NACZELNA RADA ADWOKACKA
KRAKOWSKA IZBA ADWOKACKA

Przewodnik po RODO

DLA ADWOKATÓW

adw. dr Paweł Litwiński

Kraków 2018

NACZELNA RADA ADWOKACKA

KRAKOWSKA IZBA ADWOKACKA

Przewodnik po RODO dla adwokatów

adw. dr Paweł Litwiński

Kraków, marzec 2018

ISBN 978-83-66027-03-9

Przygotowanie do druku
FALL
ul. Garczyńskiego 2
31-524 Kraków
tel. 12 413 35 00, 502 022 027
www.fall.pl

Spis treści

Wstęp 5

1. Podstawowe informacje o RODO 5

1.1. Co to jest RODO? 5
1.2. Od kiedy będzie się stosować RODO? 6
1.3. Czy będzie polska ustawa o ochronie danych osobowych? 6
1.4. Czy czekać z wdrożeniem RODO na polskie przepisy o ochronie danych osobowych? 6
1.5. Czy w nowych przepisach będzie odpowiednik GIODO? 6
1.6. Kto podlega RODO? Kto powinien wdrożyć RODO? 7
1.7. Czy adwokaci podlegają RODO? 7
1.8. Kiedy stosujemy RODO? 8
1.9. Jakie czynności podlegają RODO? 9
1.10. Co to są dane osobowe? 9
1.11. Kto może przetwarzać dane osobowe? 10
1.12. Jakie dane osobowe przetwarza adwokat? 11
1.13. Kim jest adwokat w stosunku do przetwarzanych danych osobowych? 12

2. Zbieranie danych osobowych 13

2.1. Kiedy można przetwarzać dane osobowe? 13
2.2. Jak wiele danych osobowych można zbierać zgodnie z RODO? 14
2.3. Jakie informacje przekazywać przy zbieraniu zgody na przetwarzanie danych osobowych? 15
2.4. Przetwarzanie przez adwokatów danych osobowych dotyczących skazań 16
2.5. Jak długo mogę przechowywać dane osobowe? 17

3. Organizacja przetwarzania danych 18

3.1. Jak należy zabezpieczać dane osobowe? 18
3.2. Co się stanie z istniejącą dokumentacją ochrony danych osobowych? 20
3.3. Obowiązek rejestrowania czynności przetwarzania danych 20
3.4. Co to jest obowiązek uwzględniania ochrony danych w fazie projektowania? 21

3.5. Czym jest domyślna ochrona danych? 21
3.6. Kiedy należy wyznaczyć Inspektora Ochrony Danych? 22
3.7. Co to jest ocena skutków dla ochrony danych osobowych i kiedy należy ją przeprowadzić? 23
3.8. Czym są uprzednie konsultacje z organem nadzorczym? 24
3.9. Co to jest obowiązek zgłaszania naruszeń ochrony danych? 25
3.10. Jak zawrzeć umowę powierzenia przetwarzania danych? 26

4. Prawo do bycia zapomnianym i prawo do przenoszenia danych ... 28
4.1. Prawo do bycia zapomnianym 28
4.2. Prawo do przenoszenia danych 29

5. Kontrola przestrzegania przepisów RODO 31
5.1. Czy Prezes UODO będzie mógł kontrolować adwokatów? 31
5.2. Administracyjne kary pieniężne 32

Przydatne materiały i literatura 32

Aneks

Polityka bezpieczeństwa informacji 33
Załącznik 1. Rejestr czynności przetwarzania danych osobowych 41
Załącznik 2. Wzór upoważnienia do przetwarzania danych osobowych 42
Załącznik 3. Wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe .. 43
Załącznik 4. Wzór zgłoszenia incydentu naruszenia ochrony danych osobowych ... 44

Instrukcja zarządzania systemem informatycznym 45

Wstęp

Celem przewodnika jest przedstawienie podstawowych informacji dotyczących nowego europejskiego prawa ochrony danych osobowych z punktu widzenia wykonywania zawodu adwokata.

Autorem poradnika jest adw. dr Paweł Litwiński.

1. Podstawowe informacje o RODO

1.1. Co to jest RODO?

Pisząc i mówiąc „RODO", mamy na myśli rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Jest to akt prawny przyjęty przez Unię Europejską regulujący zasady ochrony danych osobowych – zastępuje dyrektywę 95/46/WE z 1995 r.

Tymczasem RODO nie będzie implementowane, czyli nie będzie trzeba przepisów RODO przyjąć w polskiej ustawie, jak to się dzieje w przypadku dyrektyw. RODO będzie bezpośrednio obowiązywać, będzie bezpośrednio stosowane i bezpośrednio skuteczne. To oznacza, że – z bardzo niewielkimi wyjątkami – całe prawo ochrony danych osobowych znajdziemy bezpośrednio w tekście RODO. Ten tekst można znaleźć w Dzienniku Urzędowym Unii Europejskiej L z 2016 r. nr 119, s. 1.

RODO jest elementem większego pakietu aktów prawnych składającego się na reformę europejskiego prawa ochrony danych osobowych. Prócz RODO w jego skład wchodzi tzw. dyrektywa policyjna, regulująca zasady przetwarzania danych osobowych przez organy ścigania (dyrektywa Parlamentu Europejskiego i Rady UE 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca

decyzję ramową Rady 2008/977/WSiSW). Dyrektywa policyjna powinna zostać implementowana do polskiego porządku prawnego do 6 maja 2018 r.

RODO zastąpi obowiązującą obecnie ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych.

1.2. Od kiedy będzie się stosować RODO?

RODO będzie stosowane od 25 maja 2018 r. Do tej daty wszystkie te podmioty, które podlegają RODO, powinny być gotowe do stosowania RODO – nie będzie już żadnego dodatkowego okresu przejściowego.

1.3. Czy będzie polska ustawa o ochronie danych osobowych?

Tak, Ministerstwo Cyfryzacji pracuje nad polskimi przepisami uzupełniającymi RODO. Przepisy te będą regulować m.in.:

- zasady powoływania następcy GIODO – Prezesa Urzędu Ochrony Danych Osobowych (PUODO),
- postępowanie przed POUDO,
- procedurę odwoławczą od decyzji PUODO.

W polskich przepisach o ochronie danych osobowych znajdzie się także regulacja tego fragmentu zasad ochrony danych osobowych, który nie został uregulowany w RODO, czyli niektórych zasad przetwarzania danych kadrowych.

1.4. Czy czekać z wdrożeniem RODO na polskie przepisy o ochronie danych osobowych?

Nie. Całe prawo ochrony danych osobowych znajdziemy bezpośrednio w tekście RODO, z wyjątkiem niektórych kwestii dot. ochrony danych osobowych kadrowych. Nie ma więc sensu czekać z dostosowaniem do RODO na polskie przepisy – proces wdrożenia RODO trzeba rozpocząć natychmiast.

1.5. Czy w nowych przepisach będzie odpowiednik GIODO?

Planuje się powołanie nowego organu nadzorczego, Prezesa Urzędu Ochrony Danych Osobowych (PUODO). Organ ten przejmie zadania i kompetencje GIODO, a także będzie wykonywał nowe, przyznane mu przez RODO.

