„Ochrona danych osobowych w projektach z Osi VIII i IX Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020”

Szkolenie poprowadzi:

Mgr Aneta Rozwadowska- Jachacz

Akademia Rozwoju eCONOMIC
20-357 Lublin, ul. Dulęby 1/21
tel. +48 602 266 323
NIP 713-128-82-70
REGON 432262056

Źródła prawne w zakresie ochrony danych osobowych

- **Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych** (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)
- (tekst pierwotny: Dz. U. 1997 r. Nr 133 poz. 883)
- (ostatni tekst jednolity: Dz. U. 2016 r. poz. 922)

Uwaga:

Zmiany obowiązują od 01.06.2016 r. (Dz. U. 2016 r. poz. 677).

- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z 19 listopada 2015 r. zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. 2015, poz. 2020).
- Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745).

Źródła prawne w zakresie ochrony danych osobowych

- Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015, poz. 719).
- Rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2008 r., Nr 229, poz. 1536).

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 maja 2011 r. (zmieniające) w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 103, poz. 601).

Źródła prawne w zakresie ochrony danych osobowych

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

Uwaga:

Rozporządzenie to określa środki bezpieczeństwa, sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych, podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne.

Uwaga:

Większość wyroków w sprawach dot. naruszeń ochrony danych osobowych można znaleźć w Centralnej Bazie Orzeczeń Sądów Administracyjnych na stronie:
http://orzeczenia.nsa.gov.pl/cbo/query

Definicje

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych definiuje pojęcie "**Administrator Danych Osobowych**" jako organ, instytucję organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych (art. 7 ustawy).

Administratorem Danych Osobowych jesteś wówczas, gdy:

- masz pracownika, petenta, klienta lub pacjenta.

Administrator Danych Osobowych (ADO) - jest zobowiązany zapewnić ochronę przetwarzanych danych osobowych, określa cel, środki i sposoby przetwarzania danych – czynności te może prowadzić samodzielnie lub po przez inne osoby, które może upoważnić (pisemnie) do realizacji zadań i obowiązków ADO nałożonych na niego przez ustawę, tj.:

- **Administrator Bezpieczeństwa Informacji (ABI)** - wyznaczony przez ADO pracownik odpowiedzialny za bezpieczeństwo przetwarzanych w jednostce danych osobowych;

Definicje

Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

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.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zgoda osoby, której dane dotyczą - oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Definicje

Pojęcie danych osobowych - za dane osobowe uważa się **wszelkie informacje dotyczące osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania.**

Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Uwaga:

Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Definicje

W świetle orzecznictwa sądów, do sfery prywatnej człowieka należą:

a) życie osobiste oraz rodzinne, w tym stosunki małżeńskie, a także konkubinat,

b) tożsamość jednostki i jej przeszłość,

c) sfera intymna – sprawy uczuć i seksu, zdrowia,

d) wyznanie i praktyki religijne,

e) stan majątkowy, w tym dane o wysokości otrzymywanego wynagrodzenia za pracę, stan zadłużenia,

f) tryb życia człowieka, sposób spędzania wolnego czasu, rozrywki, hobby,

g) karalność, informacje o popełnionych przestępstwach lub wykroczeniach.

Dane zwykłe a dane wrażliwe

Dane zwykłe	Dane wrażliwe
brak wyliczenia (*wszelkie inne dane osobowe oprócz danych wrażliwych*)	• dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (art. 27 ust. 1 u.o.d.o.)

Podstawowe wymogi –przesłanki legalizujące przetwarzanie danych osobowych

Co do zasady przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy zachodzi co najmniej jedna z następujących przesłanek:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych - zgoda musi być wyraźna i wyrażona świadomie, nie może ona być domniemana lub dorozumiana z oświadczenia woli o innej treści (zgoda nie jest konieczna jedynie do usunięcia danych osobowych);
- przetwarzanie odbywa się na podstawie przepisu prawa, ustanawiającego uprawnienia lub obowiązki;
- jest to konieczne do realizacji umowy, której osoba, której dane dotyczą, jest stroną lub też do podjęcia działań przed zawarciem umowy na żądanie tej osoby;

Podstawowe wymogi –przesłanki legalizujące przetwarzanie danych osobowych

- jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych (prawnie usprawiedliwione cele to, m.in. marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej), a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Uwaga:

W przypadku **danych wrażliwych przesłanki przetwarzania danych osobowych są bardziej rygorystyczne**, niż przesłanki pozwalające na przetwarzanie innych kategorii danych osobowych.

Podstawowe wymogi –przesłanki legalizujące przetwarzanie danych wrażliwych

Co do zasady przetwarzanie danych osobowych wrażliwych jest zabronione, a dopuszczalne jedynie w następujących okolicznościach:

- jeśli osoba, której dane dotyczą, wyraziła na to zgodę (chyba że chodzi o usunięcie dotyczących jej danych) - zgoda musi być udzielona w formie pisemnej;
- przepis prawa (innej ustawy innej) zezwala na przetwarzanie danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ochrony takich danych osobowych;
- przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dotyczą, lub innej osoby (gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody - do czasu ustanowienia opiekuna prawnego lub kuratora);
- jest to niezbędne do wykonywania statutowych zadań kościołów i związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych - w odniesieniu do członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością;

Podstawowe wymogi –przesłanki legalizujące przetwarzanie danych osobowych

- przetwarzanie dotyczy danych osobowych, które są niezbędne do dochodzenia praw przed sądem;
- przetwarzanie jest niezbędne do wykonania zadań administratora danych osobowych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
- przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
- przetwarzanie dotyczy danych osobowych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
- jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone (konieczna anonimizacja wyników);
- przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Oś VIII Regionalnego Programu Operacyjnego Województwa Łódzkiego

Oś priorytetowa VIII Zatrudnienie, której interwencja zakłada wsparcie dla określonych grup, które przyczyni się do wzrostu zatrudnienia i przedsiębiorczości w regionie.

- **Wsparcie dotyczy osób bezrobotnych**, zwłaszcza tych, które znajdują się w szczególnie trudnej sytuacji na rynku pracy, tj. osób po 50. roku życia, **kobiet, osób z niepełnosprawnościami, osób długotrwale bezrobotnych oraz o niskich kwalifikacjach, będzie odpowiadało na zidentyfikowane u tych osób trudności** i bariery oraz będzie się charakteryzowało zindywidualizowanym i kompleksowym podejściem do ich rozwiązania. W celu poprawy dostępu do rynku pracy prowadzone będą działania ukierunkowane na wzmocnienie umiejętności aktywnego poszukiwania pracy, podnoszenie kompetencji i nabywanie kwalifikacji zawodowych oraz zdobywanie doświadczenia zawodowego. Oferowana pomoc będzie obejmowała instrumenty i usługi rynku pracy wskazane w ustawie o promocji zatrudnienia i instytucjach rynku pracy, z wyłączeniem robót publicznych.

