Ochrona danych osobowych przez Biegłych Sądowych

Katarzyna Woźniak
Inspektor Ochrony Danych
w Sądzie Okręgowym w Gliwicach

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ BIEGŁYCH

Podstawy przetwarzania danych osobowych przez Biegłych Sądowych

Biegli przetwarzają dane osobowe pozyskane w procesie opiniowania w celu sprawowania przez sądy wymiaru sprawiedliwości, a więc rozstrzygania przez sąd sporu o prawo (art. 175 i 177 Konstytucji RP i art. 1 § 2 ustawy - Prawo o ustroju sądów powszechnych), co odpowiada usprawiedliwionym celom przetwarzania danych określonych w art. 6 ust. l pkt c) i e) oraz art. 9 ust.2 pkt f) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz. U. UE.L.2016.119.1 - *dalej RODO*.

Rodzaje przetwarzanych danych

Biegli przetwarzają dane osobowe kategorii podstawowej (np. imię i nazwisko, data urodzenia, adres zamieszkania itp.) oraz szczególnej (ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby).

Biegli przetwarzają dane osobowe stron, uczestników postępowań bądź dane innych osób, do których uzyskają dostęp w ramach polecenia sporządzenia opinii dla postępowania.

Rodzaje wykonywanych operacji na przetwarzanych danych

Biegli sądowi przetwarzając dane osobowe w procesie opiniowania wykonują takie operacje jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, pobieranie, przeglądanie, ujawnianie poprzez przesłanie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Biegli nie adaptują danych osobowych, nie mają prawa do ich modyfikowania, rozpowszechniania lub innego rodzaju udostępniania. Nie mają też prawa do ich wykorzystywania w innym celu, niż sporządzenie opinii na polecenie sądu.

Obowiązki Biegłego

Biegli sądowi zobowiązani są do zapewnienia odpowiedniego poziomu ochrony powierzonych im danych osobowych na każdym etapie procesu opiniowania, zwłaszcza zapewnienia poufności, integralności i dostępności.

Biegli sądowi zobowiązani są do zapewnienia odpowiednich warunków gwarantujących przestrzeganie zasady poufności, integralności i dostępności danych osobowych.

Ponadto ponoszą pełną odpowiedzialność za powierzone dokumenty/materiały udostępnione do wydania opinii.

Obowiązki Biegłego

Biegli sądowi mają obowiązek podjęcia wszelkich środków technicznych i organizacyjnych, o których mowa w art. 32 RODO, aby w procesie przetwarzania danych osobowych zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych. Podjęte środki powinny odpowiadać aktualnej wiedzy technicznej, uwzględniać koszty ich wdrożenia, charakter, zakres, kontekst i cele przetwarzania.

Wdrażając środki techniczne biegli powinni wziąć pod uwagę zakres przetwarzanych danych, w tym danych szczególnych kategorii, o których mowa w art. 9 RODO.

Obowiązki Biegłego

Jeżeli biegły sądowy zdecyduje się na osobisty odbiór/doręczenie materiałów potrzebnych do wydania opinii, w tym akt sprawy i innych dokumentów zobowiązany jest do:

- zachowania szczególnej ostrożności podczas transportu powierzonych materiałów/akt zawierających dane osobowe na linii Sąd - biegły i biegły - Sąd,
- zabezpieczenia dokumentów, w tym akt sprawy oraz przedmiotów oględzin, poprzez umieszczenie ich w zamykanych teczkach, torbach, walizkach, czy innych zabezpieczonych pojemnikach,
- przestrzegania bezwzględnego zakazu przenoszenia dokumentów „luzem" - bez jakiegokolwiek zabezpieczenia,
- stałego nadzoru nad powierzonymi materiałami i dokumentami.

Obowiązki Biegłego

Jeżeli biegły sądowy zdecyduje się na doręczanie przesyłek za pomocą operatora pocztowego wówczas zobowiązany jest do osobistego nadania przesyłki poleconej, jak i osobistego odbioru przesyłki (bez jakiegokolwiek pośrednictwa).

