„ZATWIERDZAM"

REKTOR

Zachodniopomorskiego Uniwersytetu Technologicznego

w Szczecinie

.....

dr hab. inż. Jacek Wróbel, prof. nadzw.

Zachodniopomorski
Uniwersytet
Technologiczny
w Szczecinie

Zatwierdzam i wprowadzam do użytku służbowego:

Wytyczne

w zakresie ochrony danych osobowych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

Inspektor Ochrony Danych

INSPEKTOR OCHRONY DANYCH
w Zachodniopomorskim Uniwersytecie Technologicznym
w Szczecinie
mgr Artur Kurek

WYKAZ ZAGADNIEŃ

1. Co to jest RODO.
2. Kto jest Administratorem danych przetwarzanych na ZUT.
3. Kto to jest Inspektor Ochrony Danych (IOD).
4. Co to są dane osobowe.
5. Co to są szczególne kategorie danych osobowych.
6. Jak wiele danych można zbierać zgodnie z RODO.
7. Co to jest przetwarzanie danych osobowych.
8. Kto może przetwarzać dane osobowe na ZUT.
9. Co to jest rejestr czynności przetwarzania.
10. Jakie operacje przetwarzania danych osobowych zachodzą na ZUT.
11. Czyje dane przetwarzane są na ZUT.
12. Jaki zakres danych przetwarzany jest na ZUT.
13. Gdzie na ZUT przetwarzane są dane osobowe.
14. W jakim celu ZUT przetwarza dane osobowe.
15. Jak długo można przechowywać dane osobowe.
16. Czy ZUT udostępnia dane osobowe.
17. Czy ZUT powierza dane osobowe.
18. Na jakich podstawach prawnych ZUT przetwarza dane osobowe.
19. Kiedy jednostki organizacyjne ZUT powinny spełniać obowiązek informacyjny.
20. Kiedy na ZUT powinniśmy pozyskiwać zgodę na przetwarzanie danych osobowych.
21. Kiedy na ZUT może dojść do naruszenia ochrony danych osobowych.
22. Co należy zrobić w przypadku stwierdzenia naruszenia ochrony danych osobowych.
23. Czym jest ochrona danych osobowych w fazie projektowania (privacy by design).
24. Czym jest domyślna ochrona danych osobowych (privacy by default).
25. Co to jest ocena skutków dla ochrony danych osobowych.
26. Jakie techniczne i organizacyjne zabezpieczenia danych osobowych są stosowane na ZUT.
27. Co powinien zrobić pracownik w przypadku czasowego opuszczenia stanowiska pracy.

28. Jak postępować z danymi osobowymi przetwarzanymi w wersji papierowej.
29. Jak postępować z elektronicznymi nośnikami danych osobowych.
30. Podstawowe zasady postępowania w zakresie zabezpieczenia danych osobowych.
31. Monitoring wizyjny.
32. Wzory dokumentów.

1/ Upoważnienie do przetwarzania danych osobowych,
2/ Klauzula informacyjna dotycząca przetwarzania danych osobowych,
3/ Klauzula informacyjna dotycząca monitoringu wizyjnego,
4/ Klauzula zgody na przetwarzanie danych osobowych,
5/ Wniosek o cofnięcie zgody na przetwarzanie,
6/ Wniosek o przeniesienie danych,
7/ Żądanie sprostowania danych,
8/ Żądanie usunięcia danych osobowych,
9/ Wniosek w sprawie uprzednich konsultacji,
10/ Ocena skutków dla ochrony danych,
11/Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych,
12/ Zgłoszenie w sprawie naruszenia ochrony danych osobowych,
13/ Ewidencja osób upoważnionych do przetwarzania danych osobowych,
14/ Wykaz pomieszczeń w których przetwarzane są dane osobowe.

33. RODO – lista audytowa.

1. Co to jest RODO.

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).

