GDPR

(GENERAL DATA PROTECTION REGULATION – OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH)

na Uniwersytecie Warszawskim

UNIWERSYTET WARSZAWSKI

Opracował: Dominik Ferenc
Administrator Bezpieczeństwa Informacji

Warszawa 2018 r.

Spis treści

1. Co to jest GDPR/RODO?

GDPR/RODO to skrót od Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych/General Data Protection Regulation).

GDPR stanowi główny element europejskiej reformy ochrony danych osobowych. Głównym celem ogólnego rozporządzenia o ochronie danych osobowych jest ujednolicenie przepisów regulujących ochronę danych osobowych w państwach UE, a także unormowanie sposobu przepływu danych między tymi państwami. GDPR jest aktem, który w sposób kompleksowy reguluje kwestie dotyczące ochrony danych osobowych i nie wymaga implementacji do krajowego systemu prawnego, oznacza to, że przepisy GDPR stosowane są wprost.

Na pakiet regulujący ochronę danych osobowych składa się także tzw. dyrektywa policyjna (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r.) oraz będąca w fazie prac legislacyjnych dyrektywa o e-prywatności.

Na gruncie prawa krajowego aktem prawnym, który wypracowuje mechanizm spójności stosowania przepisów GDPR, będzie nowa ustawa o ochronie danych osobowych.

Materiały:

- oficjalny tekst GDPR:

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679

2. Kto jest Administratorem danych przetwarzanych na UW?

Administratorem danych przetwarzanych na Uniwersytecie Warszawskim jest Uniwersytet Warszawski reprezentowany przez Jego Magnificencję Rektora, z siedzibą przy ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa.

Administrator danych ustala cele i sposoby przetwarzania danych osobowych, a także zobowiązany jest – uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – wdrożyć odpowiednie środki techniczne i organizacyjne, by przetwarzanie danych osobowych odbywało się zgodnie z GDPR.

3. Kto to jest Inspektor Ochrony Danych (IOD)?

Inspektor Ochrony Danych to wyznaczona przez Rektora Uniwersytetu Warszawskiego osoba, która jest odpowiedzialna za nadzór i bezpieczeństwo danych osobowych przetwarzanych na Uniwersytecie Warszawskim.

Inspektor Ochrony Danych odpowiada za nadzór nad funkcjonowaniem i efektywnością procesów prawidłowego przetwarzania danych osobowych.

Szczegółowy zakres zadań IOD określa zarządzenie nr 51 Rektora UW z dnia 15 maja 2018 r. w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim (Monitor UW z 2018 r. poz. 142).

4. Kto to jest Lokalny pełnomocnik ds. ochrony danych osobowych (LODO)?

To wyznaczona przez kierownika jednostki organizacyjnej lub kierownika jednostki administracji centralnej osoba, której zadaniem jest wspieranie IOD w nadzorowaniu zasad ochrony danych osobowych oraz podnoszenie poziomu ochrony danych osobowych w danym obszarze merytorycznym.

Pełen zakres zadań i obowiązków LODO opisuje Polityka ochrony danych osobowych na Uniwersytecie Warszawskim stanowiąca załącznik nr 1 do zarządzenia nr 51 Rektora UW z dnia 15 maja 2018 r. w sprawie ochrony danych osobowych na Uniwersytecie Warszawskim (Monitor UW z 2018 r. poz. 142).

5. Co to są dane osobowe?

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

Dane osobowe to wszystkie dane, które dotyczą konkretnej osoby fizycznej – od imienia i nazwiska, nr PESEL umieszczonego w dokumencie tożsamości, przez adres e-mail do danych umieszczonych na wizytówce. Danymi osobowymi może być także odcisk palca, adres IP, login do portalu internetowego czy numer telefonu.