Obowiązki Biegłego

Pomieszczenia, w których biegli przetwarzają dane osobowe, powinny być odpowiednio zabezpieczone przed dostępem osób nieuprawnionych, uwzględniając jedocześnie zasadę czystego biurka oraz zasadę czystego ekranu (zasady te opisano w dalszej części prezentacji).

Obowiązki Biegłego

Dokumenty i nośniki danych nie powinny pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pomieszczeniu.

Pomieszczenie należy zamknąć w sposób uniemożliwiający dostęp dla osób nieuprawnionych.

Po zakończeniu pracy dokumenty i komputerowe nośniki z danymi powinny być przechowywane w odpowiednio zabezpieczonych szafach (min. zamykanych na klucz) i zabezpieczonych pomieszczeniach.

Obowiązki Biegłego

Polityka czystego ekranu ma na celu zabezpieczenie przed nieautoryzowanym dostępem do systemów teleinformatycznych i zabezpieczenie przez ujawnieniem informacji chronionych.

Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu tak, aby niemożliwe było uzyskanie nieautoryzowanego dostępu do systemu.

Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wylogować się z systemu lub też zablokować dostęp do systemu.

Obowiązki Biegłego

Komputery wykorzystywane przez biegłych sądowych w celu sporządzenia opinii powinny być zabezpieczone co najmniej 8-znakowym hasłem (duże, małe litery, cyfry i znaki specjalne), a dysk twardy oraz zewnętrzne nośniki zaszyfrowane.

W razie potrzeby sporządzenia kopii bezpieczeństwa należy używać przenośnej pamięci szyfrowanej. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieuprawnionych.

Obowiązki Biegłego

Dopuszcza się, w sytuacjach nie cierpiących zwłoki, przesyłanie biegłym oraz przez biegłych do sądu materiałów zawierających dane osobowe za pomocą zaszyfrowanego załącznika do poczty elektronicznej.

W takim przypadku dane niezbędne do odszyfrowania przesłanej poczty Sąd lub biegły przekazują bezpośrednio za pomocą innego kanału komunikacyjnego niż poczta elektroniczna lub odrębną, drugą wiadomością e-mail.

Każdorazowo należy rozważyć możliwość dostarczenia danych za pomocą innych środków (np. osobiście na płycie CD).

Obowiązki Biegłego

Przetwarzanie danych osobowych przez biegłych powinno odbywać się na zaszyfrowanym nośniku danych. Dopuszczalne jest szyfrowanie nośnika w sposób sprzętowy i/lub programowy.

Zaleca się przetwarzanie danych osobowych na komputerze odłączonym od jakiejkolwiek sieci teleinformatycznej, w każdym wypadku z zainstalowanym aktualnym oprogramowaniem antywirusowym.

Obowiązki Biegłego

Biegli sądowi mają obowiązek zachowania w tajemnicy danych osobowych, które przetwarzają w związku ze sporządzaniem opinii.

Biegli przetwarzając dane osobowe nie mogą korzystać z usług innych podmiotów przetwarzających bez uprzedniej zgody sądu, który zlecił wydanie opinii. Jeżeli zgoda taka zostanie wydana, kolejne podmioty przetwarzające mają w zakresie przetwarzania danych nie mniejsze obowiązki, niż biegli sądowi. Jeżeli te inne podmioty przetwarzające nie wywiążą się ze spoczywających na nich obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na biegłych sądowych.

Obowiązki Biegłego

Biegli sądowi udostępniają sądowi, który zlecił wykonanie opinii, oraz Prezesowi Sądu Okręgowego w Gliwicach wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w artykule 28 RODO.