Oś priorytetowa VIII –grupy docelowe

11. GRUPA DOCELOWA/ OSTATECZNI ODBIORCY WSPARCIA	
Działanie VIII.2	
Poddziałanie VIII.2.1	1. osoby po 29. roku życia pozostające bez pracy (bezrobotne, poszukujące pracy i bierne zawodowo), które znajdują się w szczególnie trudnej sytuacji na rynku pracy, tj.: – osoby po 50. roku życia – osoby długotrwale bezrobotne – kobiety – osoby z niepełnosprawnościami – osoby o niskich kwalifikacjach 2. w przypadku uruchomienia ukierunkowanych schematów mobilności transnarodowej: – osoby poszukujące pracy – pracodawcy krajowi oraz pracodawcy z Unii Europejskiej i Europejskiego Obszaru Gospodarczego i Szwajcarii
Poddziałanie VIII.2.2	1. osoby po 29. roku życia pozostające bez pracy (bezrobotne, poszukujące pracy i bierne zawodowo), które znajdują się w szczególnie trudnej sytuacji na rynku pracy, tj.: – osoby po 50. roku życia – osoby długotrwale bezrobotne – kobiety – osoby z niepełnosprawnościami – osoby o niskich kwalifikacjach

11. GRUPA DOCELOWA/ OSTATECZNI ODBIORCY WSPARCIA	
Działanie VIII.3	
Poddziałanie VIII.3.1	Osoby po 29. roku życia pozostające bez pracy (bezrobotne, poszukujące pracy i bierne zawodowo), zamierzające rozpocząć prowadzenie działalności gospodarczej, znajdujące się w najtrudniejszej sytuacji na rynku pracy: – osoby po 50. roku życia – osoby długotrwale bezrobotne – kobiety – osoby z niepełnosprawnościami – osoby o niskich kwalifikacjach
Poddziałanie VIII.3.2	Osoby po 29. roku życia pozostające bez pracy (bezrobotne, poszukujące pracy, bierne zawodowo), zamierzające rozpocząć prowadzenie działalności gospodarczej
Poddziałanie VIII.3.3	Osoby po 29. roku życia pozostające bez pracy (bezrobotne, poszukujące pracy i bierne zawodowo), zamierzające rozpocząć prowadzenie działalności gospodarczej, znajdujące się w najtrudniejszej sytuacji na rynku pracy: – osoby po 50. roku życia – osoby długotrwale bezrobotne – kobiety – osoby z niepełnosprawnościami – osoby o niskich kwalifikacjach
Poddziałanie VIII.3.4	Osoby po 29. roku życia pozostające bez pracy (bezrobotne, poszukujące pracy i bierne zawodowo), zamierzające rozpocząć prowadzenie działalności gospodarczej, znajdujące się w najtrudniejszej sytuacji na rynku pracy: – osoby po 50. roku życia

Oś IX Regionalnego Programu Operacyjnego Województwa Łódzkiego

Oś priorytetowa IX Włączenie społeczne zakłada wsparcie w zakresie aktywizacji społeczno-zawodowej osób zagrożonych ubóstwem lub wykluczeniem społecznym oraz poprawę dostępu do usług społecznych i zdrowotnych odpowiadających na zdiagnozowane potrzeby w regionie oraz rozwój ekonomii społecznej.

Celem szczegółowym działania jest przywrócenie zdolności do zatrudnienia osób zagrożonych ubóstwem lub wykluczeniem społecznym.

Oś priorytetowa IX –grupy docelowe

11. GRUPA DOCELOWA/ OSTATECZNI ODBIORCY WSPARCIA	
Działanie IX.1 Poddziałanie IX.1.1 Poddziałanie IX.1.2 Poddziałanie IX.1.3	– Osoby zagrożone ubóstwem lub wykluczeniem społecznym, które w pierwszej kolejności wymagają aktywizacji społecznej, w tym osoby bezrobotne dla których zgodnie z ustawą z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy został określony trzeci profil pomocy (w odniesieniu do osób sprofilowanych w powiatowych urzędach pracy). – Otoczenie osób zagrożonych ubóstwem lub wykluczeniem społecznym (o ile jest ono niezbędne dla skutecznego wsparcia osób zagrożonych ubóstwem lub wykluczeniem społecznym) zdefiniowane w Wytycznych w zakresie realizacji przedsięwzięć w obszarze włączenia społecznego i zwalczania ubóstwa z wykorzystaniem środków EFS i EFRR na lata 2014-2020. Uczestnikami projektu mogą być osoby ze społeczności romskiej, o ile osoby te są osobami zagrożonymi ubóstwem lub wykluczeniem społecznym, a projekt nie ma charakteru wsparcia dedykowanego wyłącznie społeczności romskiej. Ze wsparcia wyłączone zostały osoby odbywające karę pozbawienia wolności. Wsparciem objęte będą w szczególności: – osoby zagrożone ubóstwem lub wykluczeniem społecznym doświadczające wielokrotnego wykluczenia społecznego rozumianego jako wykluczenie z powodu więcej niż jednej z przesłanek, o których mowa w rozdziale 3 pkt 11 *Wytycznych w zakresie realizacji przedsięwzięć w obszarze włączenia społecznego i zwalczania ubóstwa z wykorzystaniem środków Europejskiego Funduszu Społecznego i Europejskiego Funduszu Rozwoju Regionalnego na lata 2014-2020;* - osoby o znacznym lub umiarkowanym stopniu niepełnosprawności; -osoby z niepełnosprawnościami sprzężonymi, z niepełnosprawnością

11. GRUPA DOCELOWA/ OSTATECZNI ODBIORCY WSPARCIA	
Działanie IX.2	
Poddziałanie IX.2.1	– osoby lub rodziny zagrożone ubóstwem lub wykluczeniem społecznym oraz ich otoczenie, o ile jest ono niezbędne dla skutecznego wsparcia osób zagrożonych ubóstwem lub wykluczeniem społecznym – w przypadku wszystkich typów projektów Osoby zagrożone ubóstwem lub wykluczeniem społecznym oraz ich otoczenie zostały zdefiniowane w Wytycznych w zakresie realizacji przedsięwzięć w obszarze włączenia społecznego i zwalczania ubóstwa z wykorzystaniem środków EFS i EFRR na lata 2014-2020 – osoby będące kandydatami do sprawowania rodzinnej pieczy zastępczej oraz osoby będące kandydatami do przysposobienia dziecka – w przypadku typu projektu 1 – podmioty świadczące usługi na rzecz osób zależnych lub niesamodzielnych – w przypadku typu projektu 3 – dzieci w zakresie wczesnego wykrywania wad rozwojowych i rehabilitacji oraz ich otoczenie zgodnie z założeniami Policy paper dla ochrony zdrowia na lata 2014-2020 Krajowe ramy strategiczne. W szczególności dzieci z rodzin zagrożonych ubóstwem lub wykluczeniem społecznym – w przypadku typu projektu 4 Uczestnikami projektu mogą być osoby ze społeczności romskiej, o ile osoby

Upoważnienie pracowników do przetwarzania danych osobowych

Z art. 37 ustawy o ochronie danych osobowych wynika ,że :

„do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych”.

- Upoważnienie takie posiadać muszą wszystkie osoby, które podlegając administratorowi danych, w ramach swoich obowiązków, **rzeczywiście uzyskują dostęp do danych osobowych i wykonują jakiekolwiek operacje na tych danych** – zbierają je, przechowują, zmieniają lub usuwają.
- Mówimy nie tylko o pracownikach, ale również o osobach fizycznych działających na rzecz administratora na podstawie innych stosunków prawnych, w tym zleceniobiorcach, wykonawców działających na podstawie umowy o dzieło czy praktykantów.