RODO 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. RODO jest aktem, który w sposób kompleksowy reguluje kwestie dotyczące ochrony danych osobowych i nie wymaga implementacji do krajowego systemu prawnego, oznacza to, że przepisy RODO 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 RODO jest nowa ustawa o ochronie danych osobowych.

2. Kto jest Administratorem danych przetwarzanych na ZUT.

Administratorem danych przetwarzanych na ZUT jest uczelnia reprezentowana przez Jego Magnificencję Rektora, z siedzibą przy al. Piastów 17, 70-310 w Szczecinie.

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 RODO.

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

Inspektor Ochrony Danych to wyznaczona przez Rektora Zachodniopomorskiego Uniwersytetu Technologicznego osoba, która jest odpowiedzialna za nadzór i bezpieczeństwo danych osobowych przetwarzanych na uczelni.
Inspektor Ochrony Danych odpowiada za nadzór nad funkcjonowaniem i efektywnością procesów prawidłowego przetwarzania danych osobowych. Szczegółowy zakres zadań IOD określa zarządzenie nr 37 z dnia 22.05.2018 roku w sprawie powołania inspektora ochrony danych w Zachodniopomorskim Uniwersytecie Technologicznym w Szczecinie

4. 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.

5. 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 RODO, m.in.:

1. zgoda osoby, której dane dotyczą ,
2. 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,
3. 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,
   1) gdy przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
   2) 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,
   3) 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 ZUT są między innymi w: badaniach naukowych, projektach czy w celu zapewnienia równych szans osobom niepełnosprawnym.

6. Jak wiele danych można zbierać zgodnie z RODO.

RODO 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.

7. 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.

8. Kto może przetwarzać dane osobowe na ZUT.

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 RODO, tzn. uczelnia 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.:

1. kandydatów na studia
2. studentów
3. pracowników

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

9. Co to jest rejestr czynności przetwarzania.

Rejestr czynności przetwarzania to dokument, który pokazuje, w jakich procesach uczelnia 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.

10. Jakie operacje przetwarzania danych osobowych zachodzą na ZUT.

Uczelnia przetwarza dane osobowe w procesach dotyczących m.in. :

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

11. Czyje dane przetwarzane są na ZUT.

ZUT przetwarza m.in. dane:

1. pracowników uczelni i ich rodzin,
2. kandydatów na określone funkcje,
3. studentów, doktorantów, słuchaczy studiów podyplomowych oraz osób ubiegających się o przyjęcie na studia, studia doktoranckie lub studia podyplomowe,
4. osób, które uzyskały stopień naukowy doktora lub doktora habilitowanego,
5. cudzoziemców podejmujących i odbywających studia, studia doktoranckie i inne formy kształcenia, a także uczestniczące w badaniach naukowych lub pracach rozwojowych,
6. studentów i doktorantów, w tym cudzoziemców ubiegających się o stypendia lub świadczenia z zakresu pomocy materialnej,
7. czytelników bibliotek,
8. osób biorących udział w postępowaniach konkursowych,
9. uczestników badań naukowych,
10. uczestników konferencji, projektów, seminariów,
11. absolwentów.

12. Zakres danych przetwarzany na ZUT.

ZUT przetwarza dane między innymi w zakresie:

1. imion i nazwisk,
2. dat urodzenia,
3. numeru PESEL,
4. numeru indeksu,
5. serii i numeru dokumentu potwierdzającego tożsamość,
6. adresu e-mail,
7. numeru telefonu,
8. wizerunku,
9. obywatelstwa.

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

1. stanie zdrowia, stopniu niepełnosprawności,
2. pochodzeniu rasowym lub etnicznym,
3. przynależności do związków zawodowych.

13. Gdzie na uczelni przetwarzane są dane osobowe.

Dane osobowe przetwarzane są w:

1. systemach informatycznych,
2. pakietach biurowych,
3. systemach pocztowych,
4. zbiory tradycyjne (papierowe) np.: akta pracownicze, akta studenckie, teczki osobowe, korespondencja papierowa itp.