1.6. Kto podlega RODO? Kto powinien wdrożyć RODO?

RODO podlega każdy przedsiębiorca, który prowadzi działalność w Unii Europejskiej. Może to być działalność w jakiejkolwiek formie prawnej: spółka, jednoosobowa działalność gospodarcza czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią. Nie ma znaczenia narodowość osób, których dane osobowe są przetwarzane. Nie ma znaczenia to, gdzie są przetwarzane dane osobowe (gdzie znajdują się serwery).

Przykłady

- korzystanie przez polską spółkę z o.o. z usług przetwarzania danych w chmurze nie zwalnia tej spółki z konieczności stosowania RODO,
- polski podmiot oferujący swoje usługi obywatelom Ukrainy podlega przepisom RODO,
- oddział w Polsce przedsiębiorcy z USA podlega przepisom RODO.

RODO nie znajduje zastosowania do działalności osobistej lub domowej. To oznacza, że osoba fizyczna prowadząca działalność gospodarczą musi stosować RODO do danych osobowych swoich klientów czy pracowników, ale nie stosuje RODO do danych przetwarzanych w celach czysto prywatnych, np. do danych adresatów wysyłanych corocznie kartek świątecznych.

1.7. Czy adwokaci podlegają RODO?

Przepisy RODO znajdują zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii (art. 3 ust. 1 RODO).

Pojęcie jednostki organizacyjnej użyte w art. 3 ust. 1 RODO to pojęcie autonomiczne dla unijnego prawa ochrony danych osobowych i należy je interpretować w oderwaniu od przepisów krajowych. Motyw 22 preambuły RODO wskazuje wprost, że pojęcie jednostki organizacyjnej zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur nie jest w tym względzie czynnikiem decydującym. Nie budzi więc wątpliwości, że pod względem podmiotowym osoby wykonujące zawód adwokata podlegają przepisom RODO.

1.8. Kiedy stosujemy RODO?

RODO znajduje zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. RODO wyróżnia więc dwa przypadki przetwarzania danych osobowych:

a) przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany
b) przetwarzanie w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Przetwarzanie danych osobowych w sposób zautomatyzowany najczęściej odbywa się w systemie informatycznym.

Przykłady

- program do obsługi poczty elektronicznej,
- edytor tekstów,
- program służący do zarządzania kancelarią.

Przetwarzanie danych w sposób inny niż zautomatyzowany to te wszystkie przypadki, w których dane mają postać papierową – są przetwarzane w postaci wydruków, zbiorów akt itp. Na gruncie RODO dane w postaci papierowej podlegają ochronie nie tylko wtedy, gdy stanowią część zbioru danych, ale także wtedy, gdy mają stanowić część zbioru. Zbiór danych to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów (art. 4 pkt 6 RODO). Definicja ta nie różni się co do swej istoty od definicji z art. 7 pkt 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, aktualny pozostaje więc pogląd wyrażony przez GIODO, zgodnie z którym zbiorem danych osobowych są „wszelkie materiały gromadzone w formie akt, w tym sądowe, prokuratorskie, policyjne i inne zawierające dane osobowe" (stanowisko Generalnego Inspektora Ochrony Danych Osobowych dostępne na stronie www.giodo.gov.pl w dziale „Odpowiedzi na pytania").

Dane osobowe podlegają ochronie bez względu na to, czy ostatecznie znajdą się w zbiorze danych osobowych. Taki wniosek dodatkowo wzmacnia posłużenie się w art. 2 ust. 1 RODO zwrotem „mają stanowić" część zbioru danych osobowych, który wskazuje na intencję towarzyszącą procesowi gromadzenia danych osobowych. Ochrona danych osobowych wynikająca z przepi-

sów RODO obejmuje więc informacje już na etapie ich gromadzenia, a zatem nawet wówczas, gdy zbiór danych jeszcze nie istnieje, ale ma zostać utworzony na podstawie zbieranych danych.

1.9. Jakie czynności podlegają RODO?

RODO stosuje się do przetwarzania danych osobowych. Przetwarzaniem danych osobowych są jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

- zbieranie danych,
- przechowywanie danych,
- usuwanie danych,
- opracowywanie danych,
- udostępnianie danych.

RODO obejmuje wszelkie czynności, które mają za przedmiot dane osobowe – czyli nie tylko np. usługę archiwizowania dokumentów, ale wszelkie usługi, w których dochodzi do zbierania danych osobowych. RODO powinni więc stosować:

- przedsiębiorcy zajmujący się przetwarzaniem danych – archiwizowanie danych, niszczenie dokumentów, usługi kurierskie itp.,
- podmioty, które przetwarzają dane osobowe przy okazji świadczenia innych usług, np. osoby wykonujące zawód adwokata.

1.10. Co to są dane osobowe?

Dane osobowe to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Osobą zidentyfikowaną jest taka osoba, której tożsamość znamy, którą możemy wskazać spośród innych osób. Osobą możliwą do zidentyfikowania jest taka osoba, której tożsamości nie znamy, ale możemy poznać, korzystając z tych środków, które mamy.

Przykłady

- osoba zidentyfikowana: osoba fizyczna korzystająca z pomocy prawnej adwokata; świadek, którego dane osobowe podał klient; aplikant, z którym współpracuje adwokat; osoba zatrudniona przez adwokata do obsługi sekretariatu kancelarii,
- osoba możliwa do zidentyfikowania: nadawca listu poleconego na podstawie numeru przesyłki;

Dane osobowe to informacje o osobach fizycznych – osoby prawne nie mają danych osobowych. Ale pracownicy osób prawnych mogą mieć dane osobowe, jak każda inna osoba fizyczna:

a. informacja „XYX sp. z o. o." – nie stanowi danych osobowych tego podmiotu,
b. informacja „Jan Kowalski, prezes zarządu XYZ sp. z o. o." – może stanowić dane osobowe Jana Kowalskiego.

Możliwość uznania informacji za dane osobowe nie zależy ani od wieku danej osoby, ani od jej narodowości.

Wyróżnia się dwie kategorie danych osobowych:

a. tzw. dane osobowe zwykłe,
b. dane osobowe zaliczające się do szczególnych kategorii danych (dawniej zwane danymi wrażliwymi).

Do szczególnych kategorii danych osobowych zaliczamy dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Dane osobowe, które nie należą do żadnej z tych kategorii, to dane zwykłe. Zgodnie z RODO, do kategorii danych osobowych zwykłych należą także dane osobowe dotyczące wyroków skazujących.

1.11. Kto może przetwarzać dane osobowe?

Przetwarzanie danych osobowych to bardzo ogólne sformułowanie, oznaczające jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

- zbieranie danych,
- przechowywanie danych,
- usuwanie danych,
- opracowywanie danych,
- udostępnianie danych.

Jeżeli jakiś przedsiębiorca przetwarza dane osobowe, to może to robić jako jeden z dwóch kategorii podmiotów:

a. administrator danych,
b. podmiot przetwarzający dane.

Administrator danych to taki podmiot, który decyduje o celach i sposobach przetwarzania danych. Innymi słowy, decyduje o tym, po co (cele) i jak (sposoby) wykorzystać dane osobowe. Przykłady:

- pracodawca w stosunku do danych osobowych swoich pracowników,
- sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów,
- właściciel strony internetowej w stosunku do danych osobowych osób, które zaprenumerowały newsletter.

