Technik administracji II semestr

(zajęcia na 18 kwietnia 2021 r.)

Temat 1: Wykaz akt, symbol sprawy w systemie bezdziennikowym

System bezdziennikowy oparty jest na jednolitym rzeczowym wykazie akt. Jest to dokument zawierający klasyfikację wszystkich akt powstających w toku działalności firmy/instytucji. Rzeczowy wykaz akt to wykaz haseł rzeczowych oznaczonych symbolami klasyfikacyjnymi i kwalifikacją archiwalną. Wykaz akt opiera się na systemie klasyfikacji dziesiętnej, dlatego też system bezdziennikowy zwany jest też czasami systemem dziesiętnym. Na jego podstawie nadaje się pismom sygnatury, porządkuje dokumenty w teczkach i przechowuje.

W systemie kancelaryjnym bezdziennikowym, pracownik nadaje każdemu pismu odpowiedni znak, zgodny ze znakiem załatwianej sprawy. Sposób nadawania znaku jest opisany w instrukcji kancelaryjnej i opiera się na tzw. wykazie akt.

Wykaz akt jest to środek klasyfikowania wszystkich dokumentów przedsiębiorstwa według występujących w nich zagadnień. Jest to jeden z podstawowych normatywów organizujących pracę biurową (inne to instrukcja kancelaryjna i instrukcja archiwalna); służy do oznaczenia, rejestracji, łączenia i przechowywania akt.

Jako pomoc w pracy kancelaryjnej (biurowej) zaczęto używać go w początkach XIX w.

- alfabetyczno–rzeczowy wykaz akt, jeden z pierwszych systemów, teczki przechowywane były alfabetycznie.

Jednolity rzeczowy wykaz akt

- wykaz akt strukturalnych, polega on na tym, że każda komórka organizacyjna zakładu tworzy na własny użytek odrębny spis dokumentów (akt). W tym obrębie akta ułożone są w zależności od znaczenia. Z wykazami z innych komórek tworzy wykaz akt dla całego zakładu.
- jednolity rzeczowy wykaz akt – obecnie najpowszechniejszy. Jest to druga podstawowa norma regulująca organizację biurowości w danej jednostce organizacyjnej (pierwszą jest instrukcja kancelaryjna, do której stanowi on najczęściej załącznik uzgadniany w podobnym trybie). Stanowi on jednolitą, niezależną od struktury organizacyjnej urzędu lub instytucji, klasyfikację dokumentacji powstającej w toku ich działalności oraz zawiera kwalifikację archiwalną. Obejmuje wszystkie sprawy i zagadnienia z zakresu działalności instytucji, oznaczone w poszczególnych pozycjach symbolami, hasłami i kategorią archiwalną. Wykaz ten służy do oznaczania, rejestracji, łączenia i przechowywania akt. Jest oparty na systemie klasyfikacji dziesiętnej. Dzieli całość wytwarzanej w danej instytucji dokumentacji na maksymalnie 10 grup zasadniczych oznaczonych symbolami

