OCHRONA DANYCH OSOBOWYCH

SZKOLENIE DLA PRACOWNIKÓW POWIŚLAŃSKIEJ SZKOŁY WYŻSZEJ

Podstawowe akty prawne dotyczące ochrony danych osobowych

- 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) zwane „RODO”;
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000);
- Ustawa dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. z 2019 r. poz.730)

Polityka ochrony danych osobowych

Zarządzeniem Rektora Nr 13/10/20 z dnia 31 października 2020 r. w Powiślańskiej Szkole Wyższej została wprowadzona Polityka Ochrony Danych Osobowych.

Polityka Ochrony Danych Osobowych określa zasady przetwarzania oraz zabezpieczenia danych osobowych w Uczelni w celu zapewnienia zgodności przetwarzania z wymaganiami RODO oraz przepisami obowiązującego prawa w zakresie przetwarzania danych osobowych.

Procedura nadawania upoważnień do przetwarzania danych osobowych

Zasady nadawania upoważnień do przetwarzania danych osobowych zostały uregulowane w Procedurze nadawania upoważnień do przetwarzania danych osobowych w Powiślańskiej Szkole Wyższej Zarządzenie Rektora Nr 13/10/20 z dnia 31 października 2020 r. z późn. zmianami.

Źródła informacji o ochronie danych osobowych

Powiślańska Szkoła Wyższa zamieszcza na stronie internetowej treść aktów prawnych oraz zarządzeń wewnętrznych dotyczących ochrony danych osobowych.

Zakładka Inspektora Ochrony Danych jest aktualizowana na bieżąco i uzupełniana o praktyczne porady i wskazówki dot. stosowania przepisów prawa dotyczącego ochrony danych osobowych .

Cennym źródłem informacji i interpretacji przepisów o ochronie danych osobowych jest również strona internetowa Urzędu Ochrony Danych Osobowych https://uodo.gov.pl/

Pojęcie danych osobowych

Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny Pesel, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

DANE OSOBOWE-DEFINICJE

DANE OSOBY FIZYCZNEJ UMOŻLIWIAJĄCE JEJ BEZPOŚREDNIĄ LUB POŚREDNIĄ IDENTYFIKACJĘ W SZCZEGÓLNOŚCI:

- 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.

DANE OSOBOWE-DEFINICJE

Na dane osobowe składają się informacje takie jak:

- Komunikaty (niezależnie od sposobu utrwalenia)
- litery, słowa, dźwięki, fotografie, zdjęcia rentgenowskie, DNA…

DANE OSOBOWE-DEFINICJE

DANE SZCZEGÓLNEJ KATEGORII-DANE WRAŻLIWE

- Dane dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych i światopoglądowych, przynależności do związków zawodowych, seksualności lub orientacji seksualnej.
- Dane biometryczne
- Dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane DNA

Podstawowe zasady ochrony danych osobowych

RODO wprowadza obowiązek przestrzegania zasad ochrony danych osobowych.

Podstawowe zasady dot. danych osobowych stanowią, że dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość);
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu);
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);

Podstawowe zasady ochrony danych cd.

- prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (prawidłowość);
- przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (ograniczenie przechowywania)
- 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).

DANE OSOBOWE-PRZETWARZANIE

Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

Przetwarzanie	Zbieranie	Utrwalanie	Organizowanie
Porządkowanie	Przechowywanie	Adaptowanie lub modyfikowanie	Pobieranie
Przeglądanie	Wykorzystywanie	Ujawnianie poprzez przesłanie	Rozpowszechnianie lub innego rodzaju udostępnianie
Dopasowywanie lub łączenie	Ograniczanie	Usuwanie	Niszczenie

Legalność przetwarzania danych osobowych

Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie wtedy, gdy został spełniony co najmniej jeden z następujacych warunków:

- osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie(art. 6 ust.1a RODO)
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub jest konieczne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust.1 b RODO),
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze(art. 6 ust.1 c RODO),

Legalność przetwarzania danych osobowych cd.