Obowiązki Biegłego

Biegli mają obowiązek niezwłocznego zawiadamiania sądu, który zlecił wykonanie opinii i Prezesa Sądu Okręgowego w Gliwicach:

- o każdym żądaniu osoby, której dane osobowe przetwarza, a związanym z realizacją jej praw odnośnie tych danych,
- o zaginięciu, zniszczeniu, kradzieży bądź usunięciu dokumentów zawierających dane osobowe,
- o zagrożeniu naruszenia bezpieczeństwa przetwarzania danych osobowych oraz o stwierdzonym naruszeniu ochrony danych przetwarzanych z wykorzystaniem urządzeń i programów informatycznych (komputery, nośniki, sieci teleinformatyczne itp.),
- o wszelkich okolicznościach niezbędnych do przeprowadzenia kompleksowej, rzetelnej i wyczerpującej analizy procesu przetwarzania danych osobowych, w szczególności informacji o rodzaju stosowanych przez biegłych środków bezpieczeństwa, certyfikacji w określonych obszarach, zidentyfikowanych zagrożeń i ryzyk przetwarzania - w razie zagrożenia naruszenia bezpieczeństwa przetwarzania danych osobowych oraz w razie stwierdzenia naruszenia ochrony danych.

Obowiązki Biegłego

Biorąc pod uwagę charakter przetwarzania danych związany z wykonywaniem przez sądy wymiaru sprawiedliwości, biegli sądowi, w miarę możliwości, pomagają Administratorowi Danych Osobowych, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw wynikających z RODO oraz w zakresie realizacji obowiązków ciążących na administratorze danych, a dotyczących bezpieczeństwa przetwarzania danych, zgłaszania naruszeń ochrony danych organowi nadzorczemu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków dla ochrony danych oraz uprzednich konsultacji.

Obowiązki Biegłego

Po zakończeniu postępowania, biegli są zobowiązani do zwrotu wszelkich dokumentów (papierowych, elektronicznych, innych) i ich kopii zawierających dane osobowe pozyskane w procesie opiniowania oraz zniszczenia danych osobowych z pozostałych dokumentów, kopii, nośników, pamięci komputera, które nie podlegały przekazaniu sądowi, chyba, że dalsze przetwarzanie danych będzie zgodne z celem wynikającym z przepisu prawa - w takim razie biegły sądowy zapewni odpowiednie do celu przetwarzania środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych.

KONIECZNOŚĆ OCHRONY DANYCH OSOBOWYCH

Dlaczego warto zabezpieczać informacje, w tym dane osobowe?

- spełnienie wymogów prawnych,
- uniknięcie kar za naruszenie bezpieczeństwa informacji,
- wzrost świadomości osób mających styczność z informacjami w zakresie ich bezpieczeństwa,
- gwarancja wobec osób trzecich, że ich dane są prawidłowo chronione.

Konieczność ochrony danych osobowych - prawo międzynarodowe -

Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób ze względu na automatyczne przetwarzanie danych o charakterze osobowym

- cel Konwencji to zagwarantowanie, na terytorium każdej ze stron konwencji, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowania jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych.

Konieczność ochrony danych osobowych - prawo międzynarodowe -

Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej 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 osobowych)

- cele to m.in. zharmonizowanie ochrony podstawowych praw i wolności osób fizycznych w związku z czynnościami przetwarzania oraz zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi.

Konieczność ochrony danych osobowych - prawo międzynarodowe -

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 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 .

Konieczność ochrony danych osobowych - polskie prawodawstwo -

Konstytucja Rzeczypospolitej Polskiej

z dnia 2 kwietnia 1997 r.

Art. 47

Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Konieczność ochrony danych osobowych - polskie prawodawstwo -

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.

Art. 51

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Konieczność ochrony danych osobowych - polskie prawodawstwo -

Ochrona danych osobowych w innych ustawach, w tym m.in.:

- Kodeks Pracy, np. wskazano jakie dane może żądać od nas pracodawca,
- Ustawa o systemie ubezpieczeń społecznych,
- Ustawa o świadczeniu usług drogą elektroniczną,
- Ustawa prawo telekomunikacyjne,
- Ustawa o dokumentach paszportowych,
- Ustawa o policji,
- Ustawa o pomocy społecznej,
- Ustawa o aktach stanu cywilnego.

Zmiany, które wprowadza RODO

Nowe przepisy wprowadzają szereg obowiązków, nowe rodzaje odpowiedzialności, ale też sankcje finansowe.

Prognozowane kary to miliony euro lub setki tysięcy złotych w zależności od podmiotu, który zostanie ukarany.