Administratorem danych jest zawsze określony podmiot – np. spółka, a nie jego pracownik. Przykłady:

- administratorem danych jest spółka z o.o., a nie jej prezes zarządu czy dyrektor marketingu,
- administratorem danych jest Jan Kowalski prowadzący jednoosobową działalność gospodarczą.

Podmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego. Przykłady:

- biuro rachunkowe przetwarza na zlecenie adwokata dane osobowe przekazane mu w tym celu przez kancelarię,
- podmiot utrzymujący na zlecenie swoich klientów konta poczty elektronicznej przetwarza na zlecenie dane osobowe,
- podmiot zajmujący się profesjonalnie niszczeniem danych osobowych przetwarza w tym zakresie dane osobowe na zlecenie swoich klientów.

Podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych odpowiednią umowę, tzw. umowę powierzenia, w której określone zostaną zasady przetwarzania danych.

W kancelarii dane osobowe faktycznie przetwarzają konkretne osoby fizyczne – adwokaci, aplikanci, prawnicy, personel biurowy. Takie osoby powinny posiadać upoważnienie do przetwarzania danych osobowych.

1.12. Jakie dane osobowe przetwarza adwokat?

W kancelarii dochodzi do przetwarzania danych osobowych – można wskazać dwie typowe grupy danych osobowych, które przetwarzane są w każdej kancelarii:

a. dane osobowe związane z udzielaniem pomocy prawnej,
b. dane osobowe pracowników i osób współpracujących.

Dane osobowe związane z udzielaniem pomocy prawnej to przede wszystkim dane klientów: imię, nazwisko i adres (lub informacje o osobach działających w imieniu osób prawnych), informacje dotyczące sprawy, sygnatury postępowań, numery w wewnętrznym rejestrze spraw w kancelarii itp. Do tej grupy zaliczają się także dane osobowe przeciwników procesowych klientów oraz dane osobowe świadków, biegłych i innych uczestników postępowania.

Dane osobowe pracowników i osób współpracujących obejmują informacje o osobach zatrudnionych na umowę o pracę i na podstawie innych umów tzw. cywilnoprawnych, dane osobowe współpracujących adwokatów i aplikantów. Do tej grupy zaliczają się także dane osobowe aplikantów, w stosunku do których adwokaci pełnią funkcję patronów. Dane osobowe będą także przetwarzane w związku z wykonywaniem obowiązków związanych z zatrudnieniem pracowników, w szczególności w celu wykonania obowiązków z zakresu ubezpieczenia społecznego i obowiązków podatkowych.

1.13. Kim jest adwokat w stosunku do przetwarzanych danych osobowych?

W stosunku do danych osobowych pracowników i osób współpracujących adwokatowi przysługuje status administratora danych osobowych – na zasadach ogólnych, tak jak np. każdemu pracodawcy przysługuje status administratora danych osobowych w stosunku do danych osobowych jego pracowników.

Na gruncie ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, odpowiedź na pytanie o status adwokata w odniesieniu do danych osobowych związanych z udzielaniem pomocy prawnej nastręczała wiele trudności. Na gruncie RODO i towarzyszących RODO polskich przepisów o ochronie danych osobowych ten problem zostanie wreszcie rozwiązany – zgodnie z projektem ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, w art. 16a ustawy Prawo o adwokaturze ma zostać przesądzone, że adwokaci pełnią rolę administratorów danych osobowych w stosunku do danych osobowych przetwarzanych w ramach wykonywania zawodu. Adwokat w stosunku do danych osobowych przetwarzanych związanych z udzielaniem pomocy prawnej powinien więc zostać uznany za administratora danych osobowych.

2. Zbieranie danych osobowych

2.1. Kiedy można przetwarzać dane osobowe?

Dane osobowe można przetwarzać wyłącznie wtedy, gdy istnieje tzw. podstawa prawna przetwarzania danych. Podstawa przetwarzania danych wynika jednak z konkretnych sytuacji faktycznych i prawnych spośród wyliczonych w RODO w formie zamkniętego katalogu: w art. 6 w odniesieniu do danych osobowych zwykłych, w art. 9 w odniesieniu do szczególnych kategorii danych osobowych.

Przetwarzanie danych osobowych zwykłych jest dopuszczalne m.in. wtedy, gdy jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (art. 6 ust. 1 pkt. f RODO). Jednym z takich celów jest dochodzenie roszczeń. W przypadku szczególnych kategorii danych osobowych dochodzenie roszczeń zostało wprost wskazane jako okoliczność uzasadniająca przetwarzanie danych (art. 9 ust. 2 pkt f RODO). Przetwarzanie danych osobowych w celu dochodzenia roszczeń znajduje co do zasady podstawę prawną w przepisach RODO. Przetwarzanie danych osobowych jest zgodne z prawem także wtedy, gdy na takie przetwarzanie zezwalają szczególne przepisy prawa (art. 6 ust. 1 pkt c i art. 9 ust. 2 pkt g RODO). Przykładem takich przepisów są poszczególne przepisy proceduralne, które wskazują konkretny zakres danych osobowych, jaki powinien zostać podany w związku z konkretnymi czynnościami procesowymi – tytułem przykładu można wskazać art. 126 § 1 i 2 KPC czy art. 63 § 2, 3 i 3a KPA. Skoro więc pełnomocnik pełni rolę administratora danych osobowych w stosunku do danych, które przetwarza w ramach wykonywania zawodu, może – a nawet powinien – powołać się na podstawę przetwarzania danych osobowych związaną z koniecznością podania danych osobowych przy poszczególnych czynnościach procesowych.

Przetwarzanie danych osobowych w innym celu niż związany z dochodzeniem roszczeń, np. w celu udzielania porad prawnych czy sporządzania opinii prawnych, znajduje swoje uzasadnienie w umowie łączącej adwokata (któremu przysługuje status administratora danych) z klientem. Jedną z podstaw przetwarzania danych zwykłych jest bowiem niezbędność takiego przetwarzania do wykonania umowy z osobą, której dane dotyczą (art. 6 ust. 1 pkt b RODO). Dane zwykłe mogą być także przetwarzane, jeżeli jest to niezbędne do wykonania zadania realizowanego w interesie publicznym – takim zadaniem jest bez wątpienia udzielanie pomocy prawnej przez osoby wykonujące zawód zaufania publicznego, jakim jest zawód adwokata. Jeżeli w tych samych celach dochodziłoby do przetwarzania danych wrażliwych, wówczas podstawą prawną takiego przetwarzania byłby art. 9 ust. 2 pkt g RODO.

Adwokaci mogą także zbierać zgody na przetwarzanie danych osobowych: na ogólnych zasadach, ale nie w celach związanych z wykonywaniem zawodu, ponieważ w tym zakresie dysponują oni ustawową podstawą przetwarzania danych. Jeżeli dodatkowo zebraliby zgodę na przetwarzanie danych, powstaje pytanie, jak się powinni zachować, jeżeli zgoda zostałaby odwołana? Czy oznaczałoby to wypowiedzenie pełnomocnictwa? Z tego względu zgoda na przetwarzanie danych może być użyteczną podstawą przetwarzania danych w innych celach, np. w celu przesyłania klientom biuletynów informujących o zmianach w prawie, oczywiście w granicach wyznaczonych przez odpowiednie regulacje dotyczące reklamy.