Upoważnienie pracowników do przetwarzania danych osobowych

Uwaga:

- Przepisy ustawy o ochronie danych osobowych nie nakładają na administratorów danych obowiązku udzielania upoważnień na piśmie.
- W praktyce często stosowana jest forma elektroniczna, np. w postaci e-maila.
- Przepisy nie wykluczają przy tym możliwości ustnego udzielenia stosownego upoważnienia.

Uwaga:

- Na wypadek kontroli warto posiadać odpowiednie upoważnienia sporządzone w formie pisemnej.
- Pozwala to w szczególności na wykazanie, że pracownik został zapoznany z zakresem udzielonego upoważnienia, co ma niebagatelne znaczenie w kontekście obowiązku zapewnienia przez administratora odpowiedniego poziomu bezpieczeństwa danych.

Prawa i obowiązki administratora danych

Administratorem danych osobowych jest:

organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych.

Mogą to być:

- podmioty publiczne (organ państwowy, organ samorządu terytorialnego lub państwowa albo komunalna jednostka organizacyjna),
- podmioty prywatne (osoby fizyczne, osoby prawne oraz jednostki organizacyjne nie posiadające osobowości prawnej, jeżeli przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych (art. 3 ust. 2 ustawy).

Prawa i obowiązki administratora danych

Administrator danych ma obowiązek przetwarzać dane osobowe po spełnieniu jednego z warunków zawartych w art.23 – dotyczących legalności.

Prawa i obowiązki administratora danych

Administrator danych jest obowiązany do prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz podjęte środki organizacyjne i techniczne, zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń i kategorii danych nią objętych.

Na dokumentację składają się:

- polityka bezpieczeństwa,
- instrukcja zarządzania systemem informatycznym,
- upoważnienia dla pracowników,
- ewidencja upoważnień,
- umowy powierzenia przetwarzania danych osobowych.

Prawa i obowiązki administratora danych

- ✓ **przeprowadzenie analiza ryzyka** w zakresie utraty poufności przetwarzanych danych, ich zniszczenia, utraty lub nieuprawnionej modyfikacji,
- ✓ **ustanowienie** – odpowiedniej do celów i zakresu przetwarzania danych – polityki bezpieczeństwa i **procedur zarządzania** tym bezpieczeństwem,
- ✓ **wdrożenie** i stosowanie **środków** przewidzianych w ustanowionej polityce bezpieczeństwa,
- ✓ **szkolenie pracowników** w zakresie zgodnego z prawem przetwarzania danych osobowych, w tym odpowiedzialności za jego naruszenie,
- ✓ **zapewnienie odpowiednich relacji** między administratorem danych i podmiotem, któremu powierzono przetwarzanie danych lub administratorem danych i użytkownikiem będącym jednocześnie podmiotem, którego dane są przetwarzane.

Prawa i obowiązki administratora danych

Ewidencja osób upoważnionych powinna być sporządzona w formie pisemnej (z podpisem lub pieczątką).

Ewidencja musi zawierać poniższe informacje:

a) imię i nazwisko osoby upoważnionej,

b) datę nadania i ustania upoważnienia,

c) zakres upoważnienia do przetwarzania danych,

d) identyfikator, w przypadku gdy dane przetwarzane są w systemie informatycznym.

Uwaga:

Osoby upoważnione do dostępu do danych osobowych, są zobowiązane zachować te dane w tajemnicy

Obowiązki pracowników dot. przetwarzania danych osobowych

Obowiązki pracowników:

- Obowiązkiem, jaki przede wszystkim musi spełnić każdy podmiot przetwarzający dane osobowe (np. pracownik) jest legitymowanie się odpowiednią podstawą prawną, uzasadniającą sam fakt przetwarzania przez ten podmiot określonych danych osobowych.
- Przestrzeganie zakresu nadanego w upoważnieniu przez ABI.
- Zabezpieczanie i „pilnowanie" zgromadzonych danych.
- Nieudostępnianie danych innym osobom /pracowników/ kontrahentom.
- Korzystanie z nadanych uprawnień w okresie wskazanym w upoważnieniu.

Przetwarzanie danych kadrowych (akta pracowników)

Jednym z podstawowych obowiązków pracodawcy wynikających z art. 94 pkt 9a kodeksu pracy jest prowadzenie dokumentacji w sprawach związanych ze stosunkiem pracy. **Przypomnę,** że pracodawca musi założyć i prowadzić dla każdego pracownika akta osobowe, w tym:

1. prowadzenia dokumentacji dotyczącej podejrzeń o choroby zawodowe, chorób zawodowych, wypadków przy pracy oraz wypadków w drodze do pracy i z pracy, a także świadczeń związanych z tymi chorobami i wypadkami;
2. prowadzenia kart ewidencji czasu pracy;
3. kart ewidencji przydziału odzieży i obuwia roboczego oraz środków ochrony indywidualnej, a także wypłaty ekwiwalentu pieniężnego za używanie własnej odzieży i obuwia oraz ich pranie i konserwację:
4. przechowywania listy płac, karty wynagrodzeń albo innych dowodów, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika.

Przetwarzanie danych kadrowych (akta pracowników)

Uwaga:

W 2016 roku planowano, że od 1 czerwca 2017 r. będzie można prowadzić i przechowywać akta osobowe pracownika i pozostałą dokumentację w nowy sposób. Zmiany dotyczyły w szczególności:

- możliwość prowadzenia akt osobowych **w postaci elektronicznej,**
- zasady dokonywania zmiany postaci przechowywanych dokumentów z papierowej na elektroniczną,
- zasady postępowania z dokumentami sporządzonymi w formie pisemnej po zmianie postaci dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych (obowiązek zwrócenia pracownikowi),
- zasady potwierdzania prawdziwości odwzorowań dokumentów posiadanych w aktach osobowych pracowników i składających się na dotyczącą ich pozostałą dokumentacje pracowniczą.

Dane osobowe w działaniach marketingowych

W działaniach marketingowych często są przetwarzane dane osobowe przedsiębiorców, które podlegają ochronie, o ile dotyczą oznaczonych osób fizycznych.

Uwaga:

- Dane firm prowadzonych w formie jednoosobowej działalności gospodarczej są danymi osobowymi, ale nazwy i dane spółek cywilnych, osobowych lub kapitałowych (nawet gdyby w nazwie spółki występowały imię lub nazwisko jej właściciela) już nie są.
- Zbieranie danych osobowych wymaga uzyskania zgody osoby, od której takie informacje są zbierane. Bardzo często zdarza się, że klauzule takiej zgody są źle przygotowane, sformułowane bez znajomości reguł i praktyki interpretacyjnej GIODO oraz sądów, co skutkuje tym, że bardzo często są one (także i zgody) nieważne.).
- Zakup baz danych- nabywca może je przetwarzać dla celów marketingowych wprost na podstawie ustawy, bez zgody osoby, której one dotyczą, ale musi poinformować wszystkie osoby, których dane nabył o przetwarzaniu przez siebie.