Polskie propozycje nowych przepisów o ochronie danych osobowych przewidziały możliwość nakładania kar finansowych na podmioty publiczne w wysokości **do 100 tyś zł.** Tak stanowi art. 102 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

Są też inne zmiany:

- rozszerzające kategorie odpowiedzialności za naruszenie,
- wskazujące kierowników jednostek, jako osoby odpowiedzialne bezpośrednio za poprawność przetwarzania danych osobowych
- powołujące nowych inspektorów danych osobowych (IOD) w miejsce dotychczasowych Administratorów Bezpieczeństwa Informacji,
- nakazujące przeprowadzanie audytów bezpieczeństwa, czy prowadzenie rejestrów ryzyka i naruszeń.

NAJWAŻNIEJSZE POJĘCIA

Dane osobowe

Rozporządzenie dokonało znaczącej redefinicji pojęcia „danych osobowych” (art. 4 RODO), w porównaniu do poprzednio obowiązującej ustawy o ochronie danych osobowych.

Podobnie jak miało to miejsce na gruncie Dyrektywy, dane osobowe to nadal informacje dotyczące osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania. Niemniej jednak, ze względu na szybki rozwój nowych technologii, pojęcie „danych osobowych” należało rozszerzyć o kolejne kategorie danych, które chociażby w potencjalny sposób mogłyby identyfikować daną osobę tj.: dane lokalizacyjne, adresy IP, identyfikatory internetowe czy też dane dotyczące stanu zdrowia.

Dane wrażliwe
– dane szczególnie chronione -

Artykuł 9 RODO
Przetwarzanie szczególnych kategorii danych osobowych

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Dane wrażliwe
– dane szczególnie chronione -

Powyższe nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

„**f)** przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy”.

Przetwarzanie danych
- art. 4 RODO -

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

Ochrona danych osobowych

W celu ochrony danych osobowych w sądach wprowadzono System Zarządzania Bezpieczeństwem Informacji, na który składa się m.in. Polityka Bezpieczeństwa Informacji, Polityka Bezpieczeństwa Danych Osobowych, Polityka Bezpieczeństwa Systemów Teleinformatycznych, Polityki Bezpieczeństwa poszczególnych systemów informatycznych.

Odpowiedzialność za bezpieczeństwo informacji

Zarządzanie bezpieczeństwem informacji w sądach opiera się na następującym podziale odpowiedzialności:

- Administratorzy Danych odpowiedzialni są za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji oraz poszczególnych zabezpieczeń, a także za nadzór nad przestrzeganiem Polityki Bezpieczeństwa Informacji oraz dokumentów związanych.

Odpowiedzialność za bezpieczeństwo informacji

- Kierownicy komórek organizacyjnych odpowiadają za:

a) przestrzeganie zasad ochrony informacji przez nich samych jak i przez podległych im pracowników,
b) identyfikowanie i dokumentowanie zagrożeń dla bezpieczeństwa informacji,
c) definiowanie oraz realizację działań zapobiegających zagrożeniom,
d) zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy,
e) przeszkolenie pracowników w zakresie przepisów prawa oraz wewnętrznych zasad w sądzie dotyczących ochrony informacji.

Odpowiedzialność za bezpieczeństwo informacji

Odpowiedzialność za bezpieczeństwo informacji w sądach **ponoszą wszystkie osoby,** które biorą udział w przetwarzaniu danych osobowych, **W TYM BIEGLI SĄDOWI.**

Każdy kto przetwarza dane obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi w sądach przepisami wewnętrznymi.

Odpowiedzialność za bezpieczeństwo informacji

Każdy przetwarzający obowiązany jest:

- chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych,
- chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,
- chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione,
- utrzymywać w tajemnicy powierzone hasła,
- stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej,
- powiadomić Administratora Danych Osobowych lub Inspektora Ochrony Danych o:
  - ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym,
  - nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian,
  - zniszczeniu lub możliwości zniszczenia informacji chronionych.

Administrator Danych Osobowych
- art. 4 RODO -

„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.