2.2. Jak wiele danych osobowych można zbierać zgodnie z RODO?

RODO wprowadza tzw. zasadę minimalizacji danych osobowych. Zgodnie z nią, można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych. Przetwarzanie danych powinno więc zostać ograniczone do takich danych, bez których nie można osiągnąć celu przetwarzania danych.

Przykład

Jeżeli celem przetwarzania danych jest reprezentacja klienta w postępowaniu przed sądem, dopuszczalne jest przetwarzanie takiego zakresu danych, jaki uzasadniony jest przez przedmiot toczącego się postępowania.

2.3. Jakie informacje przekazywać przy zbieraniu zgody na przetwarzanie danych osobowych?

Dane osobowe mogą być gromadzone:

- bezpośrednio od osób, których dane dotyczą – np. klient podaje adwokatowi swoje dane osobowe przy zawieraniu umowy o obsługę prawną,
- niebezpośrednio od osób, których dane dotyczą – np. klient podaje adwokatowi dane osobowe przeciwnika procesowego.

Przy gromadzeniu danych osobowych bezpośrednio od osób, których dane dotyczą, zgodnie z art. 13 RODO należy tym osobom przekazać następujące informacje:

- o tożsamości administratora danych i o jego danych kontaktowych,
- jeżeli administrator danych powołał Inspektora Ochrony Danych (IOD) – o danych kontaktowych IOD,
- o celach i podstawie przetwarzania danych, a jeżeli przetwarzanie odbywa się na tej podstawie, że jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – o tych prawnie uzasadnionych interesach,
- o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego,
- o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe – kryteria ustalania tego okresu,
- o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- jeżeli przetwarzanie odbywa się na podstawie zgody – o prawie do cofnięcia zgody w dowolnym momencie,
- o prawie wniesienia skargi do organu nadzorczego,
- o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy, oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- jeżeli dochodzi do tzw. zautomatyzowanego podejmowania decyzji lub profilowania – należy poinformować o tym fakcie oraz podać istotne informacje o zasadach automatycznego podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Przy gromadzeniu danych osobowych niebezpośrednio od osób, których dane dotyczą, zgodnie z art. 14 RODO, należy tym osobom dodatkowo przekazać informację o źródle danych, a więc o tym, skąd adwokat pozyskał ich dane osobowe.

Obowiązki informacyjne związane z gromadzeniem danych bezpośrednio od osób, których dane dotyczą, znajdują zastosowanie do adwokatów zbierających dane osobowe bezpośrednio od osób, których dane dotyczą.

Przykład

- Adwokat, przy zawieraniu umowy o obsługę prawną z klientem, powinien wykonać obowiązek informacyjny i przekazać klientowi informacje wymagane przez art. 13 RODO.

Jeżeli jednak adwokat zbiera dane nie od osób, których te dane dotyczą, wówczas zgodnie z projektem ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, adwokat będzie zwolniony z obowiązku informacyjnego wobec takich osób.

Przykład

- klient podaje adwokatowi dane osobowe przeciwnika procesowego,
- klient podaje adwokatowi dane osobowe świadków.

W takich przypadkach adwokaci nie będą mieli obowiązku przekazywania tym osobom, których dane osobowe uzyskają od innych osób, informacji wymaganych przez art. 14 RODO.

2.4. Przetwarzanie przez adwokatów danych osobowych dotyczących skazań

RODO – inaczej, niż to ma miejsce na gruncie ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych – nie zalicza danych osobowych dotyczących wyroków skazujących do szczególnych kategorii danych osobowych. Zgodnie z art. 10 RODO, dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa mogą być przetwarzane „pod nadzorem" władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Przetwarzanie danych „pod nadzorem" władz publicznych nie oznacza, że administratorem takich danych może być wyłącznie podmiot publiczny, jednak

jego czynności składające się na przetwarzanie danych muszą być nadzorowane przez odpowiednie władze publiczne. Odwołanie do art. 6 ust. 1 RODO powoduje natomiast, że podstawą przetwarzania takich danych może to być każda z podstaw prawnych wskazanych w tym przepisie. Adwokaci mogą więc przetwarzać dane dotyczące wyroków skazujących na takich samych zasadach, jak to zostało opisane wyżej w pkt. 1. Element nadzoru nad takim przetwarzaniem można natomiast utożsamiać z nadzorem, jaki nad wykonywaniem zawodu adwokata jest sprawowany przez odpowiednie władze Adwokatury.

2.5. Jak długo mogę przechowywać dane osobowe?

Dane osobowe powinny być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (art. 5 ust. 1 pkt e RODO).

W przypadku przetwarzania danych osobowych przez adwokatów okres, przez który dane powinny być przetwarzane, jest uzależniony od celu ich przetwarzania. Można w tym zakresie wskazać kilka typowych sytuacji:

- przetwarzanie danych w celu związanym z wykonywaniem zawodu adwokata – w przypadku adwokatów dokumenty związane z prowadzeniem sprawy należy przechowywać co najmniej przez okres jednego roku od wykonania zlecenia, chyba że w umowie o świadczenie usług adwokackich strony postanowiły inaczej; dokumenty mogące stanowić podstawę odpowiedzialności adwokata powinny być przechowywane do końca okresu przedawnienia ewentualnych roszczeń przeciwko adwokatowi (§ 5 ust. 2 Regulaminu wykonywania zawodu adwokata w kancelarii indywidualnej lub spółkach);
- przetwarzanie danych w celu związanym z zatrudnieniem pracowników – przez czas trwania zatrudnienia, a po jego ustaniu pracodawca jest zobowiązany przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, przez okres 50 lat od dnia zakończenia u niego pracy przez pracownika;
- przetwarzanie danych w celu przesyłania klientom materiałów informacyjnych – przez okres, w którym adwokat danych dysponuje zgodą na przetwarzanie danych w tym zakresie, a po odwołaniu zgody – przez okres przedawnienia roszczeń związanych z takim celem przetwarzania danych, tj. 10 lat.

3. Organizacja przetwarzania danych

3.1. Jak należy zabezpieczać dane osobowe?

RODO odchodzi od praktyki polegającej na wskazywaniu w przepisach prawa konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora danych. Zamiast tego RODO wprowadza tzw. podejście oparte na ryzyku.

Istota podejścia opartego na ryzyku sprowadza się do tego, że każdy podmiot przetwarzający dane osobowe powinien samodzielnie określić, jakie konkretne środki zabezpieczenia danych należy wdrożyć. Dobór środków zabezpieczenia powinien być oparty o:

a. charakter, zakres, kontekst i cele przetwarzania,
b. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,
c. stan wiedzy technicznej,
d. koszt wdrażania.

Każdy podmiot przetwarzający dane osobowe powinien więc:

a. ustalić, jakie dane osobowe, w jakim charakterze, po co i w jakim środowisku przetwarza,
b. określić ryzyko naruszenia praw lub wolności osób fizycznych związane z takim przetwarzaniem,
c. dobrać odpowiednie środki zabezpieczenia danych, uwzględniając istniejące możliwości techniczne i własne możliwości finansowe.