Dane osobowe w działaniach marketingowych

1. Najczęstszym błędem jest zawieranie w treści jednej klauzuli od razu kilku oświadczeń („zgód") – na przetwarzanie danych do celów promocyjnych, marketingowych, na wysyłanie korespondencji drogą elektroniczną – gdzie pod taką przygotowaną szeroką klauzulą zainteresowana osoba składa jeden podpis (jedną „zgodę"). Takie działanie jest nieprawidłowe i skutkuje nieważnością tak uzyskanej zgody (przynajmniej w kwestii pozyskania zgody do celów marketingowych i wysyłania informacji drogą elektroniczną).
2. Podmioty organizujące działania marketingowe robią to przede wszystkim po to, aby zebrać rekordy osób zainteresowanych ich produktami lub usługami i móc je przetwarzać dla celów marketingowych (na potrzeby własnych badań, ale też w celu przesyłania ulotek, ofert). Zamieszczanie klauzuli „dla celów marketingowych" jest niepotrzebne i podważane jako ograniczająca swobodę co do zasad wyrażania zgody przez zainteresowane osoby. Mogą być uznane za nieważne przez GIODO i tym samym podmiot utraci w ogóle możliwość przetwarzania zebranych danych, w tym dla celów marketingowych.

Bezpieczeństwo danych

- Administrator danych osobowych zobowiązany jest do zapewnienia ochrony przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
- Jakość zapewnianej ochrony powinna być odpowiednia do zagrożeń oraz kategorii danych nią objętych.
- Ponadto zgodnie z art. 38 ustawy administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

• Ogólnie przez pojęcie zapewnienia ochrony przetwarzanym danym należy rozumieć działanie mające na celu zabezpieczenie przed czymś niekorzystnym, niebezpiecznym. W odniesieniu do danych osobowych będą to działania mające na celu zapewnienie, aby były one pozyskiwane i przetwarzane zgodnie z przepisami prawa. Oznacza to, że muszą być zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem.

Bezpieczeństwo danych

Uwaga:

- Pojęcie „ochrony danych” należy utożsamiać z pojęciem „bezpieczeństwa informacji”, stosowanym w literaturze z zakresu bezpieczeństwa teleinformatycznego. Według normy PN-ISO/IEC-17799:2005 mówimy o **zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności.**
- Gdy przetwarzamy dane osobowe w systemach informatycznych, ważne jest zabezpieczenie właściwości tych systemów, tj. zapewnieniu skuteczności i ciągłości zachowywania przez systemy wymaganych właściwości, które mogą być utracone na skutek błędów popełnionych przez administratora systemu lub celowych działań osób nieupoważnionych do ingerowania w dany system informatyczny. Zatem należy chronić przetwarzane dane ale też system informatyczny, którego używamy do ich przetwarzania. Stąd też w przepisach wykonawczych do ustawy, wydanych na podstawie delegacji zawartej w art. 39a, określone zostały wymagania dotyczące nie tylko polityki bezpieczeństwa, ale również systemu informatycznego oraz sposobu zarządzania nim.

Odpowiedzialność pracowników

Ustawa mówi o 4 rodzajach odpowiedzialności:

- Karnej (cały rozdział ustawy),
- Administracyjnej,
- Dyscyplinarnej
- Opartej na przepisach prawa cywilnego.

Odpowiedzialność karna wynikająca z ustawy

- Część z przepisów art. 49 – 54a dotyczy tylko administratora danych.
- Pracownik może ponieść odpowiedzialność z art. 51-52 i 54a.

Art. 51 mówi o odpowiedzialności za udostępnienie lub umożliwienie dostępu do danych osobowych osobom nieupoważnionym. Jest to jeden z niewielu przykładów w ustawodawstwie regulującego kwestie **tzw. przestępstwa bezskutkowego** – polegającego na tym, że nie musi nastąpić skutek w postaci udostępnienia danych osobom nieupoważnionym, a wystarczy samo stworzenie sposobności, żeby takie przestępstwo popełnić.

Odpowiedzialność pracowników

Odpowiedzialność karna wynikająca z ustawy

Art. 52 ustawy przewiduje odpowiedzialność karną, którą mogą ponieść również pracownicy administratora danych, zagrożoną karą grzywny, ograniczenia wolności lub pozbawienia wolności do roku.

Art. 54a ustawy przewiduje odpowiedzialność karną za utrudnianie lub udaremnianie inspektorowi GIODO kontroli.

Odpowiedzialność administracyjna

Ten rodzaj odpowiedzialności został wprowadzony do ustawy nowelizacją z marca 2011 r. **Art. 12 pkt. 3** ustawy wśród zadań Generalnego Inspektora Ochrony Danych Osobowych wymienia zapewnienie wykonania obowiązków o charakterze niepieniężnym wynikających z decyzji i daje możliwość GIODO stosowania środków egzekucyjnych przewidzianych w ustawie o postępowaniu egzekucyjnym w administracji.

Odpowiedzialność pracowników

Odpowiedzialność dyscyplinarna

- **Art. 17** ustawy przewiduje kompetencję dla inspektorów GIODO dla żądania wszczęcia wobec pracownika, który dokonał naruszeń postępowania dyscyplinarnego, a także informowania o wynikach postępowania i podjętych działań.

- Jeśli pracownik został zapoznany z obowiązującymi procedurami, otrzymał upoważnienie do przetwarzania danych osobowych, odebrano od niego oświadczenie o zachowaniu danych w poufności to naruszenie zasad ochrony danych osobowych określonych w ustawie lub wewnętrznych procedurach może skutkować ciężkim naruszeniem obowiązków pracowniczych w rozumieniu art. 52 kodeksu pracy i skutkować rozwiązaniem umowy o pracę bez wypowiedzenia z winy pracownika, nie wspominając o karach dyscyplinarnych wyodrębnionych w kodeksie pracy.

Odpowiedzialność pracowników

Odpowiedzialność cywilna

Zagadnienia związane z ochroną danych osobowych stanowią cześć naszego prawa do prywatności, które to z kolei jest dobrem osobistym podlegającym ochronie na podstawie **art. 24** kodeksu cywilnego.

W związku z tym, jeżeli pracownik swoim działaniem naruszy kwestie związane z ochroną danych osobowych to może narazić się na to, że osoba poszkodowana jej działaniem wytoczy powództwo w sądzie cywilnym.

Uwaga:

Osobie poszkodowanej przysługują następujące roszczenia: roszczenie o zaniechanie naruszeń, o odszkodowanie lub zadośćuczynienie.

Podstawowe dokumenty funkcjonujące w zakresie ochrony danych osobowych

- **Polityka bezpieczeństwa informacji i ochrony danych osobowych.**

(należy ją opracować zawsze niezależnie od tego czy przetwarzane zbiory danych podlegają rejestracji w GIODO).

- **Instrukcja zarządzania systemem informatycznym.**

Oba dokumenty muszą być:

- sporządzone przez Administratora Danych,
- prawidłowe podpisane,
- przechowywane w formie papierowej lub elektronicznej,
- aktualizowane i przeglądane pod kątem poprawności ich stosowania co najmniej raz w roku,
- zawierać terminologię, zakres i cel stosowania w/w dokumentacji.

