Dokumentacja medyczna i ochrona danych osobowych oraz innych informacji prawnie chronionych.

Zagadnienia do omówienia:

1. Podstawy prawne ochrony danych osobowych – ogólne i sektorowe;
2. Definicje pojęć z zakresu ODO – Administrator danych, przetwarzanie danych osobowych, dane osobowe i ich rodzaje;
3. Konsekwencje dla jednostki niewłaściwego przetwarzania danych osobowych;
4. Ryzyko w ODO;
5. Obowiązki dokumentacyjne;
6. Praktyczne wskazówki dla przetwarzających dane, najczęstsze błędy w sektorze ochrony zdrowia;
7. Odpowiedzialność i kary za niewłaściwe przetwarzanie danych osobowych;

Informacje prawnie chronione:

- Tajemnica państwowa (ściśle tajne, tajne, poufne, zastrzeżone)
- Tajemnica przedsiębiorstwa
- Tajemnica zawodowa – tajemnica obowiązująca określone grupy zawodowe
- Tajemnica pracownika
- Dane osobowe

Podstawa prawna:

1.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) – RODO

Egzekwowane od 25.05.2018 r.

2.Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r.poz. 1781).

Przykładowe przepisy sektorowe krajowe orazUnii Europejskiej regulujące ODO:

- Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j.Dz. U. z 2022 r. poz. 1876, 2280)
- Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (tj. Dz.U. 2022 poz. 1304),
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE,

Dodatkowe:

- Standardy akredytacyjne dla Szpitali
- Normy ISO

1. Podstawowe definicje

- Administrator danych osobowych

Administrator danych osobowych (ADO) to organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. Odnośnie sektora ochrony zdrowia, administratorem danych jest każdy lekarz czy też lekarz dentysta prowadzący indywidualną praktykę. W przypadku innych form prowadzonej działalności leczniczej, administratorem danych jest osoba prawna lub jednostka organizacyjna, np. przychodnia czy szpital (za wyjątkiem sytuacji, kiedy właścicielem przychodni lub szpitala jest osoba fizyczna prowadząca działalność gospodarczą). W związku z tym, iż administratora danych osobowych określa sama ustawa, **wyznaczanie ADO w jakikolwiek sposób, np. poprzez wewnętrze akty prawne (np. zarządzenie lekarza prowadzącego indywidualną praktykę, uchwały organów spółek prawa handlowego) jest niezgodne z przepisami prawa. Funkcji ADO nie można na nikogo cedować.**

Dane osobowe:

Elastyczny podział europejskich organów nadzorczych:

(belgijski organ nadzoru – Autorite de protection des donnees)

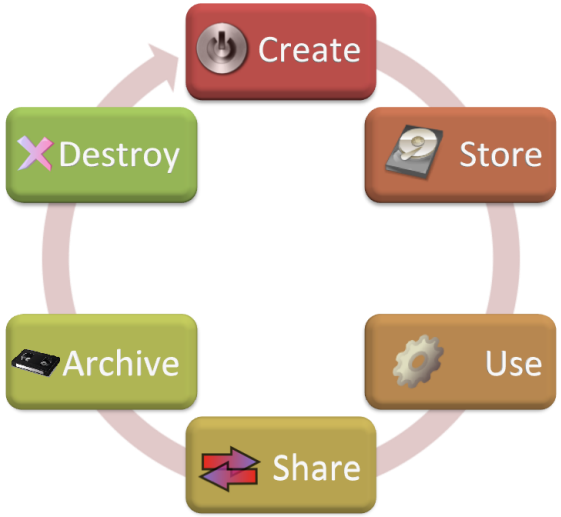
- Dane identyfikacyjne przyznane przez organy publiczne,
- Biometryczne dane identyfikacyjne,
- Wypłacalność,
- Pożyczki, hipoteki, linie kredytowe,
- Umowy oraz ugody,
- Szczegóły osobiste,
- Prywatne zwyczaje,
- Dane dotyczące podróży oraz przemieszczania się
- Szczegóły dotyczące innych członków rodziny lub domowników,
- Informacje prawne dotyczące podejrzeń,
- Poziomy uprawnień,
- Organizacja pracy,
- ……(ok.80)

