobie kontaktów w celach marketingowych.



Na Węgrzech marketing bezpośredni reguluje wiele instrumentów prawnych. Różne zasady odnoszą się do komunikacji za pośrednictwem poczty tradycyjnej, elektronicznej i telefonu oraz marketingu bezpośredniego prowadzonego za pośrednictwem poczty tradycyjnej, elektronicznej i telefonu. Warto zwrócić uwagę na tzw. firmy internetowe, które odgrywają znaczącą rolę na rynku. Nie jest jasne, czy węgierska ustawa o ochronie danych i wolności informacji ma zastosowanie do takich firm.

ORGANY OCHRONY DANYCH UCZESTNICZĄCE W PROJEKCIE



Biuro Generalnego Inspektora Ochrony Danych Osobowych

Generalny Inspektor Ochrony Danych Osobowych, powołany w roku 1998, jest niezależnym organem nadzorczym, którego uprawnienia obejmują szeroko pojęty obszar ochrony danych. Do obowiązków Generalnego Inspektora Ochrony Danych Osobowych należą: nadzorowanie zgodności przetwarzania danych z ustawą o ochronie danych osobowych, wydawanie decyzji administracyjnych i rozpatrywanie skarg związanych z zastosowaniem przepisów o ochronie danych osobowych, prowadzenie publicznego rejestru zbiorów danych, wydawanie opinii o projektach ustaw i przepisów, uczestnictwo w pracach organizacji i instytucji międzynarodowych zaangażowanych w ochronę danych osobowych, a także inicjowanie i podejmowanie działań mających na celu poprawę ochrony danych osobowych poprzez publikację ulotek i innego rodzaju działalność edukacyjną.

Generalny Inspektor Ochrony Danych Osobowych posiada uprawnienia do wydawania decyzji administracyjnych i rozpatrywania skarg związanych z zastosowaniem przepisów o ochronie danych osobowych.



Kontakt

ul. Stawki 2

00-193 Warszawa

Tel. (+48 22) 860 70 81

Fax: (+48 22) 860 70 90

E-mail: kancelaria@giodo.gov.pl

www.giodo.gov.pl

Godziny pracy: 8.00 – 16.00 od poniedziałku do piątku



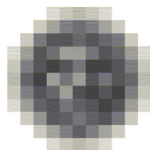
CZECHY

Biuro Ochrony Danych Osobowych

Utworzone w czerwcu 2000 roku Biuro Ochrony Danych Osobowych jest niezależnym organem nadzorczym obdarzonym licznymi uprawnieniami. Jego misją jest zapewnienie przestrzegania zasad ochrony danych przez przedsiębiorstwa i władze oraz uświadamianie obywatelom ich praw wynikających z ustawy o ochronie danych. Biuro prowadzi różnorodną działalność, od rozpatrywania skarg i prowadzenia dochodzeń, przez konsultacje i promocje, po prowadzenie rejestru zgłoszonych operacji przetwarzania, wydawanie zezwoleń na przekazywanie danych za granicę czy przygotowywanie stanowisk w określonych sprawach. Działalność Biura reguluje czeska ustawa o ochronie danych.

Biuro jest szanowanym uczestnikiem procesu ustawodawczego, w którym uczestniczy jako konsultant, zawsze starając się promować przestrzeganie zasad ochrony danych w projektach ustaw przedkładanych przez rząd.

Biuro służy poradnictwem i wsparciem osobom fizycznym i profesjonalistom i rozprowadza wiele cennych publikacji. Poza ukazującymi się regularnie Dziennikiem Oficjalnym, Biuletynem i Sprawozdaniem Rocznym, czytelnicy mają do dyspozycji różne ulotki i broszury koncentrujące się na interesujących tematach. Jedną z takich publikacji jest niniejszy przewodnik, przygotowany wspólnie z partnerami z Polski i Węgier.



**úřad pro ochranu
osobních údajů**
the office for personal
data protection

Kontakt

Pplk. Sochora 27

170 00 Prague 7

Tel. +420 234 665 111

Fax: +420 234 665 444

E-mail: posta@uouu.cz

www.uouu.cz

Godziny Pracy: 7.30 – 16.15 od poniedziałku do czwartku
7.30 – 15.00 piątek



Rzecznik Ochrony Danych i Wolności Informacji

Ustawa LXIII z roku 1992 o ochronie danych osobowych i dostępie do informacji publicznej (ustawa DP&FOI), uchwalona 17 listopada 1992 roku, ustanowiła Rzecznika Ochrony Danych i Wolności Informacji, mającego chronić konstytucyjne prawa i wolności w zakresie ochrony danych osobowych i dostępu do informacji publicznej. Rzecznik Ochrony Danych powoływany jest przez Parlament; instytucję utworzono 30 lipca 1995 roku.

Obowiązki i uprawnienia Rzecznika reguluje ustawa DP&FOI i inne ustawy. Rzecznik Ochrony Danych nadzoruje zgodność z przepisami w zakresie ochrony danych, rozpatruje przedłożone skargi i odpowiada za prowadzenie rejestru ochrony danych. Rzecznik Ochrony Danych ułatwia jednolite wdrażanie przepisów w zakresie przetwarzania danych osobowych i dostępu do informacji publicznej, posiada również uprawnienia do wydawania zaleceń ogólnych lub dla określonych administratorów. Rzecznik wyraża opinie w zakresie udostępniania danych ogółowi społeczeństwa oraz działalności władz państwowych i lokalnych oraz innych organów wypełniających przewidziane ustawowo obowiązki publiczne. Istotnym obowiązkiem Rzecznika jest wydawanie opinii w sprawie projektów ustawodawczych z zakresu ochrony danych i wolności informacji oraz zaleceń w sprawie nowych przepisów.

Rzecznik Ochrony Danych współpracuje z określonymi ustawowo organami i osobami, reprezentując Węgry we wspólnych organach nadzorczych Unii Europejskiej do spraw ochrony danych.

Po stwierdzeniu nielegalności operacji przetwarzania danych, Rzecznik Ochrony Danych zaleca administratorowi zaprzestanie takiego przetwarzania. Jeśli administrator lub przetwarzający nie zastosuje się do zalecenia, Rzecznik Ochrony Danych może wydać nakaz zatrzymania, usunięcia lub zniszczenia nielegalnie przetwarzanych danych. Rzecznik Ochrony Danych może podać do publicznej wiadomości informację o rozpoczęciu postępowania i o nielegalnym przetwarzaniu danych, identyfikując przy tym administratora (przetwarzającego).

Oprócz obowiązków określonych w ustawodawstwie, Rzecznik odpowiada również za informowanie społeczeństwa o pojęciu ochrony danych i jego znaczeniu dla poszczególnych obywateli oraz o prawie do wolności informacji. W tym celu współpracuje z mediami lokalnymi i krajowymi, informuje o aktach prawnych, reklamuje swoją działalność i wspiera rozwój edukacji i badań w tym obszarze. Niniejszy przewodnik, przygotowany we współpracy z partnerami z Polski i Czech, służy temu celowi.



HUNGARIAN PARLIAMENTARY COMMISSIONER FOR
DATA PROTECTION AND FREEDOM OF INFORMATION

Kontakt

Nádor str. 22
1051 Budapest,
1387 Budapest Po. box. 40
Tel. (+36 1) 475 7100
Fax: (+36 1) 269 3541
E-mail: adatved@obh.hu
www.adatvedelmibiztos.hu