Podstawowe dokumenty funkcjonujące w zakresie ochrony danych osobowych

Polityka bezpieczeństwa	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu
Sposób przepływu danych pomiędzy poszczególnymi systemami	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	Sposób, miejsce i okres przechowywania: • elektronicznych nośników informacji zawierających dane osobowe • kopii zapasowych
	Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania
	Sposób realizacji wymogów rejestracji przez system informacji związanych z przetwarzaniem danych osobowych
	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Instrukcja zarządzania systemem informatycznym

Instrukcja powinna zawierać w szczególności:

a) procedury nadawania i rejestrowania uprawnień do przetwarzania danych w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności;

b) opis stosowanych metod i środków uwierzytelnienia,

c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

e) opis sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz ich kopii zapasowych,

f) opis sposobu zabezpieczania systemów informatycznych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

g) opis sposobu realizacji wymogów stawianych systemom informatycznym

h) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Polityka bezpieczeństwa informacji i danych osobowych

Pojęcie „**polityki bezpieczeństwa**”, należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz określonej organizacji.

Polityka bezpieczeństwa powinna odnosić się w sposób wyczerpujący do problemu zabezpieczenia danych osobowych przetwarzanych, zarówno w formie tradycyjnej, jak i w systemach informatycznych.

Celem jej opracowania jest wskazanie tych działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

Polityka bezpieczeństwa informacji i danych osobowych

W Polityce bezpieczeństwa muszą obligatoryjnie znaleźć się:

a) wykazy zbiorów danych,

b) opisy struktury tych zbiorów,

c) sposoby przepływu danych pomiędzy systemami,

d) wykazy budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym dane osobowe są przetwarzane,

e) środki techniczne i organizacyjne.

Uwaga:

Zawsze dobór środków bezpieczeństwa, jakie należy zastosować w celu ochrony danych, uzależniony jest od przyjętego dla danego zbioru poziomu bezpieczeństwa danych w systemie informatycznym.

Zbiory danych osobowych

- **Zbiór danych osobowych to,** zgodnie z art. 7 pkt 1 ustawy, „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie”.

- Cechą wyróżniającą zbiór danych od innego zestawu danych jest struktura, czyli takie uporządkowanie, które daje możliwość wyszukania konkretnych danych według określonego kryterium.

Rejestracja/aktualizacja baz danych

- Obowiązek rejestracji został wprost wpisany w art. 40 ustawy, który mówi, że administrator danych **-„właściciel”** zbioru danych osobowych; gdyż poszczególne dane osobowe są dobrami osobistymi tych osób) jest obowiązany zgłosić zbiór danych do rejestracji GIODO, chyba że zachodzi jeden z wyjątków przewidzianych w ustawie (przykładem takiego wyjątku mogą być dane przetwarzane w celu zatrudnienia pracownika u administratora danych). Wyjątki określa art. 43 ust. 1.

Uwaga:

- Rozpoczęcie przetwarzanie danych osobowych zawartych w zbiorze danych dopiero po zgłoszeniu tegoż zbioru do GIODO.
- Natomiast jeśli firma ma zamiar przetwarzać tzw. dane wrażliwe (np. informacje o stanie zdrowia, przekonaniach religijnych) to, aby robić to w sposób legalny, musi zaczekać aż zgłoszony zbiór zostanie zarejestrowany, co trwa zwykle do kilku tygodni (a czasami nawet miesięcy).

Rejestracja/aktualizacja baz danych

Zanim zarejestruje się wniosek należy:

- zebrać dane zgodnie z którąś z przesłanek określonych w art. 23 ust. 1 (w przypadku danych wrażliwych będzie to art. 27 ust. 2); dopełnić obowiązki informacyjne (art. 24 i 25); podjąć środki techniczne niezbędne do zabezpieczenia przetwarzanych danych osobowych (art. 36 ust. 1 oraz przepisy wskazane w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; podjąć środki organizacyjne niezbędne do zabezpieczenia przetwarzanych danych osobowych (art. 36, art. 37, art. 38, art. 39 oraz przepisy wskazane w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

Rejestracja/aktualizacja baz danych

- zadbać o legalne powierzenie przetwarzania danych osobowych, jeżeli firma ma zamiar wykorzystywać w procesie przetwarzania danych także inne firmy (np. w przypadku hostingu, biura rachunkowego, call center);
- udostępnić dane osobowe zgodnie z wymogami ustawy.

Już na samym początku zdecydować czy będziemy rejestrować nowy zbiór, w którym przetwarzać będziemy tylko dane zwykłe (zgłoszenie na podstawie art. 40) czy też wrażliwe (zgłoszenie danych przetwarzanych na podstawie jednej z przesłanek wskazanych w art. 27).

Uwaga:

W przypadku, kiedy nasze zgłoszenie dotyczy jedynie **aktualizacji istniejącego już zbioru,** należy zaznaczyć opcję nr 2, gdzie mowa jest o aktualizacji z art. 41 ust. 2 .

Ważnym elementem jest nazwanie zgłaszanego zbioru np. baza uczestników projektu, baza marketingowa, newsletter, etc. Kolejny element to wskazanie administratora danych, a więc przedsiębiorcę prowadzącego zbiór, który dokonuje zgłoszenia.

Rejestracja/aktualizacja baz danych

- W ten sam sposób, w jaki zgłasza się zbiory danych osobowych, dokonuje się również **ich aktualizacji**, która powinna nastąpić **w terminie 30 dni od daty dokonania zmiany** (z wyłączeniem zbiorów zawierających dane wrażliwe, w których można dokonać zmian dopiero po ich zarejestrowaniu).

W ustawie o ochronie danych osobowych przewidziano zwolnienia z obowiązku rejestracji, administratorzy danych osobowych nie muszą zgłaszać, m.in. zbiorów:

- w których dane przetwarzane są w związku z zatrudnieniem u nich oraz świadczeniem im usług na podstawie umów cywilnoprawnych;
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
- powszechnie dostępnych;
- przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

Rola i zadania ABI

ABI – Administrator Bezpieczeństwa Informacji

- Administrator bezpieczeństwa informacji musi być osobą fizyczną, dlatego też administrator danych osobowych niebędący osoba fizyczną nie może pełnić tej funkcji.

Uwaga:

W przypadku gdy administrator danych osobowych jest osobą fizyczną, ma on możliwość wyboru, czy wyznaczać ABI (powinien posiadać dokumenty poświadczające ten fakt), czy samemu wykonywać jego zadania. Ustawa nie określa jakie powinny być kwalifikacje osoby pełniącej tą funkcję. Przyjąć jednak należy, dla własnego bezpieczeństwa, ze osoba sprawująca tą funkcję powinna posiadać wiedze w dziedzinie informatyki i bezpieczeństwa jej systemów oraz znać podstawy prawne ochrony danych osobowych.

- **ABI jest odpowiedzialny za sprawdzanie zgodności przetwarzania danych z przepisami o ochronie danych osobowych** oraz opracowywanie w tym zakresie sprawozdania dla administratora danych oraz prowadzi jawny rejestr danych przetwarzanych przez administratora danych.

Rola i zadania ABI

- **Głównym zadaniem ABI** jest nadzorowanie przestrzegania stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
- **Do podstawowych zadań ABI** należy także nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Oznacza to, że osoba posiadające uprawnienia Administratora Bezpieczeństwa Informacji w szczególności powinna dbać o to, aby dane osobowe przetwarzane w firmie nie były udostępnione osoba nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz uległy zmianą, utratą, uszkodzeniem lub zniszczeniem.
- Ponadto **ABI powinien prowadzić dokumentację**, w której opisane są sposoby przetwarzania danych oraz środki zapobiegawcze wyżej wymienionym sytuacją.
- **Opracowanie i wdrożenie** Polityki Bezpieczeństwa Ochrony Danych Osobowych -niezależnie od tego czy przetwarzane zbiory danych podlegają rejestracji w GIODO.