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej (art. 6 ust.1 d RODO),
- przetwarzanie jest niezbędne do wykonywania zadania realizowanego w interesie publicznym (art. 6 ust.1 e RODO),
- 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 prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem. Na przesłankę prawnie uzasadnionego interesu realizowanego przez administratora lub osobę trzecią nie mogą się powołać organy publiczne w ramach wykonywania swoich zadań (art.6 ust.1 f RODO).

Legalność przetwarzania danych osobowych cd.

Każda z wyżej wymienionych przesłanek ma charakter autonomiczny i może stanowić samodzielną podstawę przetwarzania danych osobowych.

W Powiślańskiej Szkole Wyższej najczęściej przetwarzanie danych odbywa się na podstawie przepisów prawa. W takiej sytuacji nie ma konieczności wyrażenia zgody przez osobę, której dane dotyczą.

O zgodę na przetwarzanie danych osobowych należy prosić jedynie wtedy, gdy nie istnieją inne przesłanki przetwarzania danych.

Zgoda jako podstawa przetwarzania danych osobowych

Zgoda osoby, której dane dotyczą jest to dobrowolne, konkretne, świadome oraz jednoznaczne okazanie woli, które składa osoba, której dane dotyczą w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwolenie na przetwarzanie dotyczących jej danych osobowych.

Przetwarzanie danych osobowych na podstawie zgody

Jeżeli przetwarzanie danych odbywa się na podstawie zgody Powiślańska Szkoła Wyższa musi być w stanie wykazać, że osoba, której dane dotyczą, a w przypadku osób niepełnoletnich – jej opiekun prawny, wyraziła zgodę na przetwarzanie swoich danych osobowych.

Jeżeli zgoda zawarta jest w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w taki sposób aby można wyraźnie go odróżnić od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, przekazane jasnym i prostym językiem.

DANE OSOBOWE-KOMPETENCJE

ADMINISTRATOR DANYCH

Decyduje o celach i środkach przetwarzania danych osobowych.

INSPEKTOR OCHRONY DANYCH

Nadzoruje system ochrony danych współdziała z Urzędem Ochrony Danych Osobowych.

UPOWAŻNIONY PRACOWNIK

Przetwarza dane w zakresie niezbędnym do wykonania swoich obowiązków zgodnie z zasadami przetwarzania danych.

Administrator danych

Zgodnie z definicja zawartą w RODO, administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania

Obowiązki Administratora Danych

Do obowiązków Administratora Danych należy:

- wypełnienie względem osób, których dane dotyczą obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO,
- zabezpieczenie przetwarzanych danych osobowych przez zastosowanie odpowiednich środków technicznych i organizacyjnych, tak aby dane te nie były udostępniane osobom nieupoważnionym oraz były chronione przed zniszczeniem albo utratą (np. poprzez szyfrowanie danych, pseudonimizację, zapewnienie integralności i poufności danych),
- przestrzeganie praw osób, których dane są przetwarzane, tzn. udzielanie informacji co do celów, sposobów, źródeł, zakresu przetwarzania danych osobowych, spełniania żądań osób w zakresie sprostowania, uaktualnienia albo uzupełnienia bądź czasowego wstrzymania ich przetwarzania,
- wyznaczenie inspektora ochrony danych, opublikowanie jego danych w tym danych do kontaktu, powiadomienie o jego powołaniu organ nadzorczy, czyli Prezesa UODO.

- **Administrator danych osobowych (ADO) - zadania**
- Do podstawowych zadań przedsiębiorcy, jako administratora danych można zaliczyć m.in:

- stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
- prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz środków zapewniających ochronę danych osobowych;

- Ponadto jednym z najważniejszych zadań, które może wykonywać **administrator danych osobowych** jest powołanie Inspektora Ochrony Danych Osobowych (IODO) - jeśli przepisy go do tego zobowiązują. IOD musi powołać
- Do wyznaczenia IOD zobowiązane są podmioty publiczne, podmioty przetwarzające na dużą skalę dane wrażliwe oraz podmioty, których główna działalność polega na monitorowaniu osób na dużą skalę. Pozostałe podmioty również mogą wyznaczyć IOD, jednak nie jest to dla nich obowiązkowe. Jednak jeśli mimo braku takiego obowiązku, wyznaczą one IOD, to powinny postępować zgodnie wymaganiami dla niego (odnośnie do zadań, roli inspektora).