Przykład

przetwarzanie danych osobowych przez adwokata:

- zakres danych: ryzyko wzrasta, gdy przetwarzane są dane osobowe dotyczące wyroków skazujących, stanu zdrowia czy sytuacji rodzinnej klientów,
- cele przetwarzania: ryzyko wzrasta, gdy dane są przetwarzane w celu związanym z reprezentacją klienta przed sądem, jako że tego rodzaju dane mogą być ujawniane w ramach postępowania,
- ryzyko wzrasta, gdy dane są przetwarzane na zewnętrznych serwerach, z którymi komunikacja odbywa się w sposób nieszyfrowany z wykorzystaniem sieci publicznych, a maleje, gdy dane są przetwarzane na własnych serwerach.

RODO nie nakazuje stosowania żadnych konkretnych środków zabezpieczenia danych. RODO wskazuje tylko przykładowe środki techniczne i organizacyjne, które mogą służyć osiągnięciu tego celu, tj. zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku. Są nimi w szczególności:

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

Podejście oparte na ryzyku zakłada, że każdy podmiot przetwarzający dane w sposób świadomy podejmie decyzję o stosowanych środkach zabezpieczenia. Ma to tym większe znaczenie, że podmiot ten ponosi odpowiedzialność w przypadku naruszenia bezpieczeństwa danych osobowych.

MATERIAŁY:

Jak rozumieć i stosować podejście oparte na ryzyku? – poradnik GIODO, http://www.giodo.gov.pl/pl/1520282/10294

3.2. Co się stanie z istniejącą dokumentacją ochrony danych osobowych?

Ustawa z 29 sierpnia 1997 r. nakładała na administratorów danych obowiązek przygotowania i wdrożenia tzw. dokumentacji ochrony danych osobowych, na którą składały się:

- polityka bezpieczeństwa danych osobowych,
- instrukcja zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe.

Adwokaci powinni więc byli na gruncie dotychczasowych przepisów opracować i wdrożyć dokumentację ochrony danych osobowych.

RODO nie nakłada już obowiązku wdrożenia konkretnej dokumentacji, zgodnie z podejściem opartym na ryzyku. Z drugiej strony RODO wielokrotnie odwołuje się do „polityk ochrony danych" stosowanych przez administratora. Z tego względu zaleca się dalsze stosowanie dokumentacji ochrony danych osobowych – po jej dostosowaniu do przepisów RODO, w szczególności po uwzględnieniu rejestru czynności przetwarzania danych.

3.3. Obowiązek rejestrowania czynności przetwarzania danych

Rejestr czynności przetwarzania danych osobowych jest elementem dokumentacji ochrony danych. Rejestr powinien być prowadzony odrębnie dla każdego procesu przetwarzania danych.

Adwokat, jako administrator danych, odnotowuje w rejestrze:

a. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także – gdy ma to zastosowanie – przedstawiciela administratora oraz IOD,
b. cele przetwarzania,
c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
e. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego,
f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych.

Rejestr może być prowadzony w formie pisemnej bądź w postaci elektronicznej.

Rejestr czynności nie musi być prowadzony przez przedsiębiorców zatrudniających mniej niż 250 osób, chyba że:

a. przetwarzanie może naruszać prawa lub wolności osób, których dane dotyczą,
b. przetwarzanie obejmuje szczególne kategorie danych lub dane dotyczące wyroków skazujących,
c. przetwarzanie nie ma charakteru sporadycznego.

Z tego względu jako zasadę należy przyjąć, że adwokaci powinni prowadzić rejestr.

3.4. Co to jest obowiązek uwzględniania ochrony danych w fazie projektowania?

Obowiązek uwzględniania ochrony danych osobowych w fazie projektowania to rodzaj podejścia do ochrony danych osobowych, które jest promowane w przepisach RODO. Ta filozofia opiera się na takich konkretnych rozwiązaniach jak:

- proaktywne podejście do ochrony danych osobowych,
- konieczność włączania ochrony prywatności w projekty od początku ich realizacji,
- poszanowanie dla prywatności użytkowników.

W rezultacie zasady prywatności w fazie projektowania powinny prowadzić do uczynienia prywatności domyślnym sposobem działania w organizacji przy jednoczesnym utrzymaniu pełnej funkcjonalności.

3.5. Czym jest domyślna ochrona danych?

Skutkiem zastosowania zasady uwzględniania ochrony danych w fazie projektowania powinno być doprowadzenie do sytuacji, w której domyślnie przetwarzane byłyby wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Przykład

Domyślne wyłączenie wszelkich funkcji gromadzenia danych o użytkowniku przez aplikację mobilną i konieczność ich aktywnego i świadomego uruchomienia przez użytkownika.

3.6. Kiedy należy wyznaczyć Inspektora Ochrony Danych?

Inspektor Ochrony Danych (IOD) to następca Administratora Bezpieczeństwa Informacji (ABI). Inaczej niż w przypadku ABI, wyznaczenie IOD w pewnych przypadkach jest obowiązkowe na gruncie RODO:

a. gdy dane są przetwarzane przez podmioty z sektora publicznego,
b. gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
c. gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących.

Działalność główną należy rozumieć, włączając w to działalność nierozerwalnie związaną z działalnością główną. Inspektora powinien więc np. powołać szpital, choć jego główną działalnością jest leczenie, a przetwarzanie danych działalnością nierozerwalnie związaną z taką działalnością główną.

Nie jest możliwe wskazanie konkretnej wartości czy to rozmiaru zbioru danych, czy liczby osób, których dane dotyczą, która determinowałaby dużą skalę. Zaleca się jednak, aby za przetwarzanie na dużą skalę uznawać np.:

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności,
- przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności,
- przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki.

Jednocześnie przywołuje się następujące przykłady przetwarzania danych niemieszczącego się w zakresie dużej skali:

- przetwarzanie danych pacjentów dokonywane przez pojedynczego lekarza,
- przetwarzanie danych dotyczących wyroków skazujących lub naruszeń prawa przez adwokata.

Stosując to podejście do wykonywania zawodu adwokata, należy przyjąć, że adwokat prowadzący jednoosobową kancelarię nie ma prawnego obowiązku wyznaczenia IOD, mimo że z pewnością przetwarza dane dotyczące wyroków skazujących – decydujące znaczenie ma niespełnienie przez

niego przesłanki dużej skali przetwarzania danych. Z drugiej strony wieloosobowe kancelarie z pewnością powinny zostać uznane za takie, które będą miały prawny obowiązek wyznaczenia IOD.

MATERIAŁY:
Wytyczne dotyczące inspektorów ochrony danych (WP 243),
http://www.giodo.gov.pl/1520282/id_art/9740/j/pl

3.7. Co to jest ocena skutków dla ochrony danych osobowych i kiedy należy ją przeprowadzić?

RODO odchodzi od obowiązku rejestracji zbiorów danych osobowych w GIODO – po 25 maja 2018 r. zbiory danych osobowych nie będą podlegały rejestracji, a rejestr zbiorów danych zostanie zlikwidowany. Zamiast tego jednak RODO wprowadza procedurę tzw. oceny skutków dla ochrony danych.