Rola i zadania ABI

Na ABI spoczywają również obowiązki:

- Wydawanie i odbieranie upoważnień dla pracowników instytucji oraz prowadzenie rejestru umożliwiającego rzetelny nadzór nad systemem określającym dostęp pracowników do poszczególnych zbiorów danych.

- Nadzorowanie technicznych elementów sytemu ochrony danych osobowych takich jak np. administrowanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających zasady ich zmiany zgodnie z ustalonymi wytycznymi, dopilnowywanie, aby komputery pracowników, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby nie były udostępniane osobom nieupoważnionym czy nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe tworzonych w systemie informatycznym.

Przechowywanie i zabezpieczanie danych osobowych

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

1. **Płaszczyzna formalno-prawna;**
2. **Płaszczyzna organizacyjna;**
3. **Płaszczyzna techniczna.**

Przechowywanie i zabezpieczanie danych osobowych

Aby spełnić wymogi formalno-prawne dotyczące przetwarzania danych osobowych należy przygotować niezbędną dokumentację, między innymi taką jak:

- polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
- wnioski rejestracyjne do Generalnego Inspektora Ochrony Danych Osobowych, upoważnienia do przetwarzania danych osobowych,
- ewidencję upoważnień do przetwarzania danych osobowych,
- oświadczenia dla pracowników o zachowaniu w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
- umowy powierzenia przetwarzania danych osobowych,
- klauzule spełniające obowiązek informacyjny administratora danych osobowych,
- klauzule zgód na przetwarzanie danych osobowych,
- inne niezbędne dokumenty stosowne do metod przetwarzania i rodzaju danych osobowych.

Przechowywanie i zabezpieczanie danych osobowych

Aspekty organizacyjne.

- Przedmiotem analizy organizacyjnej jest ustalenie sposobu przetwarzania posiadanych zbiorów informacji przez poszczególne osoby mające do nich dostęp.
- W wyniku tej analizy powstają zasady pracy ze zbiorami krytycznymi - pod kątem ich ochrony.
- Ustalane są osoby mające do nich dostęp oraz wprowadzane są procedury zabezpieczające w postaci szeregu dokumentów, takich jak oświadczenia, upoważnienia czy instrukcje postępowania.

Aspekty techniczne:

Przykładowymi środkami zabezpieczającymi mogą być:

- programy antywirusowe,
- ograniczanie dostępu do danych przez właściwą politykę haseł, szyfrowanie danych,
- zastosowanie urządzeń podtrzymujących napięcie,
- materialne środki ograniczające dostępu do pomieszczeń, np. kraty w oknach, drzwi antywłamaniowe, systemy alarmowe itp.

Archiwizacja danych osobowych w wersji papierowej i elektronicznej

- Ustawa o ochronie danych osobowych **nie wskazuje** w jaki sposób należy przechowywać dokumentację zawierającą dane osobowe. Nie ma szczegółowych wytycznych dotyczących przechowywania dokumentów zawierających dane osobowe. Wskazówki można znaleźć w przepisach branżowych.
- Jest szereg rekomendacji i zaleceń odnośnie postępowania z dokumentacją zawierającą dane osobowe. Jednak żaden przepis nie nakazuje wprost np. stosowania np. drzwi antywłamaniowych, czy szaf pancernych. Trzeba stosować adekwatne zabezpieczenia - odpowiednio do ewentualnych zagrożeń oraz kategorii danych objętych ochroną.

Usuwanie dokumentów

- Po zakończeniu wymaganych okresów przechowywania i archiwizacji - dokumenty należy skutecznie usunąć. Na tą okoliczność powinna funkcjonować odpowiednia procedura brakowania dokumentów, protokoły zniszczenia, a w przypadku korzystania z usług firm zewnętrznych odpowiednia umowa.

Archiwizacja danych osobowych w wersji papierowej i elektronicznej (UOR)

Aby jednostka mogła przechowywać dokumenty w formie elektronicznej konieczne są zgodnie z art. 71–73 uor. :

- przechowywanie dokumentów w należyty sposób (m.in. chronologia, właściwy opis, łatwość odszukania);
- ochrona dokumentów przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem oraz zniszczeniem;
- stosowanie odpornych na zagrożenia nośników danych;
- dobór stosownych środków ochrony zewnętrznej;
- systematyczne tworzenie rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych, pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania dokumentów księgowych;
- zapewnienie ochrony programów komputerowych i danych systemu informatycznego przed nieupoważnionym dostępem lub zniszczeniem.

Archiwizacja danych osobowych (akt pracowników) w wersji elektronicznej

- Dodatkowo jednostka musi posiadać urządzenie pozwalające na odtworzenie dowodów w postaci wydruku, o ile inne przepisy nie stanowią inaczej.

Ograniczenia czasowe

- Artykuł 73 ust. 2 uor wprost wskazuje, że treść dowodów księgowych może być przeniesiona na informatyczne nośniki danych po zatwierdzeniu sprawozdania finansowego. Czas trwałości zapisu i możliwości jego odtworzenia w formie wydruku nie może być krótszy niż czas, przez który jednostka jest zobowiązana do przechowywania dowodów księgowych.

- **Zdaniem PIP**
  W obecnym stanie prawnym brak jest podstaw do stosowania przez pracodawców nośników elektronicznych, jako wyłącznej formy prowadzenia i przechowywania akt osobowych pracownika .
  Stanowisko Głównego Inspektoratu Pracy z 9 kwietnia 2010 r. w sprawie prowadzenia akt osobowych wyłącznie w wersji elektronicznej, nr GPP-87-4560-29/10/PE/RP

Archiwizacja danych osobowych (akt pracowników) w wersji elektronicznej

- Zdarza się, że pracodawcy posługują się dokumentacją elektroniczną i przechowują akta osobowe w formie skanów na firmowych komputerach. Taka forma prowadzenia akt osobowych aktualnie jest jednak uznawana wyłącznie za pomocniczą i nie może całkowicie zastąpić papierowych akt osobowych. Wkrótce ma to jednak ulec zmianie.

- Przepisy rozporządzenie Ministra Pracy i Polityki Socjalnej z 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika nie przewidują możliwości prowadzenia akt osobowych w formie elektronicznej. Zobowiązuje to zatrudniającego do gromadzenia i przechowywania dokumentów związanych ze stosunkiem pracy w tradycyjnej formie papierowej. Brak możliwości całkowitego „przejścia” na dokumentację elektroniczną potwierdza również Państwowa Inspekcja Pracy.

Archiwizacja danych osobowych (akt pracowników) w wersji elektronicznej

- Prowadzenie teczek pracowników w formie elektronicznej jest możliwe tylko dodatkowo i ma charakter pomocniczy. Trwają prace legislacyjne nad zmianą tych regulacji.
- Pierwotnie podawano termin 1 czerwca 2017 roku na wprowadzenie możliwości prowadzenia akt osobowych w formie elektronicznej.
- Kolejna data wprowadzenia zmian to maj 2018 roku.
- Projekt ustawy zakłada znaczne skrócenie okresu archiwizacji – z obecnie obowiązujących 50 lat do 10 lat oraz możliwość prowadzenia przez pracodawcę akt pracowniczych i dokumentacji pracowniczej w postaci elektronicznej.
- Pracodawcy mają odczuć znaczne oszczędności w obszarze realizacji zadań działów kadrowych, a nowe rozwiązania wpłynąć na unowocześnienie tego obszaru poprzez wykorzystanie technologii.