Inspektor ochrony danych

- **Inspektor Ochrony Danych Osobowych** to osoba powoływana przez administratora lub podmiot przetwarzający do pomocy przy przestrzeganiu w firmie lub organizacji przepisów o ochronie danych osobowych. IOD pełni rolę pośrednika pomiędzy zainteresowanymi podmiotami (Urzędem Ochrony Danych Osobowych, podmiotem przetwarzającym dane oraz osobą, której dane są przetwarzane). Ponadto **Inspektor Ochrony Danych Osobowych** zapewnia realizację zasady rozliczalności - pomaga przy sporządzaniu oceny ryzyka, czy oceny skutku ochrony danych osobowych.

- Na podstawie art. 39 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) dalej RODO Inspektor ochrony danych ma następujące zadania:

a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich
o ochronie danych i doradzanie im w tej sprawie;

b. monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d. współpraca z organem nadzorczym;

e. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

- Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Wycofanie zgody na przetwarzanie danych osobowych

Udzielona zgoda na przetwarzanie danych osobowych może być w dowolnym momencie wycofana. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Należy bezwzględnie poinformować osobę, której dane dotyczą, o możliwości wycofania zgody zanim wyrazi zgodę.

Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

Bezpieczeństwo danych

Jednym z podstawowych obowiązków Powiślańskiej Szkoły Wyższej wynikającym z RODO jest prawidłowe zabezpieczenie danych osobowych.

Powiślańska Szkoła Wyższa zobowiązana jest, zgodnie z art. 32 RODO, przy uwzględnieniu różnych czynników o charakterze technicznym oraz organizacyjnym, zapewnić należyte bezpieczeństwo przetwarzanych danych.

Podstawy prawne przetwarzania danych w Powiślańskiej Szkole Wyższej

Podstawowymi aktami prawnymi, w oparciu o które przetwarzane są dane osobowe w Powiślańskiej Szkole Wyższej są w szczególności:

- Ustawa Prawo o szkolnictwie wyższym i nauce
- Ustawa Kodeks pracy
- Ustawa o systemie ubezpieczeń społecznych
- Ustawa o rachunkowości
- Ustawa o podatku dochodowych od osób fizycznych

DANE OSOBOWE-DEFINICJE

PSEUDONIMIZACJA

Pseudonimizacja jest działaniem odwracalnym, które polega na utajnieniu tożsamości, np. poprzez zaszyfrowanie danych przy pomocy określonego klucza. Zakłada możliwość reidentyfikacji danych osobowych, dlatego właśnie dane spseudonimizowane uważane są za dane osobowe na gruncie RODO.

DANE OSOBOWE-DEFINICJE

ANONIMIZACJA

Proces nieodwracalny polegający na pozbawieniu danych cech identyfikacyjnych.

Na podstawie danych zanonimizowanych w ogóle nie można zidentyfikować osób fizycznych których pierwotnie dotyczyły.

Dane przekazywane innym jednostkom do celów naukowo badawczych poddaje się anonimizacji.

DANE OSOBOWE-PRZESŁANKI PRAWNE

SPEŁNIENIE ZASADY LEGALNOŚCI CO DO PRZETWARZANIA DANYCH OSOBOWYCH

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych;
- przetwarzanie odbywa się na podstawie przepisu prawa, ustanawiającego uprawnienia lub obowiązki;
- przetwarzanie jest konieczne do realizacji umowy, której osoba, której dane dotyczą, jest stroną lub też do podjęcia działań przed zawarciem umowy na żądanie tej osoby;
- 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 a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

DANE OSOBOWE-BEZPIECZEŃSTWO

ZABEZPIECZENIE DANYCH PRZED

- nieupoważnionym udostępnieniem
- zabraniem przez osobę nieuprawnioną
- utratą
- uszkodzeniem lub zniszczeniem
- zmianą

DANE OSOBOWE-BEZPIECZEŃSTWO FIZYCZNE

Wyraźne granice obszarów w których przetwarzane są dane osobowe.
Fizyczne zabezpieczenie wejść do pomieszczeń i obiektów.
Ochrona przed zagrożeniami zewnętrznymi .
Praca w obszarach bezpiecznych wyznaczonych do przetwarzania danych osobowych.
Wyodrębnione obszary dostaw i załadunku.