Ocena skutków dla ochrony danych to proces mający opisać przetwarzanie, ocenić niezbędność i proporcjonalność przetwarzania oraz pomóc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych (oceniając ryzyko i ustalając środki mające mu zaradzić). Oceny skutków dla ochrony danych to narzędzie istotne dla celów rozliczalności, ponieważ pomaga administratorom nie tylko w przestrzeganiu wymogów RODO, ale również w wykazaniu, że podjęto odpowiednie środki w celu zapewnienia zgodności z rozporządzeniem. Innymi słowy: ocena skutków dla ochrony danych to proces służący do zapewnienia i wykazania zgodności przetwarzania danych z RODO.

Ocena skutków dla ochrony danych osobowych jest obowiązkowa, jeżeli dany rodzaj przetwarzania danych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W przepisach RODO wskazano trzy przypadki, gdy przeprowadzenie oceny z pewnością będzie wymagane – będzie tak, jeżeli dochodzi do:

a. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,
b. przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących, lub
c. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Przykłady

- przeprowadzenie oceny jest obowiązkowe w wieloosobowej kancelarii – ze względu na przetwarzanie na dużą skalę danych osobowych dotyczących wyroków skazujących
- przeprowadzenie oceny nie jest obowiązkowe w indywidualnej kancelarii – ze względu na niespełnienie przesłanki przetwarzania na dużą skalę danych osobowych dotyczących wyroków skazujących.

Ocena skutków dla ochrony danych osobowych może być przeprowadzana według różnych metodyk i na różne sposoby. W przepisach RODO wskazano wyłącznie obowiązkowe elementy takiej oceny:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Zaleca się sporządzanie oceny w taki sposób, żeby w razie konieczności można było przedstawić ją organowi nadzorczemu.

MATERIAŁY:
Wytyczne dotyczące oceny skutków dla ochrony danych (WP 248),
http://www.giodo.gov.pl/pl/1520285/10078

3.8. Czym są uprzednie konsultacje z organem nadzorczym?

Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator danych nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. Uprzednie konsultacje są więc rodzajem postępowania administracyjnego, które należy wszcząć z w oparciu o wynik oceny skutków dla ochrony danych.

W wyniku przeprowadzonego postępowania, organ nadzorczy (PUODO) może wydać zalecenia, które ich adresat powinien wdrożyć.

3.9. Co to jest obowiązek zgłaszania naruszeń ochrony danych?

RODO nakłada na podmioty przetwarzające dane osobowe prawny obowiązek informowania o incydentach bezpieczeństwa dotyczących danych osobowych. Jest to bardzo istotna zmiana w stosunku do ustawy z 29 sierpnia 1997 r., która tego rodzaju rozwiązania w ogóle nie zawierała.

Incydent bezpieczeństwa zwany jest w przepisach RODO naruszeniem ochrony danych osobowych i może polegać na:

a. naruszeniu bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych,
b. naruszeniu bezpieczeństwa prowadzącym do nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Przykłady

- zagubienie nośnika z danymi osobowymi,
- uzyskanie dostępu do danych przez osobę do tego nieuprawnioną,
- włamanie do systemu służącego do przetwarzania danych osobowych.

O wystąpieniu incydentu należy poinformować organ nadzorczy (PUODO). Informacja powinna zostać przekazania niezwłocznie, lecz nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. W pewnych przypadkach należy również informować o incydencie osoby, których dane dotyczą – będzie tak wtedy, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą.

Przykład

zagubienie akt sprawy klienta

Treścią zgłoszenia nie jest objęta treść samych danych osobowych, stąd nie istnieją przeszkody, aby takie zgłoszenie dotyczyło również przypadków incydentów bezpieczeństwa obejmujących dane osobowe chronione tajemnicą adwokacką.

3.10. Jak zawrzeć umowę powierzenia przetwarzania danych?

W związku z wykonywaniem zawodu adwokata bardzo często dochodzi do powierzenia przetwarzania danych osobowych.

Przykłady

- korzystanie z usług zewnętrznego podmiotu świadczącego usługi księgowe,
- korzystanie z usług podmiotu zapewniającego usługi poczty elektronicznej,
- zlecenie zewnętrznemu podmiotowi zniszczenia dokumentów zawierających dane osobowe,
- zlecenie zewnętrznemu podmiotowi archiwizacji dokumentów zawierających dane osobowe.

Adwokat powinien zawrzeć z podmiotem przetwarzającym dane na zlecenie odpowiednią umowę, tzw. umowę powierzenia, w której określone zostaną zasady przetwarzania danych.

W stosunku do ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, RODO wprowadza nowe – znacznie rozbudowane – wymagania co do treści umowy powierzenia. Są to zobowiązania podmiotu przetwarzającego do:

a. przetwarzania danych wyłącznie na udokumentowane polecenie administratora,
b. zapewniania, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
c. podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomagania administratorowi w wywiązaniu się z tych obowiązków,
d. przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego – tzw. podpowierzenie przetwarzania danych jest dopuszczalne wyłącznie za zgodą administratora danych,
e. pomagania administratorowi w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,
f. usunięcia danych lub do zwrotu danych administratorowi danych po zakończeniu przetwarzania, zgodnie z decyzją administratora,
g. udostępnia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów.

Sama umowa powinna także określać:
a. przedmiot i czas trwania przetwarzania,
b. charakter i cel przetwarzania,
c. rodzaj danych osobowych,
d. kategorie osób, których dane dotyczą,
e. obowiązki i prawa administratora.

Umowa powierzenia może zostać zawarta w formie pisemnej oraz w formie elektronicznej, pod warunkiem zapewnienia integralności i autentyczności dokumentu w postaci elektronicznej.

Tym, co istotnie różni zasady powierzania przetwarzania danych w RODO od ustawy z 29 sierpnia 1997 r., jest prawny obowiązek wyboru takiego podmiotu przetwarzającego, który gwarantuje odpowiednią ochronę danych osobowych. Adwokat może mieć praktyczną trudność w wyborze takiego podmiotu – zwłaszcza gdy przetwarzanie danych ma się odbywać przez renomowanych dostawców. Z pomocą przychodzi w tym przypadku tzw. procedura certyfikacji podmiotów przetwarzających dane osobowe. Certyfikaty wydawane będą po to, żeby zaświadczyć o zgodności przetwarzania danych przez certyfikowany podmiot. Będzie to więc wskazówka dla tych, którzy poszukują odpowiedniego podmiotu przetwarzającego dane osobowe – wybór podmiotów posiadających certyfikat.

4. Prawo do bycia zapomnianym i prawo do przenoszenia danych

4.1. Prawo do bycia zapomnianym

Prawo do bycia zapomnianym jest jednym z nowych uprawnień przyznanych przez RODO osobom, których dane dotyczą. Prawo to składa się z dwóch uprawnień:

a. możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez administratora danych,
b. możliwości żądania, aby administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych lub ich kopie.

Prawo do bycia zapomnianym można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

a. jeżeli dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
b. jeżeli osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych,
c. jeżeli osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych,
d. jeżeli dane osobowe były przetwarzane „niezgodnie z prawem",
e. jeżeli dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator",

f. jeżeli dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W praktyce najważniejszym z tych przypadków będzie sytuacja, w której osoba, której dane dotyczą, wycofuje udzieloną zgodę bądź zgłasza sprzeciw.