od 0 do 9, klasy pierwszego rzędu i kolejnych rzędów dzielą się na dalsze klasy, przy czym ich liczba, w zależności od potrzeb może być mniejsza od 10. Pierwsze 4 klasy pierwszego rzędu wykazu akt obejmują zawsze tylko tzw. akta typowe, tzn. występujące we wszystkich jednostkach organizacyjnych. Klasami tymi są grupy rzeczowe akt obejmujące: 0 – Zarządzanie, 1 – Kadry, 2- Środki rzeczowe, 3 – Ekonomikę. Każda z klas pierwszego rzędu dzieli się na klasy drugiego rzędu, które obejmują hasła już bardziej szczegółowe, przez dodanie do symbolu klasyfikacyjnego pierwszego rzędu jednej z cyfr od 0-9, tj. 00-99. Tytuły klas pierwszego i drugiego rzędu nie oznaczają jeszcze tytułów teczek, ponieważ byłyby one zbyt ogólne i nieadekwatne do ich treści. Dlatego klasy drugiego rzędu ulegają dalszemu podziałowi, w wyniku czego możemy otrzymać klasy trzeciego rzędu oznaczone symbolami trzycyfrowymi, tj. 000-999, a w ramach klas trzeciego rzędu można, w miarę potrzeby, tworzyć klasy czwartego rzędu oznaczone symbolami czterocyfrowymi, tj. 0000-9999 i klasy dalszych rzędów. Klasy końcowe w poszczególnych jednorodnych tematycznie grupach spraw (hasłach), oznaczone kategorią archiwalną, odpowiadają tematycznym (rzeczowym) teczkom aktowym oznaczonym tym samym znakiem (symbolem) akt, co klasy końcowe w wykazie. Akta tematycznie jednorodne z różnych komórek organizacyjnych instytucji będą posiadały ten sam symbol klasyfikacyjny (cyfrowy) i tytuł teczki, tj. nazwę hasła klasyfikacyjnego według wykazu akt. Wyróżniać je będą symbole literowe, niekiedy cyfrowe, stanowiące oznaczenia nazwy danej komórki organizacyjnej. Dlatego zalecane jest, aby poszczególne komórki urzędu czy innej instytucji sporządziły dla własnych potrzeb szczegółowy wyciąg z wykazu akt, który będzie zawierał tylko odpowiednie symbole i hasła klasyfikacyjne występujące w ich działalności.

Klasyfikacja może być:

- treściowa (grupowanie wg treści czyli tematyki)
- formalna (wg pewnych cech zewnętrznych np. wg wymiarów, rodzaju sprawy)
- przedmiotowo-rzeczowa (jeżeli podział nastąpił wg przedmiotu sprawy)
- podmiotowa (podział został dokonany wg osób w przedsiębiorstwie)
- alfabetyczna (np. dla akt osobowych)
- geograficzna (wg państw, do których wysyłany jest towar.

Wykaz akt jest stałą klasyfikacją akt, opiera się na klasyfikacji rzeczowej wg zagadnień których dotyczą, przy czym ogólniejsze dzielone są na coraz bardziej szczegółowe.

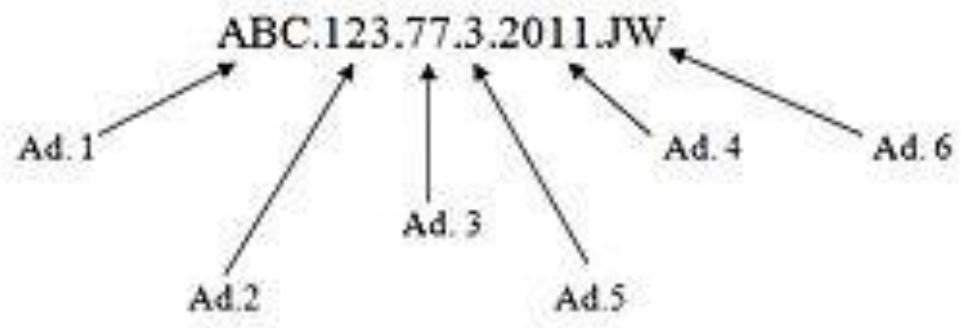
Wykaz akt opracowuje się wg dziesiętnego systemu klasyfikacji. Akta dzieli się na 10 klas zasadniczych (tj. pierwszego stopnia) o symbolach od 0 do 9. Każdą z tych klas zasadniczych można podzielić na 10 klas drugiego stopnia (powstanie więc symbol dwucyfrowy). Potem można tworzyć klasę trzeciego stopnia itd.

Znak sprawy – stała cecha rozpoznawcza całości akt danej sprawy. Nadawany jest dokumentacji tworzącej akta sprawy, która została przyporządkowana do sprawy. Dzięki niemu można łatwo odnaleźć daną sprawę w systemie teleinformatycznym oraz zapisywać pliki z daną sprawą[1].
Przykład znaku sprawy

Konstrukcja znaku sprawy (instrukcja kancelaryjna). Znak sprawy składa się z:
- oznaczenia komórki organizacyjnej (może być przyporządkowane w jednym roku kalendarzowym tylko do jednej komórki organizacyjnej, niezależnie od zmian organizacyjnych w podmiocie),
- symbolu klasyfikacyjnego z wykazu akt,
- kolejnego numeru sprawy, wynikającego ze spisu spraw,
- czterech cyfr roku kalendarzowego, w którym sprawa się rozpoczęła.