Wrażliwe dane osobowe = Szczególne kategorie danych osobowych (RODO)

(obecna ustawa)

Szczególne kategorie danych osobowych:

- dane genetyczne
- dane biometryczne
- dane dotyczące zdrowia
- pochodzenie rasowe lub etniczne
- Poglądy polityczne
- Przekonania religijne lub światopoglądowe
- Seksualność, orientacja seksualna
- Przynależność do związków zawodowych



- **Przetwarzanie danych osobowych**

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

Sposoby przetwarzania – szczegółowe:

- Przegląd/odczyt
- Modyfikacja
- Drukowanie
- Eksport
- Usunięcie
- Transport
- Archiwizacja
- ….

Konsekwencje dla jednostki:

- Nadszarpnięcie reputacji
- Stres/lęk/niepewność
- Straty finansowe
- Utrata zdrowia czasowa/trwała,
- Utrata życia,
- Wstyd
- Utrata pracy
- Utrudniony rozwój zawodowy
- Przegrane procesy sądowe

Informacja to władza

Handel danymi

RODO – podejście oparte na ryzyku.

I. Brak gotowych, narzuconych rozwiązań – ADO sam ocenia ryzyko związane z przetwarzaniem danych i dobiera odpowiednie zabezpieczenia, neutralność technologiczna, inteligentny akt prawny.

II. ADO ma obowiązek rozliczalności – wykazuje organowi nadzorczemu czy dokłada odpowiedniej staranności przy przetwarzaniu danych (np. odpowiednia dokumentacja, zabezpieczenia, kultura organizacyjna, przeprowadzanie oceny skutków dla ochrony danych).

Przykłady zagrożeń:

- Kradzież nośników lub dokumentów
- Kradzież urządzenia
- Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników
- Nieautoryzowane użycie urządzeń
- Poważny wypadek – zniszczenie fizyczne
- Podsłuch/podgląd
- Zagubienie nośnika informacji

Warto wcześniej rozważyć potencjalne zagrożenia i minimalizować wystąpienie ich skutków.

Ryzyko (wielkość ryzyka) = prawdopodobieństwo wystąpienia zagrożenia/zdarzenia x skutek

Ocena ryzyka

- Bieżąca;
- Przy ocenie skutków przedsięwzięcia dla ochrony danych (DPIA);
- Przy analizie incydentów naruszenia bezpieczeństwa ochrony danych osobowych - zgłaszanie naruszeń bezpieczeństwa danych osobowych organowi nadzorczemu – ryzyko naruszenia praw i wolności osób, których dane przetwarzamy.

Kiedy wykonujemy DPIA –przykłady:

- Nowe oprogramowanie
- Zakup sprzętu medycznego (dane osobowe, medyczne, genetyczne, biometryczne)
- Monitoring wizyjny
- Umowy z podmiotami zewnętrznymi, zmiany lokalizacji komórek organizacyjnych, np. archiwum, nowe procedury wewnętrzne,

Obowiązki dokumentacyjne.

<u>Pozostaje,</u>

ponieważ RODO wymaga odpowiednich polityk,

procedur opisujących sposób przetwarzania danych:

- Polityka bezpieczeństwa danych osobowych
- Instrukcja zarządzania systemem informatycznym

<u>Dowolność w nazewnictwie</u>

- inwentaryzacja zasobów informacyjnych,
- opis przepływów danych między systemami,
- specyfikacje środków organizacyjnych i technicznych zastosowanych do ochrony przetwarzanych danych

- rejestr czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
- wytyczne dotyczące klasyfikacji naruszeń i procedurę zgłaszanie naruszenie ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO;
- procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowaniu o działaniach jakie powinni wykonać, aby ryzyko to ograniczyć – art. 34 RODO
- procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO;
- raport z przeprowadzonej, ogólnej analizy ryzyka;
- raport z ocen skutków dla ochrony danych – art. 35 ust. 7. – jeśli dotyczy;
- procedury związane z pseudonimizacją i szyfrowaniem – jeśli dotyczy;
- plan ciągłości działania – art. 32 ust 1 pkt b RODO;
- procedury odtwarzania systemu po awarii, oraz ich testowania – art. 32 ust 1 pkt c i d RODO.