ZASADA CZYSTEGO BIURKA

DANE OSOBOWE-BEZPIECZEŃSTWO SYS.

- Właściwe korzystanie z przydzielonych uprawnień (logi, hasła)
- Zasada czystego pulpitu
- Czyszczenie kosza
- Wygaszacz ekranu
- Ustawienie monitora
- Noszenie i zabezpieczanie nośników elektronicznych
- Ustawienia drukarek, niszczarek

Środki bezpieczeństwa

Środki bezpieczeństwa powinny być dostosowane do zidentyfikowanych w Powiślańskiej Szkole Wyższej ryzyk oraz uwzględniać aktualny stan wiedzy w tym zakresie. Powiślańska Szkoła Wyższa jest zobowiązana stosować wymagania określone przepisami rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Przykładowe środki służące zabezpieczeniu danych

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

Dokumentacja ochrony danych osobowych

Powiślańska Szkoła Wyższa prowadzi dokumentację opisującą zasady ochrony danych osobowych w celu zapewnienia bezpieczeństwa danych osobowych oraz dla możliwości wykazania/ potwierdzenia stosowanych zasad i zabezpieczeń.

DANE OSOBOWE W RELACJI STUDENT PRACOWNIK UCZELNI

ZACHOWANIE ZASADY POUFNOŚCI

Ochrona informacji o studencie, wynikach rekrutacji przed dostępem osób nieuprawnionych.
Udostępnianie danych jedynie zidentyfikowanym osobom uprawnionym.

Wydawanie dokumentacji studenta, zidentyfikowanym osobom upoważnionym.
Komunikacja ze studentem, kandydatem w sposób umożliwiający zachowanie dyskrecji.

Szyfrowanie danych wysyłanych
Korespondencja tradycyjna (list polecony za potwierdzeniem odbioru)