ADO w Sądach

Ustawa
z dnia 27 lipca 2001 r.
Prawo o ustroju sądów powszechnych (Dz.U.2020.2072)

Art. 175a. [Administratorzy danych osobowych]

§ 1. Administratorami danych osobowych:

1) sędziów i sędziów w stanie spoczynku oraz asesorów sądowych,

2) referendarzy sądowych, asystentów sędziów, dyrektorów sądów oraz ich zastępców, kuratorów sądowych, aplikantów aplikacji sądowej, aplikantów kuratorskich, urzędników oraz innych pracowników sądów,

3) **biegłych sądowych, lekarzy sądowych,** mediatorów oraz ławników,

4) kandydatów na stanowiska wymienione w pkt 1 i 2

- są prezesi i dyrektorzy właściwych sądów oraz Minister Sprawiedliwości, w zakresie realizowanych zadań.

Inspektor Ochrony Danych

RODO wprowadziło nową osobę w Sądach, tj. Inspektora Ochrony Danych (IOD), który odpowiedzialny jest za bezpieczeństwo danych, ale też za raportowanie naruszeń do urzędu kontroli.

Inspektor Ochrony Danych

Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań.

ZABEZPIECZENIE DANYCH OSOBOWYCH

Zabezpieczenie danych

Administrator danych i inne osoby przetwarzające dane osobowe, w szczególności powinny zabezpieczyć dane przed ich:

- udostępnieniem osobom nieupoważnionym,
- zabraniem przez osobę nieuprawnioną,
- przetwarzaniem z naruszeniem ustawy,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zabezpieczenie danych

Środki techniczne i organizacyjne zabezpieczenia danych:

- systemy alarmowe,
- kody dostępu,
- służby ochrony,
- ochrona przeciwpożarowa,
- prowadzenie dokumentacji,
- wydawanie upoważnień i ich ewidencjonowanie.

Zabezpieczenie danych

Środki techniczne i organizacyjne zabezpieczenia danych:

- poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
- integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalność danych – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Zabezpieczenie danych - zagrożenia

Zagrożenia poufności danych:

- pokonanie zabezpieczeń fizycznych lub programowych,
- niekontrolowana obecność w obszarze przetwarzania osób nieuprawnionych,
- niedyskrecja osób upoważnionych,
- niekontrolowane wyniesienie poza obszar przetwarzania nośników informacji i komputerów przenośnych,
- naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione,
- podsłuch.

Zabezpieczenie danych - zagrożenia

Zagrożenia integralności danych:

- uszkodzenie celowe lub przypadkowe systemu operacyjnego, urządzeń sieciowych, oprogramowania,
- nieuprawniona modyfikacja danych,
- infekcje wirusowe,
- klęski żywiołowe,
- atak terrorystyczny.

Zabezpieczenie danych - zagrożenia

Źródła zagrożeń danych:

1. ludzie
   - celowe – podsłuch, włamania do systemu, kradzież,
   - przypadkowe – pomyłki i pominięcia, skasowania pliku;

2. oprogramowanie, sprzęt komputerowy – awaria techniczna, uszkodzenie linii;

3. zdarzenia losowe – piorun, pożar, powódź.

WYMOGI DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH

Środki bezpieczeństwa

Konto użytkownika:

- mechanizm kontroli dostępu do danych,
- każdy pracujący w systemie informatycznym musi posiadać w nim konto użytkownika,
- konto użytkownika w systemie informatycznym identyfikuje osobę korzystającą z tego systemu oraz określa jej uprawnienia,
- rozpoczęcie pracy użytkownika w systemie wymaga podania identyfikatora i hasła (określają osobę korzystającą z systemu i jej uprawnienia),
- identyfikator osoby, która utraciła uprawnienia nie może być przydzielony inne osobie.

Środki bezpieczeństwa

Hasło użytkownika:

- hasło 8-znakowe (poziom podwyższony i wysoki) – zawiera duże i małe litery oraz cyfry lub znaki specjalne,
- wymóg zmiany hasła co 30 dni,
- hasło, stanowiące indywidualny kod dostępu do systemu, podlega szczególnej ochronie, hasła nie należy zapisywać, nawet w miejscach, które wydają się bezpieczne lub trudne do odgadnięcia,
- nie jest dopuszczalne ujawnianie hasła innym użytkownikom lub korzystanie z haseł innych osób,
- należy stosować hasła trudne do odgadnięcia, nie powinno się stosować haseł tworzonych według klucza np. „lato 1”, „lato 2”, itd..