Obowiązki dokumentacyjne.

- Rejestr czynności przetwarzania danych,
- Obowiązek informacyjny
- Procedura zarządzania ryzykiem w podmiocie medycznym
- Rejestr incydentów naruszenia bezpieczeństwa danych osobowych
- Procedura zgłaszania incydentów do organu nadzorczego
- Procedura DPIA
- Umowy powierzenia danych osobowych

Dokumenty specyficzne dla sektora ochrony zdrowia:

§8. 1. Oświadczenie pacjenta:

1) o wyrażeniu zgody na udzielanie informacji, o której mowa w art. 9 ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach

pacjenta i Rzeczniku Praw Pacjenta, ze wskazaniem imienia i nazwiska osoby upoważnionej oraz danych umożliwiających kontakt z tą osobą,

2) o upoważnieniu do dostępu do dokumentacji, o którym mowa w art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta,

3) o wyrażeniu zgody na udzielenie świadczeń zdrowotnych, o której mowa w art. 16–18 ustawy z dnia 6 listopada

2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta

– złożone w inny sposób niż za pośrednictwem Internetowego Konta Pacjenta, o którym mowa w art. 7a ustawy z dnia

28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, zamieszcza się w dokumentacji indywidualnej wewnętrznej.

2. Podmiot informuje pacjenta przed złożeniem przez niego oświadczeń, o których mowa w ust. 1, o możliwości ich

złożenia za pośrednictwem Internetowego Konta Pacjenta i skutkach ich złożenia.

Ważne:

Podmiot udzielający świadczeń zdrowotnych prowadzi wykaz zawierający informacje dotyczące udostępnianej dokumentacji medycznej (art.27 ust.4 UPP)

Wytyczne dla osób przetwarzających dane osobowe:

- prawidłowe prowadzenie, porządkowanie dokumentów
- należy zamykać na klucz pomieszczenia, w których znajdują się dane osobowe, jeżeli nie ma w nich osób uprawnionych do pracy z danymi,
- nie należy pozostawiać samotnie, bez nadzoru, osób nie mających uprawnień do danych osobowych w pomieszczeniach, w których te dane są przetwarzane,
- nie należy dopuszczać osób nie mających uprawnień do treści danych, udzielanie informacji w sposób ograniczony
- nie gromadzić w podręcznej dokumentacji danych osobowych; wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach; jeżeli posiadane druki lub zestawienia są niezbędne należy je zanonimizować (usunąć dane osobowe, np. adres, pesel, pozostawiając tylko nazwiska, imiona),
- dokumenty zawierające dane osobowe należy niszczyć w specjalistycznych niszczarkach,

- zbiory danych osobowych należy przechowywać wyłącznie w szafkach zamykanych na klucz, uniemożliwiając osobom nieuprawnionych wgląd do danych; jeśli jest to nie możliwie, wszelkie prace konserwacyjne i porządkowe powinny być prowadzone pod nadzorem osób upoważnionych do przetwarzania danych,
- nie pozostawiać dokumentach na parapetach, ladach itp.
- dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza jednostkę lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu,
- nie wolno przekazywać innym osobom swojego loginu i hasła, trzymać go w widocznym miejscu lub pracować na cudzym loginie i haśle

Czego absolutnie nie wolno:

- Omawiać przypadków medycznych/spraw z podaniem imienia i nazwiska osoby lub innych informacji, które umożliwią jej identyfikację (np. stanowisko służbowe) w miejscach publicznych,
- Rejestracja pacjenta – z poszanowaniem zasad ochrony danych i godności pacjenta,
- Nie udzielamy informacji jeśli nie jesteśmy w stanie zweryfikować tożsamości osoby – udzielanie informacji przez telefon – Wytyczne UODO i RzPP
- Wyrzucać do kosza na śmieci dokumentów z danymi osobowymi,
- Przetwarzać dane w osobistych urządzeniach mobilnych – np. zdjęcia dokumentacji medycznej telefonem, tabletem prywatnym, ewentualna możliwość po dokonaniu anonimizacji,