DANE OSOBOWE-PROCEDURY PROPOZYCJE

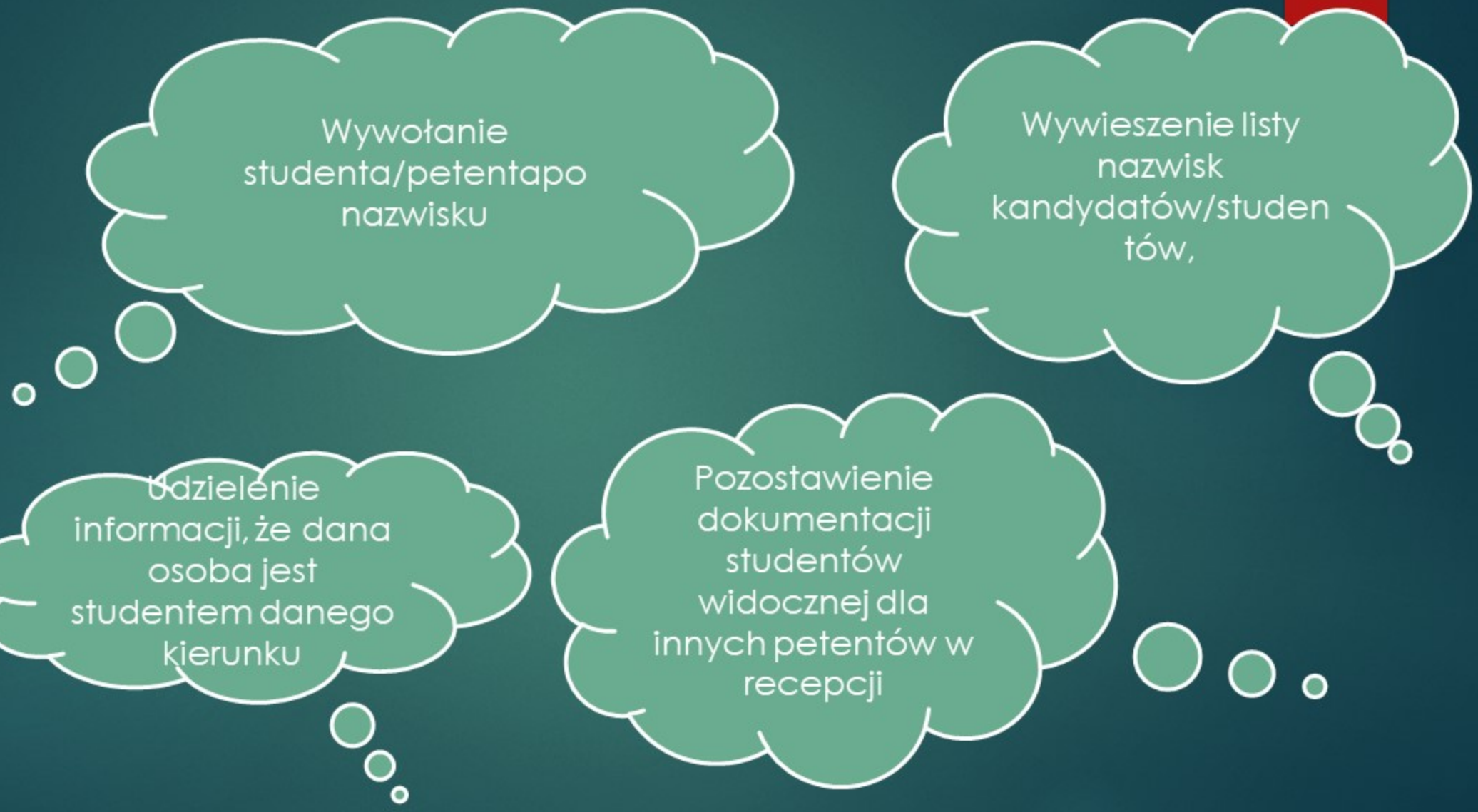
Klasyfikacja informacji
Zarządzanie incydentami i słabościami Systemu
Zarządzania Bezpieczeństwem Informacji
Bezpieczeństwo i ochrona danych osobowych
Bezpieczeństwo fizyczne i środowiskowe
Bezpieczeństwo teleinformatyczne
Bezpieczeństwo informacji w zarządzaniu zasobami ludzkimi
Monitoring wizyjny na terenie uczelni
Zasady dostępu pracowników, studentów i innych osób do Internetu
Zasady dostępu pracowników do zewnętrznych serwisów informacyjnych
Zasady wykorzystywania urządzeń przenośnych
Praca zdalna

DANE OSOBOWE-INCYDENT

ZGŁOSZENIE DO URZĘDU OCHRONY DANYCH OSOBOWYCH - 72 H

- Wykrycie
- Zgłoszenie przełożonemu, zgłoszenie IOD
- Postępowanie wyjaśniające
- Szacowanie skutków dla ochrony danych
- Poinformowanie osoby której dane dotyczą
- Wdrożenie środków zaradczych
- Zgłoszenie do UODO
- Wyciągniecie konsekwencji

DANE OSOBOWE-INCYDENT- przykłady naruszeń



DANE OSOBOWE-ODPOWIEDZIALNOŚĆ

Odpowiedzialność administracyjna

administracyjna kara pieniężna do 20 mln. EUR lub 4 % całkowitego rocznego obrotu przedsiębiorstwa – zastosowanie ma kara wyższa

UODO: podmioty publiczne – do 100 tys. zł.

Odpowiedzialność karna

Odpowiedzialność odszkodowawcza

Odpowiedzialność dyscyplinarna

Polityka ochrony danych osobowych

W celu zapewnienia, że dane osobowe w Powiślańskiej Szkole Wyższej są przetwarzane zgodnie z obowiązującymi przepisami prawa wprowadzona została polityka ochrony danych osobowych obejmująca wdrożenie odpowiednich środków organizacyjnych i technicznych zaprojektowanych w celu skutecznej realizacji ochrony danych osobowych, w tym niezbędnych zabezpieczeń odpowiednich do celów przetwarzania danych osobowych w Powiślańskiej Szkole Wyższej.