6. Co to są szczególne kategorie danych osobowych?

Szczególne kategorie danych osobowych to grupa danych sensytywnych (wrażliwych), które podlegają szczególnym zasadom przetwarzania i ochrony. Są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane: genetyczne, biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Przetwarzanie szczególnych kategorii danych osobowych jest zabronione, chyba, że zachodzi jedna z przesłanek wynikających z art. 9 GDPR, m.in.:

- zgoda osoby, której dane dotyczą;
- gdy przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw administratora lub osoby, której dane dotyczą, **w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej**;
- gdy przetwarzanie jest konieczne do **ochrony żywotnych interesów osoby,** której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

- gdy przetwarzanie dotyczy danych osobowych w sposób oczywisty **upublicznionych** przez osobę, której dane dotyczą;
- gdy przetwarzanie jest niezbędne do celów **profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej,** zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego;
- gdy przetwarzanie jest niezbędne do celów **archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.**

Szczególne kategorie danych osobowych przetwarzane na Uniwersytecie Warszawskim są między innymi w: badaniach naukowych, projektach czy w celu zapewnienia równych szans osobom niepełnosprawnym.

7. Jak wiele danych można zbierać zgodnie z GDPR?

GDPR wprowadza tzw. zasadę minimalizacji danych osobowych. Zgodnie z tą zasadą można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych. Zgodnie z zasadą minimalizacji danych należy ograniczyć zbieranie danych tylko do tych, bez których nie można osiągnąć celu przetwarzania. Zabronione jest zbieranie w sposób nadmiarowy.

8. Co to jest przetwarzanie danych osobowych?

Przetwarzanie danych osobowych to operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

Katalog czynności, które mogą składać się na przetwarzanie danych osobowych, ma charakter przykładowy – należy przyjąć, iż przetwarzanie danych osobowych to każda czynność, którą wykonujemy z wykorzystaniem danych osobowych.

9. Kto może przetwarzać dane osobowe na UW?

Do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych.

Upoważnienie do przetwarzania danych osobowych służy realizacji obowiązku rozliczalności wynikającego z GDPR, tzn. Uniwersytet Warszawski musi wykazać, iż do przetwarzania danych osobowych zostały dopuszczone tylko osoby uprawnione. Upoważnienie jest także dokumentem, który ogranicza dostęp do zasobów danych przez osoby nieuprawnione.

Przykład:

Upoważnienie do przetwarzania danych osobowych powinno być wydane dla osób, które przetwarzają dane np.:

- kandydatów na studia (system IRK),
- studentów (system USOS),
- pracowników (system SAP).

Obowiązek posiadania upoważnienia dotyczy także sytuacji, w której dane przetwarzane są w wersji papierowej.

10. Co to jest rejestr czynności przetwarzania?

Rejestr czynności przetwarzania to dokument, który pokazuje, w jakich procesach Uniwersytet Warszawski przetwarza dane osobowe.

Rejestr uwzględnienia m.in. cel przetwarzania danych, podstawy przetwarzania danych, kategorię oraz zakres przetwarzanych danych oraz w jaki sposób dane są zabezpieczone.

Rejestr czynności przetwarzania może być prowadzony w wersji papierowej lub elektronicznej.

Należy zauważyć, iż pojęcie czynności przetwarzania danych osobowych nie zostało precyzyjnie opisane w RODO, co może powodować trudności w zidentyfikowaniu czynności przetwarzania danych osobowych. Czynność przetwarzania można określić przez kategorie podmiotów danych lub celów przetwarzania.

11. Jakie operacje przetwarzania danych osobowych zachodzą na UW?

Uniwersytet Warszawski przetwarza dane osobowe w procesach dotyczących m.in.:

- działalności dydaktycznej (rekrutacja na studia, kształcenie studentów – wszystkie stopnie), kształcenie ustawiczne (kursy, studia podyplomowe, uniwersytet otwarty), kształcenie kadry naukowej),
- zarządzania zasobami ludzkimi (rekrutacja do pracy, zatrudnienie, obsługa kadrowa, działalność socjalna, bezpieczeństwo i higiena pracy),
- działalności naukowo-badawczej (badania naukowe, współpraca naukowa),
- działalności na rzecz studentów (pomoc materialna oraz ubezpieczenia studentów i doktorantów, stypendia naukowe, prowadzenie domów studenckich),
- obsługi finansowo-księgowej (rachunkowość, rozrachunki z pracownikami, kontrahentami),
- innych obszarów działalności (wolontariat, biblioteki, działania marketingowe, reklamowe, promocyjne, sklep internetowy, korespondencja przychodząca i wychodząca).

