Ochrona danych osobowych w biurach rachunkowych

w kontekście zmienianych przepisów prawa, w szczególności w zgodzie z RODO

Prowadzi: **Piotr Glen**
Ekspert ds. ochrony danych osobowych
Administrator bezpieczeństwa informacji

INFORAKADEMIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

(ogólne rozporządzenie o ochronie danych)

(dalej RODO)

Gotowość na 25 maja 2018 roku

INFORAKADEMIA

Dane osobowe

„dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);

możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak

imię i nazwisko,

numer identyfikacyjny,

dane o lokalizacji,

identyfikator internetowy

lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

INFORAKADEMIA

Zasady dotyczące przetwarzania danych osobowych

1. **Zasada legalności** – przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2. **Zasada celowości** – zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (wyjątek stanowi dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych („ograniczenie celu”);
3. **Zasada adekwatności**- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
4. **Zasada merytorycznej poprawności** - prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5. **Zasady ograniczenia czasowego** - przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
6. **Zasada integralności i poufności** - przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

INFORAKADEMIA

Administrator danych - „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

„**podmiot przetwarzający**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

INFORAKADEMIA

Podmiot przetwarzający

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. …
3. ….

Art. 28 RODO

INFORAKADEMIA

Relacja administrator – processor

przepisy RODO – najważniejsze obowiązki:

- weryfikacja i wybór processora (art.28 ust.1 i 5)
- nowa treść umowy processora z administratorem danych (art.28 ust.3, ust.7-9),
- zasady posługiwania się podprocessorami (art.28 ust.2 i ust.4)

INFORAKADEMIA

OBOWIĄZKI ADMINISTRATORA DANYCH (również procesora)

1. *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane (RODO art. 24. 1. art. 32.)*

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

***a**) pseudonimizację i szyfrowanie danych osobowych;*

***b**) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*

***c**)zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*

***d**) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*

INFORAKADEMIA

2. J*eżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki bezpieczeństwa obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.*

Stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

(art. 24. 2 i 3 RODO)

INFORAKADEMIA

3. *Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy: …… (RODO art. 37)*

W przypadkach innych można wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznacza się inspektora ochrony danych.

4. *Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego (art. 29 RODO)*.

Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego. (art. 32. 4. RODO)

INFORAKADEMIA

5. Zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

6. *Rejestrowanie czynności przetwarzania*

8. ***Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora***

(RODO art. 30)

INFORAKADEMIA

Rejestr czynności przetwarzania danych osobowych

Administrator: ……. *(nazwa, siedziba, dane kontaktowe przedsiębiorcy)*
Współadministrator (jeżeli dotyczy) : ……..
Przedstawiciel administratora (jeżeli dotyczy): …….
Inspektor ochrony danych (jeżeli został wyznaczony): ……

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zastosowanych do ochrony danych osobowych określa
Polityka Bezpieczeństwa Danych Osobowych wdrożona do stosowania u Administratora
Dane nie są przekazywane do odbiorców w państwach trzecich lub w organizacjach międzynarodowych

L.p.	NAZWA PROCESU/ CZYNNOŚCI (aktywności) przetwarzania danych osobowych (zbiory, zestawy danych osobowych)	CELE PRZETWARZANIA Podstawa prawna przetwarzania	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych („odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, więc np. odbiorca danych to również kadra zarządzająca, dyrektor czy dział HR, …, zewnętrzne IT)	Planowane terminy usunięcia poszczególnych kategorii danych (jeżeli jest to możliwe)
1.	OBSŁUGA KADROWO-PŁACOWA PRACOWNIKÓW ADMINISTRATORA	Przetwarzanie danych osobowych w związku z zatrudnieniem Ustawa z 26 czerwca 1974 Kodeks Pracy;	PRACOWNICY imię (imiona), nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji) wykształcenie, przebieg dotychczasowego zatrudnienia, nr PESEL, nr telefonu i adres email (dane kontaktowe) imiona i nazwiska oraz daty urodzenia dzieci pracownika, informacje o stanie zdrowia, informacje o zajęciach komorniczych, numer rachunku bankowego	Kadry, płace, dział księgowości, archiwum Zewnętrzna firma księgowo-kadrowa Rodl & Partner Urząd skarbowy i inne uprawnione organy państwowe	
1.	UMOWY ZAWIERANE Z KLIENTAMI	Wykonywanie umów z klientami – organizacjami Realizacja umów	Imię i nazwisko, adres siedziby, NIP, REGON, adres korespondencyjny, adres email numer telefonu numer rachunku bankowego; imię i nazwisko podwykonawców, dane korespondencyjne,		