Rejestr czynności przetwarzania

Obowiązkiem Powiślańskiej Szkole Wyższej jest prowadzenie rejestru czynności przetwarzania zgodnie z art. 30 RODO.

W związku z powyższym pracownicy zobowiązani są zgłaszać informacje o planowanych czynnościach przetwarzania określając:

Cel przetwarzania, opis kategorii osób, których dane dotyczą i kategorii danych, kategorie odbiorców, którym dane zostały lub zostaną ujawnione, dane dot. przekazania danych do państwa trzeciego lub organizacji międzynarodowej, opis zabezpieczeń, terminy usunięcia poszczególnych kategorii danych.

Naruszenie ochrony danych osobowych

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

Typy naruszenia ochrony danych osobowych

- naruszenie poufności polegające na ujawnieniu danych osobowych nieuprawnionej osobie;
- naruszenie dostępności polegające na trwałej utracie lub zniszczeniu danych osobowych;
- naruszenie integralności polegające na zmianie treści danych osobowych w sposób nieautoryzowany

Zgłoszenie naruszenia ochrony danych osobowych

W przypadku naruszenia administrator danych osobowych niezwłocznie (w miarę możliwości nie później niż w terminie 72 godzin od stwierdzenia naruszenia) zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że istnieje małe prawdopodobieństwo, żeby naruszenie powodowało uszczerbek w prawach lub wolnościach osób fizycznych.

Zawiadomienie o naruszeniu danych osobowych

Zgodnie z art. 34 pkt 1 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zatem administrator jest zobowiązany do zawiadomienia osoby, której dane dotyczą, gdy spełnione zostaną łącznie dwie przesłanki:

- dojdzie do naruszenia ochrony danych osobowych;
- może ono powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Do takich przypadków należą sytuacje, w których naruszenie prowadzi do dyskryminacji, kradzieży tożsamości, oszustwa, straty finansowej lub uszczerbku na reputacji. Jeżeli naruszenie dotyczy danych szczególnych (wrażliwych), można założyć, że jest prawdopodobne, iż takie naruszenie może prowadzić do wskazanych wyżej szkód. Nie jest konieczne, aby wysokie ryzyko zmaterializowało się i by faktycznie doszło do naruszenia praw lub wolności; dlatego nie ma znaczenia, czy ostatecznie ich naruszenie nastąpi. Wystarczający jest fakt samego pojawienia się wysokiego ryzyka naruszenia praw lub wolności.

Udostępnianie danych kontaktowych pracowników

Wymiana danych kontaktowych pracowników pomiędzy podmiotami współpracującymi ze sobą jest zjawiskiem powszechnym i koniecznym do realizacji tej współpracy zarówno na płaszczyźnie naukowej, edukacyjnej czy biznesowej.

Podstawą prawną udostępniania tych danych przez Administratora będącego np. Pracodawcą jest art. 6 ust.1 lit. f – prawnie uzasadniony interes.

Administrator danych udostępnionych przez Uczelnię

Jeżeli udostępnimy dane kontaktowe naszego pracownika np. do kontaktu w sprawie umowy to administratorem tych danych staje się podmiot korzystający z tych danych, w celu do którego zostały mu udostępnione np. komunikacji.

Obowiązek informacyjny z art.14 RODO spoczywa wówczas na administratorze, któremu ujawniono dane.

Powierzenie przetwarzania danych

Powiślańska Szkoła Wyższa, jako administrator danych osobowych może powierzyć przetwarzanie danych osobowych określonym podmiotom w celu realizacji usług na jej rzecz np. konserwacji systemu informatycznego. Podmioty którym powierzono przetwarzanie danych osobowych muszą zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Podmiot przetwarzający

Przetwarzanie danych osobowych przez podmiot przetwarzający odbywa się przede wszystkim na podstawie umowy lub innego aktu/ instrumentu prawnego , sporządzonego w formie pisemnej, w tym elektronicznej.