W przypadku wykonania prawa do bycia zapomnianym administrator danych powinien zaprzestać przetwarzania danych osobowych i usunąć dane, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym. Wśród nich na szczególną uwagę zasługują:

a. istnienie przepisu prawa, który nakazuje przetwarzanie danych osobowych,
b. sytuacja, w której przetwarzanie danych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do bycia zapomnianym nie przysługuje więc w stosunku do tych danych, które adwokat przetwarza w celach związanych z wykonywaniem zawodu adwokata. W pozostałych przypadkach, w szczególności w stosunku do danych osobowych przetwarzanych w celu związanym z zatrudnianiem pracowników czy przy zbieraniu danych dla celów przesyłania klientom materiałów informacyjnych, prawo do bycia zapomnianym przysługuje na ogólnych zasadach.

Przykład

- świadek nie może skorzystać z prawa do bycia zapomnianym i skutecznie zażądać usunięcia swoich danych osobowych z akt sprawy,
- pozwany nie może skorzystać z prawa do bycia zapomnianym i skutecznie zażądać usunięcia swoich danych osobowych z akt sprawy.

4.2. Prawo do przenoszenia danych

Prawo do przenoszenia danych to prawo do:

a. otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi,
b. prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych.

Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy:

a. przetwarzanie danych odbywa się na podstawie zgody lub w celu wykonania umowy oraz
b. przetwarzanie danych odbywa się w sposób zautomatyzowany.

Prawo do przenoszenia danych obejmuje tylko dane osobowe przetwarzane przy użyciu systemów informatycznych i nie obejmuje tradycyjnych, papierowych zbiorów danych.

Wymóg automatycznego przetwarzania danych powoduje, że prawo to nie znajdzie zastosowania w sytuacji, gdy dane są przetwarzane w związku z wykonywaniem zawodu adwokata – istota tych zawodów sprowadza się bowiem do tego, że pomoc prawna jest udzielana przez adwokata, a nie przez automat. W przypadku przetwarzania danych przez adwokata dla innych celów wyłącznie korzystanie z rozwiązań służących masowej wysyłce wiadomości elektronicznych (e-mail, SMS) będzie uzasadniało skorzystanie w tym zakresie z prawa do przenoszenia danych. Z uwagi na ograniczenia dopuszczalnej reklamy wydaje się, że będzie to jednak margines problematyki przetwarzania danych osobowych w kancelariach.

MATERIAŁY

Wytyczne dotyczące prawa do przenoszenia danych (WP 242),
http://www.giodo.gov.pl/1520282/id_art/9741/j/pl

5. Kontrola przestrzegania przepisów RODO

5.1. Czy Prezes UODO będzie mógł kontrolować adwokatów?

W stanie prawnym wynikającym z ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, inspektorzy GIODO nie mieli dostępu do treści danych osobowych objętych tajemnicą adwokacką lub radcowską. Wynikało to z art. 5 ustawy, zgodnie z którym przepisy szczególne, przewidujące dalej idącą ochronę danych osobowych niż ogólne przepisy ustawy o ochronie danych osobowych, stosowało się z pierwszeństwem przed ustawą ogólną. Takimi przepisami szczególnymi są przepisy ustanawiające obowiązek zachowania tajemnicy adwokackiej, a wobec braku przepisów umożliwiających zwolnienie z tajemnicy adwokackiej na potrzeby kontroli GIODO, nie istniała żadna możliwość uzyskania przez inspektorów GIODO dostępu do danych objętych tajemnicą.

W RODO brak jest odpowiednika art. 5 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. Z tego powodu w projekcie ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych proponuje się wprowadzenie zasady, zgodnie z którą kontrola przestrzegania RODO przez Prezesa UODO nie obejmuje dostępu organu nadzorczego do danych osobowych „otrzymanych lub pozyskanych w wyniku lub w ramach działania objętego obowiązkiem zachowania tajemnicy" adwokackiej. Nie będzie również procedury zwolnienia z tajemnicy adwokackiej na potrzeby kontroli przestrzegania przepisów RODO. Także więc na gruncie RODO nie będzie istniała możliwość uzyskania przez Inspektorów w toku kontroli dostępu do danych objętych tajemnicą.

Brak możliwości uzyskania dostępu do danych objętych tajemnicą adwokacką nie oznacza jednak braku możliwości kontroli przestrzegania przepi-

sów RODO w stosunku do tych danych. Taka kontrola może objąć np. zasady zabezpieczenia tych danych – ale bez dostępu do treści samych danych.

Dane osobowe, które nie są objęte obowiązkiem zachowania tajemnicy adwokackiej, mogą być objęte kontrolą na zasadach ogólnych. Prezes UODO może więc mieć pełny dostęp np. do danych osobowych pracowników kancelarii.

5.2. Administracyjne kary pieniężne

Prezes UODO będzie uprawniony do nakładania kar finansowych na podmioty przetwarzające dane osobowe. Kary będą mogły być nakładane w wysokości do 10 000 000 EURO lub 2% obrotu ukaranego podmiotu albo do 20 000 000 EURO lub 4% obrotu ukaranego podmiotu, w zależności od tego, jakie konkretnie obowiązki zostaną naruszone.

Przydatne materiały i literatura

Zasoby dostępne w Internecie:

- Generalny Inspektor Ochrony Danych Osobowych – http://www.giodo.gov.pl/
- Ministerstwo Przedsiębiorczości i Technologii – http://www.mpit.gov.pl/
- Ministerstwo Cyfryzacji – https://www.gov.pl/cyfryzacja

Przydatna literatura:

- D. Szostek (red.), *Bezpieczeństwo danych i IT w kancelarii prawnej radcowskiej, adwokackiej, notarialnej, komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej*. Warszawa 2017.
- E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warszawa 2018.
- P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa 2018.
- B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie RODO*. Wrocław 2017.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w

.....

[nazwa kancelarii]

.....

[data sporządzenia]

Niniejsza *Polityka bezpieczeństwa*, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

Definicje:

1. **Administrator Danych** .... [nazwa kancelarii]
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych
5. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów
6. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych
7. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie
9. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w ..... [nazwa kancelarii], niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Zgodnie z art. 6 ustawy z 26 maja 1982 r. Prawo o Adwokaturze Dane osobowe przetwarzane w ..... [nazwa kancelarii], a uzyskane w związku z udzielaniem pomocy prawnej przez adwokata, objęte są tajemnicą adwokacką. Adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.
5. W zakresie przetwarzania danych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą adwokacką Administrator stosuje się do wskazanych powyżej przepisów dotyczących zachowania tajemnicy zawodowej.
6. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.
7. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
8. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 1 do niniejszej polityki.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w ..... [nazwa kancelarii].
2. Wszystkie dane osobowe w Kancelarii są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   a) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.
   b) Dane są przetwarzane są rzetelnie i w sposób przejrzysty.
   c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
   d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.
   e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.

f) Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.
g) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.
h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Administrator danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust 5 pkt d RODO).
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
   b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
   f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
   g) naruszenie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych,
6. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
   a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
   b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" – wzór Upoważnienia stanowi Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa,

c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w kancelarii w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy" stanowi element „Upoważnienia do przetwarzania danych osobowych".