Ochrona własności intelektualnej

Własność intelektualna to zbiór praw odnoszących się w szczególności do:

- dzieł literackich, artystycznych i naukowych,
- interpretacji artystów interpretatorów oraz wykonań artystów wykonawców,
- fonogramów i programów radiowych i telewizyjnych,
- wynalazków we wszystkich dziedzinach działalności ludzkiej
- odkryć naukowych,
- ochrony przed nieuczciwą konkurencją.

Według polskich uregulowań prawnych powyższe dziedziny można przyporządkować do trzech zakresów praw:

- prawo autorskie i prawa pokrewne z prawami autorskimi,
- prawa do baz danych,
- prawo własności przemysłowej.

Ochrona własności intelektualnej

Ochrona własności intelektualnej jest ochroną praw odnoszących się do własności intelektualnej - def. Wikipedii.

Przedsiębiorstwa mogą chronić swoją własność intelektualną przez:

- prawa własności przemysłowej - patenty, wzory użytkowe, wzory, znaki towarowe, prawo do ochrony odmian roślin i oznaczenia geograficzne;
- **prawa autorskie** obejmujące oryginalne prace literackie i artystyczne, utwory muzyczne, transmisje telewizyjne, oprogramowanie, bazy danych, twórczość reklamową i multimedialną;
- strategie handlowe, jak np. tajemnice handlowe, umowy o zachowaniu poufności lub szybka produkcja.

Ochrona własności intelektualnej

Zakres ochrony

- **Dobra objęte prawem autorskim**- chronione są począwszy od momentu ich powstania, bez konieczności dokonywania ich rejestracji.
- **Ochrona ta jest co do zasady powszechna** - na podstawie umów międzynarodowych obejmuje prawie wszystkie kraje świata.
- **Ochrona baz danych-** zakres ochrony odnosi się do ochrony baz danych, ale nie obejmuje programów komputerowych użytych do sporządzenia baz danych lub korzystania z nich.
- **Dobra objęte prawem własności przemysłowej -** w większości przypadków - muszą zostać zarejestrowane w Urzędzie Patentowy RP, który na podstawie zgłoszenia (wniosku) wydaje decyzje w sprawie udzielenia patentu, praw ochronnych lub praw z rejestracji. Zakres tej ochrony jest w istotny sposób ograniczony.
- **Ochrona obejmuje wyłącznie teren RP.**

Ochrona własności intelektualnej

Najczęściej stosowane formy ochrony własności intelektualnej :

- ✓ możliwość powołania się na prawo autorskie celem zabezpieczenia interesów producenta,
- ✓ utrzymanie w tajemnicy (nieudostępnianie informacji o przedmiocie ochrony),
- ✓ udostępnianie kontrolowane (np. za pobraniem opłaty licencyjnej, po dokonaniu rejestracji użytkownika),
- ✓ zakaz kopiowania i rozpowszechniania utworu, wynalazku
- ✓ zakaz czerpania korzyści z utworu lub wynalazku, do którego danemu podmiotowi nie przysługują prawa autorskie lub pokrewne,
- ✓ prawo do kontroli nad produkcją utworów zależnych

Problemy i naruszenia w obszarze ochrony danych osobowych

- Wśród najczęściej pojawiających się problemów czy incydentów pierwsze miejsce zdecydowanie zajmuje niewłaściwie / nieprawidłowo zaadresowana poczta elektroniczna.
- Typowe jest korzystanie z przydatnej funkcji takiej jak zapamiętywanie adresów w programie pocztowym. W założeniach ma ona pomagać w wyeliminowaniu błędów, jakie pojawiają się przy ręcznym wprowadzaniu adresu odbiorcy.
- Innym częstym naruszeniem bezpieczeństwa danych w korespondencji elektronicznej jest niewykorzystywanie opcji „kopii ukrytej", czyli nieukrywanie poszczególnych odbiorców wiadomości (poza głównym).
- Utrata nośnika danych - utrata (zagubienie, kradzież) telefonu, laptopa, pamięci przenośnej, a nawet torby czy teczki z danymi w wersji papierowej.

Uwaga:

W przypadku kradzieży sprzętu elektronicznego nie zwracamy uwagi na dane, które się na nim znajdowały.

Problemy i naruszenia w obszarze ochrony danych osobowych

- **„Zapominanie”** lub zaniedbanie przez ABI dopilnowania aby pracownik, który nie przetwarza już danych osobowych miał zamknięte konto.
- Przekazywanie przez pracowników loginów i haseł do konta.
- Brak zabezpieczenia hasłem.
- Wyrzucanie notatek do kosza zamiast korzystanie z niszczarek.
- Przekazywanie danych serwisom – nie usuwanie lub brak zabezpieczenia plików - formatowanie lub defragmentowanie urządzenie przed przekazaniem go poza jednostkę jest niewystarczające.

Zagrożenia związane z bezpieczeństwem informacji

W literaturze przedmiotu problematyka zagrożeń informacyjnych prezentowana jest w bardzo szerokim ujęciu.

Zagrożenia mogące naruszać bezpieczeństwo informacji są bardzo zróżnicowane, ale można je podzielić na 4 grupy:

- zagrożenia sieciowe (technologiczne),
- zagrożenia środowiskowe (losowe),
- zagrożenia wynikające z błędów lub celowego działania człowieka,
- tradycyjne zagrożenia informacyjne.

Zagrożenia związane z bezpieczeństwem informacji

O zagrożeniach sieciowych mówimy w przypadku zagrożeń bezpośrednio związanych z gromadzeniem, przechowywaniem i przetwarzaniem informacji w sieciach i systemach teleinformatycznych (np. przestępstwa komputerowe, cyberterroryzm, walka informacyjna) oraz zagrożenia będące następstwem niedostatecznych rozwiązań strukturalnych i organizacyjnych.

Jest to spowodowane m. in. znacznym wzrostem liczby ataków internetowych, których celem jest głównie uzyskanie nieautoryzowanego dostępu, kradzież danych, spowodowanie awarii oprogramowania lub sprzętu lub przejęcia kontroli nad maszyną.

Zagrożenia związane z bezpieczeństwem informacji

Zagrożenia losowe (środowiskowe) – wszelkiego rodzaju klęski żywiołowe, katastrofy i wypadki, które wpływają na stan bezpieczeństwa informacji.

- Dotyczą one nie tylko informacji zapisanych w formie elektronicznej, ale także „tradycyjnej” – papierowej.
- Oba nośniki mogą ucierpieć w podobnym stopniu podczas pożaru, powodzi czy katastrofy budowlanej.

Tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyfikacyjna bądź sabotażowa (ukierunkowana na zdobycie informacji lub ofensywną dezinformację prowadzoną przez inne osoby, podmioty i organizacje).