12. Czyje dane przetwarzane są na Uniwersytecie Warszawskim?

Uniwersytet Warszawski przetwarza m.in. dane:

- pracowników uczelni i ich rodzin,
- kandydatów na określone funkcje,
- studentów, doktorantów, słuchaczy studiów podyplomowych oraz osób ubiegających się o przyjęcie na studia, studia doktoranckie lub studia podyplomowe,

- osób, które uzyskały stopień naukowy doktora lub doktora habilitowanego;
- cudzoziemców podejmujących i odbywających studia, studia doktoranckie i inne formy kształcenia, a także uczestniczące w badaniach naukowych lub pracach rozwojowych;
- studentów i doktorantów, w tym cudzoziemców ubiegających się o stypendia lub świadczenia z zakresu pomocy materialnej;
- czytelników bibliotek;
- osób biorących udział w postępowaniach konkursowych;
- uczestników badań naukowych;
- uczestników konferencji, projektów, seminariów;
- absolwentów.

13. Jaki zakres danych przetwarzany jest na Uniwersytecie Warszawskim?

Uniwersytet Warszawski przetwarza dane między innymi w zakresie:

- imion i nazwisk;
- dat urodzenia;
- numeru PESEL;
- numeru indeksu;
- serii i numeru dokumentu potwierdzającego tożsamość;
- adresu e-mail;
- numeru telefonu;
- wizerunku;
- obywatelstwa.

W zakresie danych osobowych przetwarzanych przez Uniwersytet Warszawski występują także szczególne kategorie danych o:

- stanie zdrowia, stopniu niepełnosprawności;
- pochodzeniu rasowym lub etnicznym;
- przynależności do związków zawodowych.

14. Gdzie na Uniwersytecie Warszawskim przetwarzane są dane osobowe?

Dane osobowe przetwarzane są w:

systemach informatycznych: IRK, USOS, SAP, HMS, systemy biblioteczne;

pakietach biurowych np.: MS World, MS Excel;

systemach pocztowych np.: MS Outlook, Mozilla Thunderbird;

zbiory tradycyjne (papierowe) np.: akta pracownicze, akta studenckie, teczki osobowe, korespondencja papierowa itp.

15. W jakim celu UW przetwarza dane osobowe?

Uniwersytet Warszawski przetwarza dane osobowe m.in. w celach:

- przyjęcia kandydatów na studia;
- przyjęcia kandydatów do pracy;
- realizacji procesu dydaktycznego;
- obsługi czytelników bibliotek;
- zatrudnienia pracownika;
- zawierania umów cywilnoprawnych;
- prowadzenia dokumentacji kadrowej;
- prowadzenia spraw bytowo-socjalnych studentów i pracowników;
- nadzoru nad przestrzeganiem zasad bezpieczeństwa i higieny pracy;
- realizacji projektów badawczych;
- przyznawania stypendiów;
- przydziału miejsc w domach studenckich;
- inicjowania i wspierania różnych form działań wolontariackich;
- działań marketingowych, zarządzania ofertą: edukacyjną, naukową, usługową, działalność promocyjna;
- obsługi i realizacji konkursów/konferencji itp.

16. Jak długo można przechowywać dane osobowe?

GDPR wprowadza zasadę ograniczenia czasowego przechowywania danych osobowych, tzn. że dane nie powinny być przechowywane w nieskończoność.

Jeżeli podstawę przetwarzania danych osobowych stanowi zgoda osoby, której dane dotyczą, wówczas dane osobowe mogą być przetwarzane do czasu odwołania zgody. Po odwołaniu zgody, dane mogą być przetwarzane przez okres odpowiadający ew. terminowi przedawnienia roszczeń, jakie może ponosić administrator danych.

Jeżeli dane przetwarzane są na podstawie umowy, wówczas mogą być przetwarzane tak długo, jak jest to niezbędne do wykonania umowy, a po tym czasie przez okres odpowiadający okresowi przedawnienia roszczeń.