Dodatkowo może zawierać:
- numer podteczki (gdy istnieje potrzeba wydzielenia określonych spraw z danej klasy w wykazie akt w osobne podzbiory),
- inicjałów osoby odpowiedzialnej za prowadzenie sprawy.

Każdy ze znaków oddzielonych jest od siebie kropką (separatorem). Jedynym przypadkiem, kiedy minus występuje między oznaczeniem komórki organizacyjnej a symbolem klasyfikacyjnym, jest wydzielenie z wydziału istniejącego w nim referatu. Np. ABC-A.123.77.3.2011.JW.



Prezentacja pozwalając utrwalić i zebrać przedstawione powyżej informacje:
https://prezi.com/uf_i_u-jf4g_/jednolity-rzeczowy-wykaz-akt/
Przykład instrukcji zakładania i prowadzenia spraw oraz sposobu postępowania z dokumentacją:
file:///C:/Users/Piotr/AppData/Local/Temp/04AK_ZaPMK_1441_za%C5%82.pdf
Przykład rzeczowego wykazu akt:
https://www.law.uj.edu.pl/pracownia/files/jednolity_rzeczowy_wykaz_akt_gmina.pdf

Temat 2: Postępowanie z pismami niejawnymi

Zgodnie z przepisami Ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. jest to informacja wymagająca ochrony przed nieuprawnionym ujawnienie, która spowodowałaby lub mogłaby spowodować szkody dla Rzeczypospolitej Polskiej, niezależnie od formy i sposobu jej wyrażania. Informacjom niejawnym nadaje się klauzulę tajności, adekwatną do szkody jaka może zostać wyrządzona przez jej ujawnienie. (szkoda potencjalna).

Kontrolę nad ochroną informacji niejawnych sprawuje Agencja Bezpieczeństwa Wewnętrznego (ABW) oraz Służba Kontrwywiadu Wojskiego (SKW) w zakresie przewidzianym w ustawie. Klauzula niejawności nadawana jest przez osobę uprawnioną do wystawienia dokumentu (podpisania go).

Taka klauzula jest nadawana przez osobę, która jest uprawniona do podpisania dokumentu, zaś nadzór nad funkcjonowaniem systemu ochrony informacji niejawnych oraz realizacją zadań prowadzą Agencja Bezpieczeństwa Wewnętrznego (ABW) i Służba Kontrwywiadu Wojskowego (SKW).

W każdej organizacji, w której wykorzystuje się informacje niejawne, jednocześnie się je przetwarza. Przetwarzanie informacji niejawnych to „wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie 4ub udostępnianie". Oznacza to, że wskazane są dokładne działania, które oznaczają przetwarzanie, np. kopiowanie.

Osoba dopuszczona do przetwarzania informacji niejawnych powinna dawać rękojmię zachowania tajemnicy. Oznacza to „zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzoną w wyniku przeprowadzenia postępowania sprawdzającego". W praktyce możliwe jest uzyskanie rękojmi zachowania tajemnicy głównie poprzez komplementarność (uzupełnianie się) procedur postępowań sprawdzających zakończonych wydaniem poświadczenia bezpieczeństwa, poprzedzonych odbyciem przeszkolenia przez osoby, które będą miały dostęp do informacji niejawnych z zakresu ich ochrony.

Wyróżnia się **cztery główne rodzaje klauzul** nadawanych informacjom niejawnym. Klauzule informacji niejawnych zostały uszeregowane od najważniejszej do najmniej ważnej z punktu widzenia możliwej szkody, która mogłaby zostać spowodowana przez nieuprawnione ujawnienie informacji.

Informacje ściśle tajne mają najwyższą z możliwych klauzul niejawności. Oznacza to, że są najistotniejsze z punktu widzenia interesów państwa. Informacjom nadaje się klauzulę

ściśle tajne, gdy ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej poprzez:

- zagrożenie niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
- zagrożenie bezpieczeństwa wewnętrznego lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- zagrożenie sojuszy lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- osłabienie gotowości obronnej Rzeczypospolitej Polskiej;
- doprowadzenie lub powstanie możliwości doprowadzenia do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
- zagrożenie lub powstanie możliwości zagrożenia życia lub zdrowia funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
- zagrożenie lub powstanie możliwości zagrożenia życia lub zdrowia świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy, albo świadków lub osób dla nich najbliższych.