14. W jakim celu ZUT przetwarza dane osobowe.

ZUT przetwarza dane osobowe m.in. w celach:

1. przyjęcia kandydatów na studia,
2. przyjęcia kandydatów do pracy,
3. realizacji procesu dydaktycznego,
4. obsługi czytelników bibliotek,
5. zatrudnienia pracownika,
6. zawierania umów cywilnoprawnych,
7. prowadzenia dokumentacji kadrowej,
8. prowadzenia spraw bytowo-socjalnych studentów i pracowników,
9. nadzoru nad przestrzeganiem zasad bezpieczeństwa i higieny pracy,
10. realizacji projektów badawczych,
11. przyznawania stypendiów,
12. przydziału miejsc w domach studenckich,
13. działań marketingowych, zarządzania ofertą: edukacyjną, naukową, usługową.

15. Jak długo można przechowywać dane osobowe.

RODO 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 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.

16. Czy ZUT udostępnia dane osobowe.

Udostępnianie danych osobowych to jedna z form operacji wykonywanych na danych osobowych w ramach przetwarzania tych danych. ZUT, 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.

Uczelnia udostępnia dane osobowe m.in.:

1. zgodnie z ustawą prawo o szkolnictwie wyższym Ministerstwu Nauki i Szkolnictwa Wyższego,
2. ZUS w celu potwierdzenia statusu studenta,
3. potencjalnym pracodawcom na podstawie zgody absolwenta.

17. Czy ZUT powierza dane osobowe.

Powierzenie przetwarzania danych osobowych zachodzi wtedy, gdy uczelnia 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.

ZUT powierza dane osobowe m.in.:

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

18. Na jakich podstawach prawnych ZUT przetwarza dane osobowe.

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

1. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie jej danych osobowych;
2. 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;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. 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 ZUT:

1. 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;

2. 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.

Uczelnia 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.

19. Kiedy jednostki organizacyjne ZUT powinny spełniać obowiązek informacyjny.

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

1. danych identyfikujących Administratora,
2. danych kontaktowych Inspektora Ochrony Danych ,
3. przysługujących jej prawach,
4. celu przetwarzania danych osobowych,
5. okresie przechowywania danych osobowych,
6. podstawie przetwarzania danych osobowych,
7. możliwości złożenia skargi do organu nadzorczego.

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.

20. Kiedy na ZUT 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 ZUT na podstawie zgody przetwarzane są m.in. dane następujących kategorii osób:

1. kandydatów do pracy,
2. absolwentów,
3. uczestników badań/projektów,
4. 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.

21. Kiedy na ZUT 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:

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

22. 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:

1. datę zdarzenia,
2. opis zaistniałego incydentu,
3. miejsce wystąpienia incydentu,
4. wskazać przyczynę lub potencjalną przyczynę wystąpienia naruszenia,
5. ustalić możliwe skutki wynikające z naruszenia,

6. opisać dotychczasowe działania w związku z incydentem,
7. opisać znane danej osobie sposoby zabezpieczenia danych osobowych.

23. 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:

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

24. 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.

25. 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 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.

26. Jakie techniczne i organizacyjne zabezpieczenia danych osobowych są stosowane na ZUT.

Na uczelni stosuje się m.in.:

Zabezpieczenia organizacyjne:

1. wyznaczenie Inspektora Ochrony Danych ,
2. opracowanie i wdrożenie dokumentacji ochrony danych osobowych,
3. do przetwarzania danych osobowych dopuszczone zostały osoby do tego upoważnione,
4. prowadzenie ewidencji osób upoważnionych,
5. przeszkolenie i zaznajomienie pracowników z przepisami ochrony danych osobowych,
6. procedura wydawania kluczy do pomieszczeń osobom uprawnionym,
7. nadzór obszarów przez służbę ochrony,
8. monitoring osób wchodzących i wychodzących z budynków,
9. osoby trzecie w obszarze przetwarzania danych osobowych przebywają w obecności osób upoważnionych,
10. osoby upoważnione zobowiązane są do zachowania danych osobowych i sposobów zabezpieczeń w tajemnicy.