Jeżeli przepisy określają termin, przez jaki powinny być przechowywane dane osobowe, to należy przechowywać je przez czas wskazany w konkretnym przepisie.

Przykład:

Uczelnia przechowuje przez okres 6 miesięcy kopie dokumentów **kandydatów nieprzyjętych na pierwszy rok studiów** wraz z kopią pisma, na podstawie którego zwrócono kandydatowi złożone oryginały dokumentów (§ 19 ust. 2 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 16 września 2016 r. w sprawie dokumentacji przebiegu studiów).

Teczkę akt osobowych **studenta** przechowuje się w archiwum uczelni przez okres 50 lat (§ 4 ust. 2 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 16 września 2016 r. w sprawie dokumentacji przebiegu studiów).

Dokumentację **pracowniczą** przechowuje się przez okres 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł (art. 94 pkt 9b ustawy z dnia 26 czerwca 1974 r. Kodeks pracy)

17. Czy UW udostępnia dane osobowe?

Udostępnianie danych osobowych to jedna z form operacji wykonywanych na danych osobowych w ramach przetwarzania tych danych. Uniwersytet Warszawski, administrując danymi, może udostępniać je osobom lub podmiotom uprawnionym do ich otrzymania na podstawie przepisów prawa (organy administracji państwowej, wymiaru sprawiedliwości) lub innym podmiotom w przypadku posiadania przez te podmioty podstaw prawnych do legalnego przetwarzania danych.

Uniwersytet Warszawski udostępnia dane osobowe m.in.:

- zgodnie z ustawą Prawo o szkolnictwie wyższym Ministerstwu Nauki i Szkolnictwa Wyższego;
- ZUS w celu potwierdzenia statusu studenta;
- potencjalnym pracodawcom na podstawie zgody absolwenta.

18. Czy Uniwersytet Warszawski powierza dane osobowe?

Powierzenie przetwarzania danych osobowych zachodzi wtedy, gdy Uniwersytet Warszawski, administrując danymi, korzysta z usług podmiotów zewnętrznych zwanych procesorami, w zakresie realizacji zadań związanych z przetwarzaniem danych osobowych. Powierzenie przetwarzania danych obywa się na podstawie umowy lub innych instrumentów prawnych. Umowa powierzenia musi określać cele i kategorie powierzanych danych osobowych. Retencja danych osobowych odbywa się co do zasady przez okres obowiązywania umowy. Umowa powierzenia może mieć postać samodzielnej umowy bądź dodatkowych postanowień do umów o świadczenie usług. Treść umowy powierzenia należy konsultować z Inspektorem Ochrony Danych.

Uniwersytet Warszawski powierza dane osobowe m.in.:

- w uzasadnionych przypadkach korzystając z miejsc na serwerach firm zewnętrznych;
- innym uczelniom np. zagranicznym.

19. Na jakich podstawach Uniwersytet Warszawski przetwarza dane osobowe?

Podstawy do legalnego przetwarzania danych osobowych określa art. 6 GDOR. Z punktu widzenia przepisu przetwarzanie jest dopuszczalne, gdy:

- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie jej danych osobowych;
- 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.

Wybrane podstawy przetwarzania danych osobowych na Uniwersytecie Warszawskim:

- **zgoda osoby, której dane dotyczą** – ma zastosowanie np. w przypadkach osób chcących wziąć udział w konkursie, badaniach naukowych itp., absolwentów (zgoda na monitoring karier zawodowych absolwentów), udostępnianie danych na wniosek osób trzecich np. potencjalnego pracodawcy, w celu weryfikacji wykształcenia;
- **przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze** – ustawa Prawo o szkolnictwie wyższym, rozporządzenia wykonawcze do ww. ustawy, ustawa Kodeks pracy, ustawa o bibliotekach, ustawa o narodowym zasobie archiwalnym i archiwach.

Uniwersytet Warszawski może przetwarzać dane osobowe na podstawie zgody osoby, której dane dotyczą, lub przesłanki wynikającej z przepisu prawa, np. przetwarzanie danych osobowych studentów odbywa się na podstawie ustawy Prawo o szkolnictwie wyższym, przetwarzanie danych osobowych pracowników odbywa się na podstawie ustawy Kodeks pracy, dane kandydatów do pracy przetwarza się na podstawie zgody kandydata.