Na co uważamy:

- Wydruki, kserokopie – by nie pozostawić w urządzeniu
- Kierownicy/koordynatorzy komórek organizacyjnych:

Aktualizacja zakresów obowiązków pracowników – organ nadzorczy weryfikuje czy zakres przyznanych uprawnień do przetwarzania danych osobowych (np. w systemie informatycznym) jest adekwatny do zakresu obowiązków i zgodny z prawem (przepisami sektorowymi dot. ochrony danych osobowych), np. czy pracownik administracyjny ma prawo dostępu do dokumentacji medycznej? Na podstawie jakiego przepisu prawa?

„Szanuj dane osobowe innych ludzi tak, jak oczekiwałbyś tego w stosunku do swojej osoby.”

Obszary problemowe w ochronie zdrowia:

- Punkty rejestracji (osobista i telefoniczna rejestracja)
- Identyfikacja pacjenta
- Dostęp do dokumentacji medycznej, informacji o stanie zdrowia
- Archiwa
- Niszczenie dokumentacji
- Monitoring wizyjny
- Analizy ryzyka
- Upoważnienia do przetwarzania danych – zbyt szerokie, nieodbierane lub odbierane zbyt późno

- Wzmocnione zostają prawa jednostki, m.in.:

a. Prawo wglądu i aktualizowania danych,

b. Prawo usunięcia danych (ograniczone przepisami szczegółowymi, np. terminami przechowywania dokumentacji medycznej, pracowniczej)

c. Prawo do przenoszenia danych – tam, gdzie podstawa przetwarzania to umowa,

d. Prawo do ograniczonego przetwarzania,

- Kary administracyjne

Art. 83 ust. 5 Rozporządzenia:

„administracyjna kara pieniężna”

(…) do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (…)

Podmioty publiczne: 100 000 zł (przepisy krajowe)

- Odpowiedzialność na gruncie przepisów Kodeksu Cywilnego

GIODO zostało zastąpione Urzędem Ochrony Danych Osobowych z Prezesem na czele.

Sposób kontroli regulować będzie nowa Ustawa o ochronie danych osobowych (Rozdział 9 Ustawy):

Kontrolę może przeprowadzić:

- Pracownik UODO
- Pracownik lub członek organu nadzorczego państwa członkowskiego UE
- Postępowanie kontrolne może trwać max.30 dni
- Prezes UODO nie musi uprzednio informować o wszczęciu kontroli, stan ochrony danych może również sprawdzać przy pomocy IOD,
- Kontrola nie wyklucza jednoczesnego lub późniejszego rozpatrywania sprawy (tej lub innej) przez sąd cywilny – np. karę może nałożyć Prezes, a następnie osoba, której dane osobowe niewłaściwie przetwarzano może ubiegać się np. zadośćuczynienia w sądzie cywilnym

Inspektor ochrony danych osobowych (IOD) – funkcja doradcza i weryfikacyjna względem ADO, zatrudniany przez ADO, ale pozostający w bezpośrednim kontakcie z UODO, quasi-audytor.

Niezależny, podległy bezpośrednio najwyższemu kierownictwu.

Wymagana wiedza fachowa na temat prawa i praktyk w dziedzinie ochrony danych osobowych

Zakaz wydawania instrukcji.

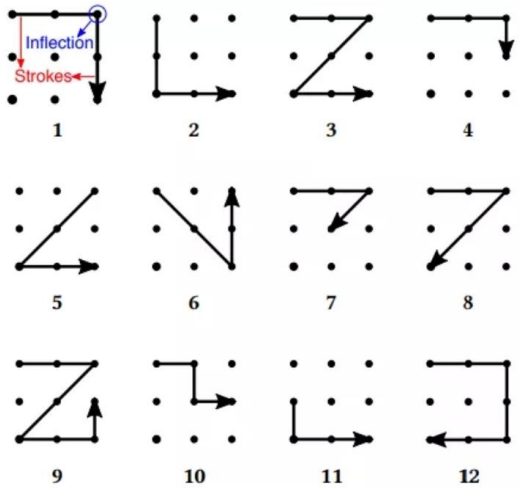
ADO gwarantuje niezależność DPO i odpowiada za to przed organem nadzorczym (kary finansowe mogą być również nałożone za niewłaściwe wykonywanie obowiązków ADO wobec IOD)

DPO stanowić ma punkt kontaktowy dla GIODO i podmiotów ochrony danych (pracowników, pacjentów, kontrahentów, innych interesariuszy).