Informacje o klauzuli tajne mają niższą rangę ważności niż informacje ściśle tajne. Ich nieuprawnione ujawnienie może spowodować poważną szkodę dla Rzeczypospolitej Polskiej poprzez:

- uniemożliwienie realizacji zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- pogorszenie stosunków Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- zakłócenie przygotowań obronnych państwa lub funkcjonowania Sił Zbrojnych Rzeczypospolitej Polskiej;
- utrudnienie wykonywania czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- zakłócenie (w sposób istotny) funkcjonowania organów ścigania i wymiaru sprawiedliwości;
- przyniesienie strat znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

Informacje, które otrzymują klauzulę poufne, mają niższą rangę ważności niż informacje tajne. Ich ujawnienie może spowodować szkodę dla Rzeczypospolitej Polskiej poprzez:

- utrudnienie prowadzenia bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- utrudnienie realizacji przedsięwzięć obronnych lub negatywne wpływanie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- zakłócenie porządku publicznego lub zagrożenie bezpieczeństwa obywateli;
- utrudnienie wykonywania zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej; utrudnienie wykonywania zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, ochronę bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości; zagrożenie stabilności systemu finansowego Rzeczypospolitej Polskiej; wywołanie niekorzystnego wpływu na funkcjonowanie gospodarki narodowej

Najniższe rangą są informacje o klauzuli zastrzeżone. Informacjom nadaje się taką klauzulę, gdy nie nadano im klauzuli wyższej, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

W każdej organizacji za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej. W szczególności jest on odpowiedzialny za zorganizowanie i zapewnienie należytego funkcjonowania ochrony. Kierownikowi jednostki organizacyjnej jest podporządkowany bezpośrednio pełnomocnik ds. ochrony informacji niejawnych (pełnomocnik ochrony), który zajmuje się zagwarantowaniem przestrzegania przepisów o ochronie informacji niejawnych.

Pełnomocnik ochrony ma do wykonania następujące zadania:

- zapewnienie ochrony informacji niejawnych;
- zapewnienie ochrony systemów teleinformatycznych;
- zarządzanie ryzykiem bezpieczeństwa informacji niejawnych;
- kontrola ochrony informacji niejawnych oraz przestrzegania przepisów w tym zakresie;
- opracowywanie i aktualizowanie planu ochrony informacji niejawnych, a także - w przypadku jego wdrożenia - monitorowanie jego realizacji;
- prowadzenie szkoleń w zakresie ochrony informacji niejawnych;

- prowadzenie zwykłych oraz kontrolnych postępowań sprawdzających;
- prowadzenie aktualnego wykazu osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
- przekazywanie odpowiednio ABW (Agencja Bezpieczeństwa Wewnętrznego) lub SKW (Służba Kontrwywiadu Wojskowego) do ewidencji danych osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania dostępu.

Pełnomocnik ochrony nie realizuje wyżej wskazanych zadań samodzielnie; robi to przy pomocy wyodrębnionej organizacyjnie komórki, która jest nazywana pionem ochrony.

Dopuszczenie do pracy z informacjami niejawnymi jest możliwe po spełnieniu dwóch głównych warunków, które są zróżnicowane w zależności od tego, do jakiej klauzuli nie-jawności informacji będzie miała dostęp osoba zatrudniona.

W przypadku dostępu do wszystkich klauzul niejawności konieczne jest odbycie **szkolenia z zakresu ochrony informacji niejawnych,** które jest przeprowadzane nie rzadziej niż raz na pięć lat. Wyróżnia się trzy główne cele, jakie mają zostać osiągnięte w efekcie realizacji szkolenia.