20. Kiedy jednostki organizacyjne Uniwersytetu Warszawskiego powinny spełniać obowiązek informacyjny?

Obowiązek informacyjny to obowiązek Administratora do poinformowania osoby, której dane dotyczą o:

- danych identyfikujących Administratora;
- danych kontaktowych Inspektora Ochrony Danych (obecnie ABI);
- przysługujących jej prawach;
- celu przetwarzania danych osobowych;
- okresie przechowywania danych osobowych;
- podstawie przetwarzania danych osobowych;
- możliwości złożenia skargi do organu nadzorczego (obecnie GIODO).

Obowiązek informacyjny ma na celu uświadomić osobę, której dane dotyczą, o tym na co się godzi, wyrażając zgodę na przetwarzanie swoich danych osobowych lub gdy przetwarzanie danych odbywa się na podstawie innych przesłanek o przysługujących osobie, której dane

dotyczą, prawach. Obowiązek ten jest realizowany najczęściej w postaci klauzul informacyjnych. Obowiązek informacyjny należy spełnić niezależnie od podstawy przetwarzania danych osobowych.

Kiedy spełniać obowiązek informacyjny?

Obowiązek informacyjny należy spełnić podczas pozyskiwania danych od osoby, której dane dotyczą, np.: w procesie rekrutacji na studia/do pracy, zapisu uczestników na organizowane wydarzenie, w procesie dotyczącym prowadzenia badań naukowych.

Najbezpieczniejszym rozwiązaniem jest umieszczanie klauzul informacyjnych tam, gdzie przetwarzamy dane osobowe.

21. Kiedy na UW powinniśmy pozyskiwać zgodę na przetwarzanie danych osobowych?

Zgoda na przetwarzanie danych osobowych to jedna z przesłanek legalności przetwarzania danych osobowych, rozumiana jako okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalającego na przetwarzanie dotyczących jej danych osobowych. Zgoda na przetwarzanie danych osobowych musi być: dobrowolna, konkretna, świadoma i jednoznaczna.

Zgoda na przetwarzanie danych osobowych może przyjąć formę oświadczenia woli, wyrażonego w formie pisemnej lub elektronicznej, np. klauzula zgody dołączona do kwestionariusza osobowego w formie papierowej lub umieszczenie klauzuli zgody w formularzu elektronicznym przy zastosowaniu checkboxa.

Zgoda na przetwarzanie danych osobowych musi być wyrażona na jasno określony cel np. zgoda na przetwarzanie danych osobowych w procesie rekrutacji do pracy czy udziału w konkursie, konferencji itp.

Na Uniwersytecie Warszawskim na podstawie zgody przetwarzane są m.in. dane następujących kategorii osób:

- kandydatów do pracy;
- absolwentów;
- uczestników badań/projektów;
- uczestników konferencji/szkoleń/seminariów.

Jeżeli dane osobowe przetwarzane są na podstawie zgody, osoba, której dane dotyczą, **ma prawo w dowolnym momencie wycofać zgodę**. Wycofanie zgody ma być równie proste do realizacji jak jej wyrażenie.

22. Kiedy na Uniwersytecie Warszawskim może dojść do naruszenia ochrony danych osobowych?

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Przykładami naruszeń mogą być:

- zagrożenia w obszarze zasobów ludzkich (ujawnianie danych osobom nieuprawnionym);
- zjawiska naturalne (zjawiska klimatyczne, sejsmiczne, pogodowe);
- utrata podstawowych usług;
- zniszczenia fizyczne (pożar, zalanie, wypadek, zniszczenie urządzeń lub nośników);
- awarie techniczne;
- nieautoryzowane zmiany, nielegalne wykorzystywanie lub nadużywanie zasobów IT;
- infekcja systemu przez szkodliwe oprogramowanie;
- ataki hakerskie;
- fałszywe wiadomości e-mail;
- naruszenia podstaw przetwarzania danych osobowych;
- włamania, wtargnięcia lub inne nieuprawnione wejście na teren Uczelni.