Art.28 RODO

Zgodnie z definicją RODO „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

SPRAWDZENIE PODMIOTU PRZETWARZAJĄCEGO

Przed powierzeniem danych Administrator powinien zweryfikować, czy podmiot, który będzie przetwarzał w jego imieniu dane osobowe daje gwarancje wdrożenia odpowiednich środków technicznych, organizacyjnych, tzn. zapewni, że przetwarzanie będzie spełniało wymogi RODO i będzie chroniło prawa osób, których dane dotyczą.

Jak rozpoznać, że powinniśmy zawrzeć umowę powierzenia danych

Niektóre przypadki powierzenia przetwarzania danych są proste i jednoznaczne, np. powierzenie danych w celu prowadzenia rachunkowości firmy, wsparcia informatycznego, usługi hostingu, inne natomiast wymagają dogłębnej analizy.

Do oceny niektórych przypadków wymagana jest również często znajomość przepisów sektorowych obowiązujących w danej branży lub w odniesieniu do niektórych zawodów. Najważniejszą cechą podmiotu przetwarzającego jest brak samodzielności przy wyznaczaniu celu i sposobu przewarzania danych, który określa administrator.

Bezpieczna praca z komputerem

Zasady pracy w systemach informatycznych regulują wewnętrzne akty prawne dotyczące zarządzania systemami informatycznymi w Powiślańskiej Szkole Wyższej.

Główne zabezpieczenia to: system haseł, system antywirusowy aktualizowany na bieżąco, wylogowanie po zakończeniu pracy i odejściu od stanowiska pracy, szyfrowanie plików i dysków zawierających dane osobowe, zabezpieczenie nośników przenośnych, zabezpieczenie laptopów, niekorzystanie z innych sieci poza siecią uczelnianą, ewentualne transakcje z użycie VPN.

Polityka czystego biurka

Polityka czystego biurka jest elementem Polityki ochrony danych osobowych w Powiślańskiej Szkole Wyższej i stanowi element zabezpieczenia danych. Dlatego pamiętajmy:

- opuszczając miejsce pracy powinniśmy schować dokumenty zawierające dane osobowe do zamkniętej szafy, tak aby uniemożliwić osobie nieuprawnionej dostęp do informacji, do których nie jest upoważniona;
- w miejscach, gdzie w trakcie pracy często odwiedzają nas osoby z zewnątrz – np. klienci, studenci – powinniśmy dodatkowo, odwracać dokumenty, które zawierają dane osobowe na drugą stronę tak, aby osoba znajdująca się przy naszym biurku nie miała wglądu w nasze poufne zapiski lub zapewnić stosowane przegrody;
- w przypadku zaistnienia ryzyka podejrzenia wyświetlanych danych minimalizujmy wszystkie programy tak aby interesant widział jedynie nasz pulpit.

Polityka czystego ekranu

Nieumieszczanie na pulpicie dokumentów zawierających dane osobowe.

Stosowanie wygaszaczy ekranu. Tak naprawdę zasada czystego ekranu to bardzo prosta sprawa – w naszym komputerze powinien być skonfigurowany wygaszacz ekranu, który aktywuje się po wykryciu np. ustalonego okresu bezczynności, z reguły jest to kilka minut. Wracając do takiej zablokowanej stacji roboczej należy użyć hasła aby kontynuować pracę.

Niszczenie dokumentów

Niszczenie powinno dotyczyć wszystkich nadmiarowych lub niepotrzebnych dokumentów zawierających dane osobowe poprzez:

- Zniszczenie w niszczarce co najmniej 2 klasy ochrony/ poziom 3, według obowiązującej normy DIN 66399 – FORMA PAPIEROWA.
- Umieszczenie w koszu zainstalowanym na stacji roboczej komputera i jego opróżnienie – FORMA ELEKTRONICZNA.

Kopiowanie dokumentów

Zabrania się kopiowania dokumentów zawierających całe zbiory, bazy danych i ich przenoszenie, przesyłanie poza użytkowane systemy informatyczne np. na pendriva, dodatkowe dyski przenośne, z wyłączeniem sytuacji wynikających z przepisów prawa ciążących na administratorze.