Zapoznanie z przepisami dotyczącymi ochrony informacji niejawnych, a przede wszystkim z zasadami odpowiedzialności karnej za nieprzestrzeganie tych przepisów, ma uświadomić pracownikowi, czym grozi nieuprawnione ujawnienie informacji. Szczególne znaczenie przypisuje się zapoznaniu z zasadami ryzyka, a także umiejętności szacowania ryzyka przez osoby pracujące z informacjami niejawnymi. Cel trzeci to poznanie sposobów ochrony informacji niejawnych, a także sposobów postępowania w przypadku wystąpienia zagrożenia oraz w przypadku ujawnienia informacji.

Kolejnym warunkiem dostępu do informacji o klauzulach: poufne, tajne i ściśle tajne jest uzyskanie **poświadczenia bezpieczeństwa.** Warunkiem dostępu do informacji o klauzuli zastrzeżone jest uzyskanie pisemnego upoważnienia kierownika jednostki organizacyjnej do pracy z informacjami niejawnymi.

Poświadczenie bezpieczeństwa to dokument wydawany w wyniku postępowania sprawdzającego względem osoby, która stara się o uzyskanie dostępu do informacji niejawnych. Postępowanie sprawdzające pozwoli określić, czy dana osoba daje rękojmię zachowania tajemnicy. Postępowanie sprawdzające kończy się:

- wydaniem poświadczenia bezpieczeństwa - w przypadku pozytywnego wyniku sprawdzenia;
- odmową wydania poświadczenia bezpieczeństwa - w przypadku negatywnego wyniku sprawdzenia;

– umorzeniem postępowania - przykładowo w sytuacji rezygnacji podmiotu sprawdzanego z dalszego procedowania.

Z uwagi na potrzebę ochrony interesów państwa, jego bezpieczeństwa i jego obywateli, ustawodawca przewidział karalność czynów wymierzonych przeciwko poufności informacji niejawnych. Za taką informację należy uznać nie tylko urzędowy dokument, ale każdy sposób komunikowania i wyrażania, także na etapie jej powstawania. Informacja jest przenaszalnym dobrem, które charakteryzuje się tym, że jest pożądane przez określone podmioty. W zależności od jej rodzaju (formy) informacja może być dobrem materialnym lub niematerialnym, z naciskiem większości doktryny na ten drugi rodzaj.

Kodeks Karny w art. 265-267 przewiduje karalność osób upoważnionych do dostępu do informacji niejawnych oraz ludzi, którzy bez uprawnienia uzyskują taki dostęp. Za ujawnienie informacji ściśle tajnej oraz tajnej k.k. przewiduje karę pozbawienia wolności od 3 miesięcy do 5 lat, zaś za ujawnianie informacji poufnych lub zastrzeżonych przez funkcjonariusza publicznego grozi kara pozbawienia wolności do 3 lat.

W celu podsumowania i utrwalenia wiadomości na temat informacji niejawnych proszę obejrzeć prezentacje udostępnione w poniższych linkach:

https://prezi.com/y0u3bdvuxzyg/klasyfikacja-i-ochrona-informacji-niejawnych/

https://prezi.com/dd7t5fxjodt4/bezpieczenstwo-informacji-niejawnych/

https://prezi.com/qi6-uj2o3nmv/ochrona-i-przetwarzanie-informacji-niejawnych/

Temat 3: Ochrona danych osobowych - pojęcia

Definicja terminu "dane osobowe" została określona w ustawie o ochronie danych osobowych (UODO) z 1997 roku. Według tego dokumentu, w artykule 6, punkcie 1:

(...) za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Informacje, dzięki którym można zidentyfikować osobę to zgodne z ustawą:

(...) numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Rozwój technologii wymusił na ustawodawcach stworzenie nowej, aktualnej definicji tego, czym obecnie są dane osobowe. Wraz z wejściem w życie RODO, będącego unijnym rozporządzeniem dotyczącym ochrony danych osobowych, zmieni się również definicja, czym te dane są (art. 4, punkcie 1 RODO):

„dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

W nowej definicji wynikającej z RODO dodano dane o lokalizacji, identyfikatory internetowe oraz informacje genetyczne.

Unijny dokument dodatkowo wyjaśnia, czym są identyfikatory internetowe:

Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób.