Stosowanie haseł trudnych do odgadnięcia bywa kłopotliwe do zapamiętania, dlatego dobrym rozwiązaniem jest stosowania haseł zbudowanych poprzez zastępowanie znaków, np. „Z@brz3M0jeM!@$t0”

Środki bezpieczeństwa

Internet:

- należy zachować szczególną ostrożność w wypadku otwierania nieznanych stron internetowych,
- dane osobowe przesyłane pocztą elektroniczną muszą być zaszyfrowane,
- należy zachować szczególną ostrożność w wypadku otrzymania wiadomości niewiadomego pochodzenia albo takiej, która w jakikolwiek sposób może sugerować, że zawiera złośliwe oprogramowanie,
- należy zachować szczególną ostrożność w wypadku otrzymania wiadomości z żądaniem podania jakichkolwiek danych.

Środki bezpieczeństwa

Sprzęt przenośny zawierający dane osobowe, np. pendrive:

- przetwarzanie danych osobowych na sprzęcie przenośnym powinno być ograniczone do niezbędnych przypadków,
- należy zachować szczególną ostrożność podczas transportu, przechowywania i użytkowania poza obszarem przetwarzania danych,
- należy stosować środki ochrony kryptograficznej (szyfrowanie partycji).

Środki bezpieczeństwa

Złośliwe oprogramowanie – spam, trojany, itp.:

- na używanym sprzęcie musi być zawsze zainstalowane oprogramowanie antywirusowe, a jego sygnatury muszą być aktualne,
- korzystanie z pamięci przenośnych należy ograniczyć do minimum, gdyż nośniki te są najczęstszą przyczyną infekcji systemu,
- system informatyczny należy zabezpieczyć przed utratą danych spowodowaną awarią zasilania, np. listwy antyprzepięciowe.

Środki bezpieczeństwa

Niszczenie dokumentów

Wszystkie dokumenty należy bezwzględnie niszczyć w niszczarkach.

Nie jest dopuszczalne wykorzystywanie błędnych lub testowych wydruków zawierających dane osobowe jako brudnopisów.

Zmiany, które wprowadza RODO – Zgłaszanie naruszeń ochrony danych osobowych-

ADO ma obowiązek zgłaszania wszelkich naruszeń bezpieczeństwa danych osobowych w czasie **do 72 godzin od naruszenia,** bezpośrednio do właściwego organu nadzoru. Oznacza to, że każde naruszenie należy zgłosić bezpośrednio do organu nadzorczego w nieprzekraczalnym czasie 72 godzin i to niezależnie od powiadomienia przełożonych.

W niektórych przypadkach należy również poinformować o takim incydencie konkretne osoby, których dane „wyciekły”.

Zmiany, które wprowadza RODO – Zgłaszanie naruszeń ochrony danych osobowych-

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 4 pkt 12).

Zmiany, które wprowadza RODO – Zgłaszanie naruszeń ochrony danych osobowych-

Rodzaje obowiązków:

1) ewidencjonowanie wewnętrzne naruszenia ochrony danych (wszelkich naruszeń),

2) zgłaszanie naruszeń przez ADO:

- do organu nadzorczego (chyba że jest mało prawdopodobne, żeby naruszenie skutkowało ryzykiem naruszenia praw i wolności),
- do osoby, której dane dotyczą (naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą)

3) zgłaszanie naruszeń przez procesora do administratora danych.