23. Co należy zrobić w przypadku podejrzenia/stwierdzenia naruszenia ochrony danych osobowych?

W przypadku podejrzenia/stwierdzenia naruszenia ochrony danych osobowych należy zaprzestać przetwarzanie danych osobowych, poinformować bezpośredniego przełożonego oraz IOD o możliwym naruszeniu ochrony danych osobowych.

W zgłoszeniu podejrzenia/stwierdzenia naruszenia należy wskazać:

- datę zdarzenia,
- opis zaistniałego incydentu,
- miejsce wystąpienia incydentu,
- wskazać przyczynę lub potencjalną przyczynę wystąpienia naruszenia,
- ustalić możliwe skutki wynikające z naruszenia,
- opisać dotychczasowe działania w związku z incydentem,
- opisać znane danej osobie sposoby zabezpieczenia danych osobowych.

24. Czym jest ochrona danych osobowych w fazie projektowania (privacy by design)?

Uwzględnianie ochrony danych w fazie projektowania to działanie, którego celem jest włączenie ochrony prywatności już na etapie zidentyfikowania czynności przetwarzania. To podejście, które mówi, iż ochrona danych powinna być wbudowana w każdy nowy projekt, przy zastosowaniu odpowiednich środków technicznych i organizacyjnych. Ochrona danych osobowych w fazie projektowania oznacza:

- proaktywne podejście do ochrony danych osobowych,
- włączenie ochrony danych osobowych w projekt od początku jego realizacji,
- poszanowanie prywatności osób, których dane dotyczą.

25. Czym jest domyślna ochrona danych osobowych (privacy by default)?

Domyślna ochrona danych to uwzględnienie jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu informatycznego. Domyślnie, czyli bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą. Domyślnie należy przetwarzać tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane.

26. Co to jest ocena skutków dla ochrony danych osobowych?

Ocena skutków dla ochrony danych osobowych to proces, który ma opisać przetwarzanie danych osobowych, ocenić niezbędność i proporcjonalność przetwarzania danych oraz pomóc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych.

Ocena skutków dla ochrony danych osobowych pozwala na podjęcie właściwych środków technicznych i organizacyjnych mających służyć zabezpieczeniu danych osobowych, a także wskazuje jakie czynności należy podjąć, by zminimalizować ryzyko przetwarzania danych osobowych.

27. Jakie techniczne i organizacyjne zabezpieczenia danych osobowych są stosowane na UW?

Na Uniwersytecie Warszawskim stosuje się m.in.:

Zabezpieczenia organizacyjne:

- wyznaczenie inspektora ochrony danych (obecnie ABI);
- opracowanie i wdrożenie dokumentacji ochrony danych osobowych;
- do przetwarzania danych osobowych dopuszczone zostały osoby do tego upoważnione;
- prowadzenie ewidencji osób upoważnionych;
- przeszkolenie i zaznajomienie pracowników z przepisami ochrony danych osobowych;
- procedura wydawania kluczy do pomieszczeń osobom uprawnionym;
- nadzór obszarów przez służbę ochrony;
- portiernie monitorujące osoby wchodzące i wychodzące z budynków;
- osoby trzecie w obszarze przetwarzania danych osobowych przebywają w obecności osób upoważnionych;
- osoby upoważnione zobowiązane są do zachowania danych osobowych i sposobów zabezpieczeń w tajemnicy.

Środki ochrony fizycznej:

- drzwi zamykane na klucz;
- drzwi o podwyższonej odporności na włamanie;
- okna zabezpieczone za pomocą krat/rolet;
- systemy alarmowe;
- systemy monitoringu wizyjnego;

- systemy przeciwpożarowe;
- szafy niemetalowe/metalowe zamykane na klucz;
- sejfy, kasy pancerne;
- niszczarki dokumentów.

Środki ochrony w ramach narzędzi programowych:

- rejestracja zmian w systemach;
- określenie praw dostępu do danych;
- identyfikatory użytkowników oraz hasła;
- token.