Dane wrażliwe w RODO

Zgodnie z motywem 10 ogólnego rozporządzenia o ochronie danych (RODO) danymi wrażliwymi są szczególne kategorie danych osobowych, wymienione w art. 9 RODO:

- dane ujawniające pochodzenie rasowe lub etniczne,
- dane ujawniające poglądy polityczne,
- dane ujawniające przekonania religijne lub światopoglądowe,

- dane ujawniające przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej),
- dane dotyczące zdrowia,
- dane dotyczące seksualności lub orientacji seksualnej.

Temat 4: Zasady przetwarzania danych osobowych. Prawa osoby, której dane są przetwarzane.

Termin „przetwarzanie” oznacza szereg różnych operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub ręczny. Obejmuje takie działania 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 danych osobowych.

Przykłady przetwarzania danych:

- zarządzanie personelem i administracja kadrowo-płacowa;
- dostęp/wgląd do bazy kontaktów zawierających dane osobowe;
- przesyłanie promocyjnych wiadomości e-mail;
- niszczenie dokumentów zawierających dane osobowe;
- publikowanie/umieszczanie fotografii osoby fizycznej na stronie internetowej;
- przechowywanie adresów IP lub MAC;
- zapis obrazu wideo (CCTV).

Przetwarzanie danych osobowych jest zgodne z prawem, gdy opiera się co najmniej jednej z poniższych przesłanek:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Wykorzystywanie (przetwarzanie) danych osobowych wrażliwych jest zakazane, o ile nie jest spełniona jedna z przesłanek wskazanych w art. 9 ust. 3 RODO, m.in.:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego UE przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu,
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego UE lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego UE, przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
   d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Prawa osoby, której dane są przetwarzane

Jednym z obowiązków, jaki regulacje RODO nakładają na podmioty przetwarzające dane osobowe, jest poinformowanie osoby, której dane przetwarzamy, jakie ma w związku z tym prawa.

Prawo dostępu do danych

Realizacja tego uprawnienia polega na żądaniu od administratora danych osobowych informacji przede wszystkim, czy dane są przetwarzane przez ten podmiot. Osoba, której dane są przetwarzane ma prawo dowiedzieć się:

– w jakim celu dane są przetwarzane,

– jakie dane administrator przetwarza,

– komu je przekazuje,

– jak długo zamierza je trzymać.

Ma również prawo do otrzymania kopii tych danych.

Prawo do sprostowania danych

Jeśli zrealizowane zostanie prawo dostępu do danych, może się okazać, że przekazane dane nie mają pokrycia w rzeczywistości np. adres e-mail albo numer telefonu się nie zgadzają. W takiej sytuacji otwiera się droga do realizowania kolejnego prawa, jakim jest „prawo do sprostowania danych", czyli inaczej mówiąc poprawienia ich.

Prawo do bycia „zapomnianym"

Jednym z najważniejszych praw jakie daje RODO, jest prawo usunięcia danych osobowych z rejestru, inaczej nazywane prawem do bycia „zapomnianym". Każda osoba, której dane osobowe są przetwarzane może zwrócić się do administratora z żądaniem ich usunięcia. Oczywiście nie jest tak, że już samo zwrócenie się do podmiotu, który przetwarza nasze dane, automatycznie powoduje konieczność ich usunięcia. RODO wskazuje przypadki, kiedy z takim żądaniem można się zwrócić:

1. Brak podstawy prawnej do ich przetwarzania – najprostszym przykładem jest tutaj cofnięcie zgody. Przykładowo wyrażono zgodę na przetwarzanie danych w postaci adresu e-mail, imienia i nazwiska przez administratora „X" w celu otrzymywania od

niego powiadomień np. o promocjach. Jeśli osoba nie chce otrzymywać takich informacji, wystarczy napisać maila z żądaniem usunięcia tych. Jeśli administrator otrzyma takie żądanie, nie ma prawa dalej wysyłać nam swoich ofert, a co więcej musi dane osoby trwale skasować.

2. Zebrane dane nie są już potrzebne do celów, w których zostały zgromadzone – przykładowo przekazano swoje dane innej osobie w celu stworzenia oferty marketingowej i jej przesłania. Jeśli nie będzie zainteresowania przesłaną ofertą, również można żądać usunięcia danych – cel przetwarzania został już zrealizowany.
3. Wniesienie sprzeciwu co do przetwarzania danych osobowych.