Hasła – błędy

Polacy najczęściej stosują:

- popularne “mnemotechniczne kombinacje klawiszowe” (123456, qwerty, qaz12wsx)
- imiona (kasia, agnieszka, kasia1)
- wulgaryzmy
- hasła związane z tematyką przewodnią serwisu (jeśli to serwis o kotkach, to kotek, jeśli serwis o filmach, to film)



12 najpopularniejszych gestów, którymi blokowane są smartfony:
Grafika pochodzi z artykułu "SonarSnoop: Active Acoustic Side-Channel Attacks" (Cheng, Bagci, Roedig, Yan),
którego źródłem danych jest opracowanie "SysPal: System-guided Pattern Locks for Android" (Cho, Huh, Cho, Oh, Song, Kim).

Zasady tworzenia mocnych haseł:

- Najważniejsza jest unikalność – im bardziej unikalne hasło, tym lepiej.
- Twórz grupy haseł – tak, aby do poczty, czy konta bankowego były zupełnie różne.
- Stosuj liczby, duże i małe litery, znaki specjalne.
- Liczba znaków w haśle - minimum 8 znaków.
- Mieszaj znaki, baw się słowami – załóżmy, że lubisz kolor karmazynowy, a urodziłeś się w roku 1970. Teoretycznie hasło karmazynowy1970 wydaje się rozsądnym wyborem. Osoba chcąca złamać to hasło metodą słownikową lub brutal force, jest w stanie sobie z tym poradzić w kilka godzin. Modyfikacja kolejności słów i znaków daje o wiele lepsze efekty, w tym przypadku mogło by to być K19armazyn70owy lub 19karMaZyn70owy a jeszcze lepiej: K19arm@zyn70owy& lub 19karM@Zyn70owy! (jedno a zastępujemy @, na końcu dodajemy znak specjalny lub symbol, np.: &, § lub interpunkcyjny: !.?
- Skorzystaj z generatorów haseł, np. generator.blulink.pl, czy też dobrehaslo.pl

Źródło: Komputer Świat, Niebezpiecznik

Zasady tworzenia mocnych haseł:

- Zmieniaj hasła – przynajmniej raz do roku.
- Nigdy nie używaj w hasłach słów związanych z Twoim otoczeniem. Niestety hasło w oparciu o nazwę Twojego pupila, monitora, lub ulubionego zespołu piłkarskiego, ulubionej marki to zły pomysł.
- Stosuj proste algorytmy. Np. Lubię Paryż a *najlepsze kasztany są na Placu Pigall*. Hasło weź z pierwszych liter czyli Lpanksnpp, a następnie dodaj do hasła liczbę i znak specjalny, np.: L37panksnpp$.
- Jeśli masz problem z zapamiętywaniem – Możesz hasło zapisać, ale w formie zmodyfikowanej - Odejmuj lub dodawaj losowo 3,4 znaki, których nigdy nie używasz:

Hasło: K19armazyn70owy

Jeśli zapiszesz je w tej formie – każda osoba, która je znajdzie, po prostu je przepisze. Ustal jednak, że 3 znaków nigdy nie używasz w swoich hasłach. Niech to będzie 0ow (ze względu na łatwość zapamiętania skrótu, choć równie dobrze może to być dowolna inna zbitka znaków). Zapisując hasło, zanotuj: K19armazyn70owy . Ale realne hasło już przy logowaniu się do jakiegoś serwisu powinno brzmieć K19armazyn7y

Źródło: Komputer Świat, Niebezpiecznik

Dziękuję za uwagę

Agnieszka Witoszek