Zagrożenia związane z bezpieczeństwem informacji

Zagrożenia informacyjne można również podzielić ze względu na **lokalizację ich źródła powstawania**, wówczas wyróżnia się zagrożenia:

- **wewnętrzne** – powstające wewnątrz organizacji; zagrożenia utratą, modyfikacją bądź uszkodzeniem mogą nastąpić w wyniku niezamierzonego (błędu lub przypadku) bądź celowego działania nieuczciwych pracowników (użytkowników);
- **zewnętrzne** – generowane poza instytucją; zagrożenia utratą, uszkodzeniem lub uniemożliwieniem wykonywania na zbiorach danych podstawowych operacji może skutkować zamierzonym bądź przypadkowym działaniem osób trzecich względem systemu czy sieci teleinformatycznej;
- **fizyczne** – bezpieczeństwo informacyjne zakłócone zostaje w wyniku wystąpienia awarii, katastrofy bądź innych nieoczekiwanych sytuacji ingerujących w system teleinformatyczny czy urządzenia sieciowe.

Zagrożenia związane z bezpieczeństwem informacji

Uwaga:

- Z jednej strony do ujawnienia, czy też wycieku informacji może nastąpić na skutek działań, bądź zaniechań samej organizacji – **błędy ludzkie**.
- Brak jakichkolwiek zasad związanych z bezpieczeństwem funkcjonujących w danej organizacji informacji, zaniedbania w tym zakresie, czy w końcu zwykła głupota, mogą spowodować zaistnienie różnych nieprawidłowości czy incydentów.
- Z drugiej strony incydent związany z bezpieczeństwem informacji może nastąpić na skutek działań podmiotów zewnętrznych wobec organizacji.

Środki zapewniające bezpieczeństwo informacji

- **Opracowanie instrukcji,** określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

- **Opracowanie procedury nadawania uprawnień** do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

- Zasady przyznawania użytkownikowi systemu informatycznego **identyfikatora,** jak również zasady nadawania lub modyfikacji uprawnień dostępu użytkownika do zasobów systemu informatycznego.

- Zasady te powinny obejmować operacje związane z nadawaniem użytkownikom **uprawnień do pracy w systemie informatycznym** - od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień, aż do momentu usunięcia konta z systemu informatycznego.

Środki zapewniające bezpieczeństwo informacji

- **Stosowane metody i środki uwierzytelnienia** oraz procedury związane z ich zarządzaniem i użytkowaniem.
- **Tryb przydzielania haseł**, tj. wskazanie, czy hasła użytkowników przekazywane mają być w formie ustnej czy pisemnej oraz wskazanie zaleceń dotyczących stopnia ich złożoności.
- Powinny zostać również wskazane, funkcjonalnie lub personalnie, osoby odpowiedzialne za przydział haseł.
- Zaleca się, aby unikać przekazywania haseł przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej.

Środki zapewniające bezpieczeństwo informacji

- **Procedury tworzenia kopii zapasowych zbiorów danych** oraz programów i narzędzi programowych służących do ich przetwarzania.

Uwaga:

- Należy wskazać metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania.
- Należy określić, dla jakich danych wykonywane będą kopie zapasowe, typ nośników, na których będą one wykonywane oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystywane.

- Powinny być także określone **Procedury wykonywania przeglądów i konserwacji systemów** oraz nośników informacji służących do przetwarzania danych.

Środki zapewniające bezpieczeństwo informacji

W opisie zabezpieczeń systemu informatycznego przed działalnością oprogramowania należy określić obszary systemu informatycznego narażone na ingerencję wirusów komputerowych oraz wszelkiego rodzaju inne szkodliwe oprogramowanie.

- Trzeba wskazać możliwe źródła przedostania się szkodliwego oprogramowania do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość jego zainstalowania się.

- Należy przedstawić zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego działania takiego oprogramowania.

Jak chronić dane osobowe – typowe błędy

Zasada „czystego biurka” pomaga zapobiegać ujawnieniu lub kradzieży informacji. Zdrowy rozsądek nakazuje, by nie zostawiać na wierzchu żadnych dokumentów, kiedy na pewien okres czasu tracimy nad nimi kontrolę (wychodzimy na zebranie lub jeśli tylko na chwilę przechodzimy do innego pokoju).

Uwaga:

Dokumenty i nośniki nie powinny pozostać niezabezpieczone po zakończeniu pracy.

Nie wolno zostawiać druków:

- na szybach skanerów;
- drukarkach;
- blatach biurek.

Pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenia.

Jak chronić dane osobowe – typowe błędy

Zasada „czystego ekranu” Urządzenia nie powinny pozostawać dostępne, ani obcym osobom, ani pracownikom, nieposiadającym stosownych uprawnień

(druk oferty handlowej na drukarce działu finansowego, gdzie drukowane są listy płac), jak również poza normalnymi godzinami pracy.

Zasada „czystego ekranu” jest analogiczna i odnosi się do serwerów, stacji roboczych oraz urządzeń przenośnych.

Uwaga:

Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone zablokowaniem klawiatury i wyłączeniem wygaszacza ekranu zabezpieczonego hasłem.

Jak chronić dane osobowe – typowe błędy

Zagrożenia, na które należy szczególnie zwrócić uwagę:

- Podglądanie ekranu lub klawiatury przez osoby nieupoważnione, podsłuchanie rozmowy telefonicznej;
- Zgubienie lub kradzież urządzenia.
- „Przypadkowa kradzież ” – złodziej nie kradnie urządzenia dla danych, a dla samego urządzenia lub „wiadoma kradzież” – istotne są dane, które urządzenie przechowuje;
- Komputery przenośne powinny być przewożone jako bagaż podręczny i jeżeli jest to możliwe maskowane podczas podróży (standardowe torby na laptopy rzucają się w oczy);
- Nie należy pozostawiać dokumentów, nośników danych i sprzętu w hotelach ani w samochodzie bez kontroli.

Zmiany w 2018 roku

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) dotyczące ochrony i przetwarzania danych osobowych od 25 maja 2018 roku ma być bezpośrednio stosowana w Polsce.

Ogólne zasady przetwarzania danych osobowych:

1. zgodność z prawem, rzetelność i przejrzystość,
2. ograniczenie celu,
3. minimalizacja danych,
4. prawidłowość,
5. ograniczenie przechowywania,
6. integralność i poufność.

Zmiany w 2018 roku

- Zgoda na przetwarzanie danych dzieci (art.8) -powyżej 16 lat za zgodą rodzica;
- Prawo do ograniczenia przetwarzania (art. 18);
- Prawo do bycia zapomnianym (art. 17);
- Prawo do przenoszenia danych (art. 20);
- Prawo sprzeciwu (art. 21);
- Wprowadzenie nowych definicji (dane biometryczne, dane genetyczne, pseudonimizancja, profilowanie);
- Wdrożenie mechanizmów „privacy by design” i „privacy by default”;
- Ułatwienia w prowadzeniu dokumentacji dla podmiotów zatrudniających poniżej 250 osób;
- Administrator Bezpieczeństwa Informacji =Inspektor Ochrony Danych;
- Nowa rola GIODO;

Fundusze Europejskie Program Regionalny

promuje łódzkie

Wojewódzki Urząd Pracy w Łodzi

Unia Europejska Europejski Fundusz Społeczny

Dziękuję za uwagę !

Aneta Rozwadowska- Jachacz

e-mail: e-conomic@wp.pl