INFORAKADEMIA

- **Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora**

Podmiot przetwarzający: …….. Sp. z o. o. , adres: ……

Inspektor ochrony danych (jeżeli został wyznaczony): ……

Dane nie są przekazywane do państwa trzeciego osobowych lub organizacji międzynarodowej

L.p.	**Nazwa i dane kontaktowe administratora, w imieniu którego działa podmiot przetwarzający**	**Kategorie przetwarzań dokonywanych w imieniu administratora;**	**Inny podmiot przetwarzający (podwykonawca, jeżeli dotyczy)**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa** (jeżeli jest to możliwe)
1.	Spółka xyz	Obsługa kadrowo-płacowa	**Firma informatyczna yxz**	Fizyczna ochrona obszaru przetwarzania Dostęp do danych mają osoby upoważnione, związane tajemnicą danych osobowych. Bezpieczeństwo informatyczne.

INFORAKADEMIA

Inne, dodatkowe, nowe obowiązki administratorów oraz prawa osób, których dane dotyczą:

- Rozszerzone obowiązki informacyjne,
- Nowe zasady uzyskiwania zgód na przetwarzanie danych
- Ograniczenie profilowania,
- Prawo do przenoszenia danych,
- Prawo do ograniczenia przetwarzania danych, do usuwania danych, prawo „do bycia zapomnianym”
- Informowanie o naruszeniach ochrony danych,
- Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych,
- Odpowiedzialność finansowa i odszkodowawcza

INFORAKADEMIA

Środki bezpieczeństwa

- Obszar (pomieszczenia) zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
- Przebywanie osób nieuprawnionych w pomieszczeniach jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych
- Przestrzegać zasady „czystego biurka”
- W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych - uwierzytelnianie
- Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie - włączony mechanizm audytowania zdarzeń – historia logów

- Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
- W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
- Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
- Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
- Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar zabezpiecza się w sposób zapewniający poufność i integralność tych danych.
- System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

- Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity
- Zastosowano środki zabezpieczające dane przed skutkami awarii i braku zasilania
- Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Zasada korzystania z urządzeń biurowych
- Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
- Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami i procedurami dotyczącymi ochrony danych osobowych.

Za nieprzestrzeganie przepisów ochrony danych osobowych grozi:

- ODPOWIEDZIALNOŚĆ ADMINISTRACYJNA
- ODPOWIEDZIALNOŚĆ DYSCYPLINARNA
- ODPOWIEDZIALNOŚĆ KARNA
- ODPOWIEDZIALNOŚĆ ODSZKODOWAWCZA
- ODPOWIEDZIALNOŚĆ FINANSOWA

INFORAKADEMIA

RODO NIE oznacza dla „małych” biur rachunkowych końca działalności

RODO ma służyć do wzmocnienia ochrony danych osobowych, a nie po to by nakładać kary finansowe.

Proces dostosowania firmy do RODO nie kończy się w dniu 25 maja.

W różnych biurach będą stosowane różne środki bezpieczeństwa, adekwatne do ilości i kategorii przetwarzanych danych.

Mają być zastosowane metody i środki ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

DZIĘKUJĘ ZA UWAGĘ

Piotr Glen

Specjalista ds. ochrony danych osobowych

tel.: 501 639 692

e-mail:

piotr.glen@wiknet.net.pl

www.wiknet.net.pl

INFORAKADEMIA