Nie można żądać usunięcia danych w sytuacji, gdy przetwarzanie jest niezbędne:

1. w celach profilaktyki zdrowotnej (przykład: zapewnienie opieki zdrowotnej);
2. do ustalenia, obrony lub dochodzenia roszczeń;
3. w celu korzystania z prawa do wolności wypowiedzi i informacji;
4. do celów archiwalnych w interesie publicznym;
5. do wywiązania się z prawnego obowiązku wymagającego przetwarzania.

Prawo do przenoszenia danych

Prawo do ograniczenia przetwarzania danych

To uprawnienie można realizować :

1. W sytuacji, gdy nasze dane są nieprawidłowe, ale tylko do czasu ich poprawienia. Innymi słowy okazało się, że administrator ma nasz zły numer telefonu. Do momentu wpisania poprawnego (realizacji prawa do sprostowania) nie będzie mógł przetwarzać tych danych.
2. W sytuacji, gdy wniesiono sprzeciw do przetwarzania naszych danych, ale również do momentu określenia, czy sprzeciw był zasadny, czy też nie.
3. Przetwarzanie danych jest niezgodne z prawem , ale osoba której dane dotyczą nie zgadza się na ich usunięcie.
4. Administrator nie potrzebuje już danych, ale są one nam niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do złożenia sprzeciwu

Ostatnim z praw jakie RODO daje osobie, której dane są przetwarzane, jest prawo do złożenia sprzeciwu w zakresie przetwarzania tych danych. Dotyczy to szczególnie sytuacji tzw. profilowania, czyli automatycznego przetwarzania danych np. na potrzeby marketingu bezpośredniego.

W sytuacji, gdy administrator stwierdzi, że sprzeciw jest niezasadny np. profilowanie jest niezbędne do realizacji umowy, będzie miał prawo do dalszego przetwarzania danych w ten sposób. W innym przypadku będzie zobowiązany do usunięcia danych.

Temat 5: Zabezpieczanie danych osobowych

Zgodnie z art. 32 RODO, administrator danych uwzględniając stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst, cele przetwarzania i ryzyko naruszenia praw lub wolności osób fizycznych, których dane przetwarza jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić odpowiedni stopień bezpieczeństwa, w tym między innymi:

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

ADO oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób.

ADO podejmuje działania w celu zapewnienia, by każda osoba działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

Analiza ryzyka

RODO zaleca administratorowi i podmiotowi przetwarzającemu dokonanie analizy ryzyka, jakie wiąże się z przetwarzaniem danych. Przeprowadzenie tego rodzaju analizy ma pozwolić na dobór odpowiednich środków technicznych i organizacyjnych pozwalających na zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych.

Zgodnie z RODO przy dokonywaniu analizy należy uwzględnić ryzyko wiążące się z przetwarzaniem danych, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Dobór odpowiednich środków technicznych i organizacyjnych

Techniczne środki bezpieczeństwa to rożnego rodzaju rozwiązania o charakterze sprzętowym oraz programowym (m.in. urządzenia, systemy, oprogramowanie), które służą

zapewnieniu odpowiedniego poziomu bezpieczeństwa danych. Mogą one mieć charakter podstawowych zabezpieczeń fizycznych (przykładowo – zamek w drzwiach, system alarmowy) bądź logicznych (na przykład oprogramowanie szyfrujące).

Jako przykłady środków technicznych RODO wskazuje pseudonimizację lub szyfrowanie danych. Ale uwaga! Wskazanie ich wcale nie oznacza obowiązku ich stosowania w każdym przypadku. Wskazanie ich w RODO oznacza jedynie na możliwość ich zastosowania – ale tylko jeśli będą one odpowiednie w konkretnym przypadku.

Oprócz środków technicznych RODO wymienia również środki organizacyjne, czyli różnego rodzaju rozwiązania odnoszące się do sposobu zorganizowania procesów przetwarzania danych. Do tego rodzaju środków zabezpieczeń można zaliczyć m.in.:

- ustalenie zasad dostępu do danych,
- reguł pobierania kluczy,
- wydzielenie stref ograniczonego dostępu osób postronnych itp.