7. Pracownicy zobowiązani są do:
   a) ścisłego przestrzegania zakresu nadanego upoważnienia;
   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
   c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
   d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie .... [nazwa kancelarii], obejmuje pomieszczenie biurowe kancelarii zlokalizowane w .... [adres kancelarii].
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych, Środki obejmują:
   a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.

b) Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
c) Wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów.
d) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
e) Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall.
f) Wykonywanie kopii awaryjnych danych na …
g) Ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem.
h) Zabezpieczenie dostępu do urządzeń Kancelarii przy pomocy haseł dostępu.
i) Wykorzystanie szyfrowania danych przy ich transmisji.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 3 do niniejszej polityki.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia adwokackiej tajemnicy zawodowej.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

VIII. Przekazywanie danych do państwa trzeciego

1. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

IX. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:

Załącznik nr 1
Rejestr czynności przetwarzania danych osobowych

Załącznik nr 2
Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 3
Wzór Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe

Załącznik nr 4
Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego

Nazwa oraz dane kontaktowe Administratora Danych	
Imię i nazwisko lub nazwa oraz dane kontaktowe Inspektora Ochrony Danych Osobowych	
Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	
Cele przetwarzania danych osobowych	
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
Informacja o przekazywaniu danych osobowych do państwa trzeciego	
Planowane terminy usunięcia poszczególnych kategorii danych	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	

……, dn. …… r.
[data sporządzenia]

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

nr …… [jeżeli jest nadawany]

Działając w imieniu …… niniejszym upoważniam:

Panią/Pana ……

Stanowisko ……

do przetwarzania danych osobowych w ……

…… [nazwa kancelarii]

w następującym zakresie*:

A. Okres upoważnienia:

- na okres zatrudnienia / współpracy z ……

  do dnia …… włącznie

B. Zakres upoważnienia:

- dane przetwarzane na nośnikach papierowych,
- system informatyczny,
- dane osobowe objęte zbiorem:

  a) ……

  b) ……

  c) …… [należy pozostawić właściwe]

* bez ograniczeń, podgląd danych, wprowadzanie danych, opracowywanie danych, zmienianie danych, usuwanie danych, na komputerach przenośnych) [należy pozostawić właściwe]

……
[administrator danych]

……, dn. …… r.
[data sporządzenia]

……
imię i nazwisko osoby upoważnionej

……
stanowisko

……
miejsce pracy

OŚWIADCZENIE

Oświadczam, że – w związku z wykonywaniem przeze mnie prac na rzecz …… [nazwa kancelarii] i upoważnieniem mnie do Przetwarzania danych osobowych – zostałem/łam zapoznany/a ze stosownymi przepisami i standardami ochrony danych osobowych, zobowiązuję się do przestrzegania:

- Przepisów o ochronie adwokackiej tajemnicy zawodowej,
- Przepisów o ochronie danych osobowych, w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
- Polityki Bezpieczeństwa informacji w …… [nazwa kancelarii],
- Instrukcji zarządzania systemem Informatycznym w …… [nazwa kancelarii].

W związku z powyższym zobowiązuję się do:

a. zapewnienia ochrony danych osobowych przetwarzanych w zbiorach administratora, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
b. zachowania w tajemnicy, także po zaprzestaniu wykonywania prac, wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych w zbiorach ……
c. natychmiastowego zgłaszania do Administratora Danych zaobserwowania próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru/zbiorów lub systemów informatycznych.

……
[podpis pracownika/współpracownika]

……, dn. …… r.
[data sporządzenia]

Prezes Urzędu Ochrony Danych Osobowych

……

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora Danych Osobowych	
Miejsce i dzień naruszenia	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Opis charakteru naruszenia ochrony danych	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

……
[podpis osoby uprawnionej
do reprezentowania Administratora Danych]

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

w

.....

[nazwa kancelarii]

.....

[data sporządzenia]

Niniejsza *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych …… [nazwa kancelarii] przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

Definicje:

1. **Administrator Danych** …… …… [nazwa kancelarii]
2. **Dane osobowe** – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu Przetwarzania danych
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych w …… …… [nazwa kancelarii]
5. **Sieć lokalna** – połączenie Systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych
6. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie
7. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w Systemach informatycznych
8. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem
9. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie

10. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi)

I. Procedury nadawania uprawnień do Przetwarzania danych i rejestrowania tych uprawnień w Systemie informatycznym

1. Za bezpieczeństwo Danych osobowych w Systemie informatycznym …… [nazwa systemu] i za właściwy nadzór odpowiedzialny jest Administrator Danych.
2. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych,
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator użytkownika. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i Hasło.
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do Danych osobowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

II. Metody i środki Uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W Systemie informatycznym stosuje się Uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do Uwierzytelnienia Użytkownika na poziomie dostępu do systemu operacyjnego stosuje się Hasło oraz Identyfikator użytkownika.
2. Hasła użytkowników umożliwiające dostęp do Systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.
3. Minimalna długość Hasła przydzielonego Użytkownikowi wynosi …… znaków alfanumerycznych i znaków specjalnych.
4. Zabrania się używania identyfikatora lub Hasła drugiej osoby.
5. Dla każdej osoby, której Dane osobowe są przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu,
   b) identyfikatora Użytkownika wprowadzającego Dane osobowe do systemu,
   c) informacji o odbiorcach, którym Dane osobowe zostały udostępnione.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez Użytkowników systemu

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfikatora Użytkownika oraz hasła do systemu informatycznego.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.
5. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 min braku aktywności).

IV. Tworzenie kopii zapasowych Zbiorów danych

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Kancelarii.
2. Do archiwizacji służy ..... [opisać, np. „do archiwizowania służą płyty DVD z zapisem danych z systemu"].
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.

V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających Dane osobowe oraz kopii zapasowych

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

VI. Sposób zabezpieczenia Systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:

	Obszar chroniony	Rodzaj ochrony	Typ
1.	Stacje robocze	System antywirusowy	…
2.		Firewall	…
3.		Szyfrowanie nośników danych	…
4.	Sieć wewnętrzna	System antywirusowy	…
5.		Firewall	…
6.	Poczta e-mail	Szyfrowanie danych	…
7.		System antiwirusowy i antyspamowy	…

2. Użytkowany system jest automatycznie skanowany z częstotliwością ….
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy:
   a) uruchomić program antywirusowy i skontrolować użytkowany system,
   b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.

   Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
   a) zakończyć pracę w systemie komputerowym,
   b) odłączyć zainfekowany komputer od sieci,
   c) powiadomić o zaistniałej sytuacji Administratora Danych lub ABI.
5. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

VII. Poczta elektroniczna

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. *phishing e-mail*). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

VIII. Sposoby realizacji w systemie wymogów dotyczących Przetwarzania danych

(sposób realizacji wymogu zapisania w Systemie informatycznym informacji o odbiorcach danych)

1. Informacje o odbiorcach danych zapisywane są w Systemie informatycznym, z którego nastąpiło udostępnienie.
2. Informacja o odbiorcy danych zapisana jest w Systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

IX. Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
   a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych,

b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,
d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.