Ochrona i dostęp do pomieszczeń

Należy zapewnić ochronę pomieszczeń w których przetwarzane są dane osobowe.

Podstawowe zasady ochrony to:

Upoważnienia do pobierania kluczy do określonych pomieszczeń,

Ochrona zewnętrzna budynków lub w ramach pracowników sprawujących dozór na portierniach,

Systemy alarmowe, przeciwłamaniowe, przeciwpożarowe,

Okresowe przeglądy techniczne pomieszczeń,

Niepozostawianie otwartych pomieszczeń bez nadzoru osób upoważnionych do przetwarzania danych osobowych,

Zabezpieczenie dokumentacji w szafach i szufladach z odpowiednimi zabezpieczeniami.

Warto zapamiętać

- Każdy pracujący z danymi osobowymi powinien przestrzegać zasad zgodności z prawem przetwarzania danych osobowych;
- Zgromadzone dane osobowe nie mogą być wykorzystywane dla swoich osobistych celów.
- Pracownicy nie powinni wykorzystywać sprzętu służbowego do osobistego użytku.
- Pracownicy nie mogą dzielić się danymi osobowymi dostępnymi w ramach wykonywanych obowiązków z osobami trzecimi.

Obowiązki pracowników - Podsumowanie

- Zachowania w poufności danych osobowych przetwarzanych w Powiślańskiej Szkole Wyższej oraz informacji o sposobach ich zabezpieczenia;
- Ochrony danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
- Informowania o każdym przypadku bądź podejrzeniu naruszenia zasad lub środków ochrony danych;
- Przechowywania dokumentów lub nośników informacji zawierających dane osobowe w miejscu niedostępnym dla osób spoza grona podmiotów i osób upoważnionych do ich przetwarzania;
- Niepozostawiania informacji zawierających dane osobowe przy urządzeniach służących do wydruku, do których mogą mieć dostęp osoby nieupoważnione tj. przy kopiarkach, drukarkach czy faksach;

Obowiązki pracowników – Podsumowanie cd.

- Pracy w systemach informatycznych służących do przetwarzania danych jedynie na przypisanych kontach oraz zachowania poufności udostępnionych mu haseł oraz kodów dostępu;
- Odpowiedniego zabezpieczenia pomieszczenia obejmującego obszar przetwarzania jeżeli nie pozostaje w nim inna osoba upoważniona, zarówno w godzinach pracy, jak i po jej zakończeniu;
- Niepozostawiania bez nadzoru jakichkolwiek dokumentów zawierających dane osobowe;
- Niszczenia nadmiarowych dokumentów zawierających dane osobowe w sposób uniemożliwiający ich ponowne odczytanie.

Odpowiedzialność

Pracownicy przetwarzający dane osobowe ponoszą odpowiedzialność z tytułu naruszenia obowiązujących procedur i przepisów prawa dot. ochrony danych osobowych odpowiednio do wagi naruszenia. Działania lub zaniechania ze strony pracowników powodujące naruszenie bezpieczeństwa, ochrony danych osobowych może skutkować m.in. nałożeniem przez administratora kary dyscyplinarnej/ porządkowej z rozwiązaniem stosunku pracy włącznie.

Kary pieniężne

- Prezes Urzędu Ochrony Danych Osobowy może nałożyć na Uczelnię kary pieniężne w wysokości 100 tys. zł .
- Kara zostaje nałożona w drodze decyzji.
- Kary pieniężne są nakładane na podstawie i warunkach określonych w art.83 RODO

Podstawa prawna – Ustawa o ochronie danych osobowych z dnia 24 maja 2018 r.

Przepisy karne

Ustawa o ochronie danych osobowych w art. 107-108 przewiduje sankcje karne w następujących przypadkach:

- Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch
- Jeżeli czyn, o którym mowa w pkt. powyżej dot. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dot. zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Dane Inspektora Ochrony Danych

Natalia Parus

Inspektor Ochrony Danych

Powiślańska Szkoła Wyższa

ido@psw.kwidzyn.edu.pl