Opis technicznych i organizacyjnych środków bezpieczeństwa danych powinien zaś stanowić element rejestru czynności przetwarzania, którego prowadzenie jest obowiązkiem administratora i podmiotu przetwarzającego.

Zabezpieczenia fizyczne chronią dane przed zagrożeniami środowiskowymi i nieupoważnionym dostępem. Ponadto należy pamiętać, że powinny tworzyć z pozostałymi zabezpieczeniami (technicznymi i organizacyjnymi) kompleksowy system ochrony danych osobowych.

Zabezpieczenia fizyczne, to środki mające na celu:

- zapewnienie odpowiedniego poziomu ochrony pomieszczeń, budynków, sprzętów, nośników informacji i elementów systemów informatycznych przed zagrożeniami środowiskowymi np. ogień, woda, pył, promieniowanie elektromagnetyczne,
- ochronę przed nieupoważnionym dostępem fizycznym, np. kradzież, włamanie.

Na zabezpieczenia fizyczne składają się:

- ochrona fizyczna – odpowiednio przygotowani do tego celu ludzie, czyli warty, patrole, portierzy,
- ochrona techniczna – na którą składają się:
- zabezpieczenia mechaniczne – szacujące czas jakiego potrzebuje intruz, aby dostać się do wnętrza chronionego pomieszczenia. W tym zakresie mamy do zastosowania drzwi, zamki, kraty, przegrody konstrukcyjne (ściany, stropy), oraz szafki, szafy pancerne, etc.,

- zabezpieczenia elektroniczne – to przede wszystkim systemy sygnalizujące o włamaniu i napadzie, monitoring wizyjny, kontrola dostępu, sygnalizacja pożaru oraz gaszenia i oddymiania.

Zabezpieczając fizycznie newralgiczne pod kątem danych osobowych pomieszczania (np. serwerownia, archiwum) należy wziąć pod uwagę m.in.:

- lokalizację,
- zastosowanie drzwi o podwyższonej odporności,
- awaryjne zasilanie,
- wyższy poziom zabezpieczeń przeciwpożarowych,
- monitoring środowiska,
- cichy alarm.

SKD – System Kontroli Dostępu

Jeśli okaże się, że chcemy wdrożyć kontrolę dostępu, musimy ustalić jaki system kontroli będzie odpowiedni dla przetwarzanych danych osobowych. W tym zakresie mamy do wyboru trzy poziomy:

- Poziom niski – bazujący na pamięci np. PIN,
- Poziom średni – bazujący na kluczach np. karta chipowa,
- Poziom wysoki – bazujący na cechach biometrycznych np. skaner siatkówki oka.

Należy jednak pamiętać, że zgodnie z art. 22 Kodeksu pracy, tzw. szczególne kategorie danych, w tym dane biometryczne (art. 9 ust. 1 RODO), mogą być przetwarzane:

- za zgodą osoby ubiegającej się o zatrudnienie bądź pracownika wyłącznie, gdy ich przekazanie następuje z inicjatywy tych osób,
- wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.

Jako podsumowanie 3 lekcji poświęconych ochronie danych osobowych proszę o zapoznanie się z poniższymi materiałami:

Strona Urzędu Ochrony Danych Osobowych – przepisy, poradniki:

https://uodo.gov.pl/

Poradnik stosowania zasad RODO:

https://lexdigital.pl/ochrona-danych-osobowych-nowe-zasady-rodo

Prezentacje multimedialne:

https://prezi.com/p/y0fwozetnvlr/ochrona-danych-osobowych/

https://prezi.com/bt30cjz1qbai/wdrozenie-systemu-ochrony-danych-osobowych/

Filmy:

https://www.youtube.com/watch?v=R_kxYrHJcrQ&feature=emb_logo

https://www.youtube.com/watch?v=7LX06VrVgRU&feature=emb_logo

https://www.youtube.com/watch?v=_tjl7pvePro&t=1s

https://www.youtube.com/watch?v=tCvq-LqWQ84