Zmiany, które wprowadza RODO – Zgłaszanie naruszeń ochrony danych osobowych-

1) Naruszenie ochrony danych jest rodzajem **incydentu bezpieczeństwa** (nie każdy incydent bezpieczeństwa jest naruszeniem ochrony danych)

2**) Warunek określenia konsekwencji naruszenia** (z punktu widzenia ryzyka dla osoby, której dane dotyczą)

3) Rodzaje naruszeń:

- naruszenie poufności (niedozwolone lub przypadkowe ujawnienie lub dostęp do danych osobowych),
- naruszenie dostępności (niedozwolona lub przypadkowa utrata dostępu do danych osobowych lub zniszczenie ich),
- naruszenie integralności (niedozwolona lub przypadkowa zmiana danych).

Zmiany, które wprowadza RODO – Zgłaszanie naruszeń ochrony danych osobowych-

Zgłoszenie musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Środki bezpieczeństwa

Wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych

Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.

Środki bezpieczeństwa

Schemat postępowania z urządzeniami, dyskami oraz innymi elektronicznymi nośnikami informacji, zawierającymi dane osobowe, w przypadku:

- likwidacji – pozbawienie zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkodzenie w sposób uniemożliwiający ich odczytanie,

- naprawy – pozbawienie zapisu tych danych albo naprawa pod nadzorem osoby upoważnionej przez administratora danych.

Środki bezpieczeństwa

Polityka czystego ekranu

- ekrany komputerów należy ustawić w sposób uniemożliwiający osobom nieupoważnionym wgląd na ekran,
- należy zwrócić uwagę na okna znajdujące się na wprost monitora,
- w wypadku braku aktywności użytkownika, automatycznie uruchamia się wygaszacz ekranu, ponowne rozpoczęcie pracy wymaga podania hasła użytkownika,
- w momencie opuszczenia stanowiska pracy, użytkownik zobowiązany jest do zablokowania dostępu do stacji.

Środki bezpieczeństwa

Polityka czystego biurka

- na biurku powinny znajdować się jedynie te dokumenty, nad którymi aktualnie pracujemy,
- nie należy zostawiać niezabezpieczonych dokumentów, gdy odchodzimy od miejsca pracy,
- po zakończeniu pracy wszystkie dokumenty muszą być zabezpieczone przed dostępem osób nieupoważnionych,
- należy zwracać uwagę, aby nie pozostawiać dokumentów w drukarkach i faksach.

Środki bezpieczeństwa

Bezpieczeństwo fizyczne i klucze

- pokoje , w których odbywa się przetwarzanie danych wyposażone są w zamki i winny być zamykane na klucz podczas nieobecności przetwarzającego,
- pomieszczenia muszą być bezwzględnie zamykane, nawet w wypadku chwilowego opuszczenia przez przetwarzającego,
- należy zwracać szczególną uwagę na wszystkie nieupoważnione osoby znajdujące się w pobliżu pomieszczeń, w których przetwarzane są dane osobowe.

O CZYM OSOBA UPOWAŻNIONA DO PRZETWARZANIA DANYCH OSOBOWYCH MUSI PAMIĘTAĆ?

O czym muszę pamiętać ?

- do danych mogą mieć dostęp jedynie osoby upoważnione – dotyczy to również mnie,
- dokumenty, a nawet pojedyncze kartki z danymi muszę niszczyć w niszczarce – nigdy nie wyrzucam ich do kosza,
- nie pozostawiam bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych oraz w samochodzie,
- nie zapisuje danych na dyskach przenośnych,

O czym muszę pamiętać ?

- nie używam powtórnie dokumentów zadrukowanych jednostronnie,
- nie zapisuję hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku,
- dane osobowe przekazywane pocztą elektroniczną udostępniam tylko w postaci zaszyfrowanej,

O czym muszę pamiętać ?

- nie pozostawiam osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
- zachowuję w tajemnicy dane i sposoby ich zabezpieczeń, w tym także wobec osób najbliższych,
- pokój musi być zamykany na klucz, nawet jeżeli opuszczam go tylko na chwilę.

O czym muszę pamiętać ?

- zamykam okna w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych,

- zamykam okna w razie opuszczenia pomieszczenia, w szczególności po zakończeniu pracy.

Dane kontaktowe
do Inspektora Ochrony Danych
w Sądzie Okręgowym w Gliwicach:

Katarzyna Woźniak
e-mail: iod@gliwice.so.gov.pl