Środki ochrony fizycznej:

1. drzwi zamykane na klucz,
2. systemy przeciwpożarowe,
3. szafy niemetalowe/metalowe zamykane na klucz,
4. sejfy, kasy pancerne,
5. niszczarki dokumentów,
6. drzwi o podwyższonej odporności na włamanie,
7. okna zabezpieczone za pomocą krat/rolet,

8. systemy alarmowe,
9. systemy monitoringu wizyjnego.

Środki ochrony w ramach narzędzi programowych:

1. rejestracja zmian w systemach,
2. określenie praw dostępu do danych,
3. identyfikatory użytkowników oraz hasła.

27. Co powinienem zrobić w przypadku czasowego opuszczenia stanowiska pracy.

W przypadku opuszczenia obszaru przetwarzania danych osobowych, gdy pozostaje on bez nadzoru osób upoważnionych, należy zamknąć pomieszczenie na klucz. Klucze do pomieszczeń powinny pozostawać pod nadzorem osób upoważnionych.

Czasowo opuszczając stanowisko pracy należy wylogować się z systemu lub uruchomić wygaszacz ekranu chroniony hasłem. Nie należy pozostawiać dokumentów zawierających dane osobowe w miejscu widocznym.

Po zakończonej pracy należy wylogować się ze wszystkich systemów, z których korzystaliśmy podczas pracy, zamknąć w szafach dokumenty zawierające dane osobowe lub inne tajemnice ustawowo chronione.

28. Jak postępować z danymi osobowymi przetwarzanymi w wersji papierowej.

1. dokumenty i wydruki w pomieszczeniach nieupoważnionych zawierające dane osobowe należy przechowywać zabezpieczonych fizycznie przed dostępem osób trzecich,
2. użytkownicy są zobowiązani do stosowania „**polityki czystego biurka”,** polega ona na zabezpieczeniu dokumentów zawierających dane osobowe w szafach, biurkach, pomieszczeniach zamykanych na klucz, ograniczając wgląd przez osoby nieupoważnione,

3. dokumenty należy przenosić w sposób zapobiegający ich kradzieży, zgubieniu lub utracie,
4. zalecane jest niszczenie dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

29. Jak postępować z elektronicznymi nośnikami danych osobowych.

1. dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika danych podlega skasowaniu,
2. dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po upływie tego celu dane podlegają archiwizacji, skasowaniu lub anonimizacji,
3. przenośne elektroniczne nośniki danych są przechowywane przez użytkowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych,
4. w przypadku konieczności wyniesienia nośników danych poza jednostkę organizacyjną, użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia nośnika, konieczne jest użycie środków ochrony kryptograficznej (szyfrowanie danych),
5. w przypadku wykorzystywania elektronicznych urządzeń mobilnych (m.in. smartphone, tablet) wymaga się zastosowania następujących środków bezpieczeństwa: blokada ekranu (pin/hasło/symbol graficzny), szyfrowanie pamięci/karty pamięci, program antywirusowy, wyłączenie nieużywanych usług (np.wi-fi, bluetooth, nfc), instalowanie oprogramowania z zaufanych źródeł, używanie szyfrowania lub VPN podczas korzystania z publicznych hotspot-ów,
6. w przypadku korzystania z komputerów przenośnych poza obszarem przetwarzania danych jednostki organizacyjnej, należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby nieuprawnione i stosować środki ochrony kryptograficznej,
7. za bezpieczeństwo komputerów przenośnych, urządzeń mobilnych, nośników danych odpowiadają ich użytkownicy. Zabrania się pozostawiania nośników danych bez nadzoru osoby upoważnionej.

30. Podstawowe zasady postępowania w zakresie zabezpieczenia danych osobowych.

1) **Zasada legalności** – przetwarzanie danych osobowych musi odbywać się zgodnie z prawem tj. musi istnieć podstawa prawna przetwarzania.
2) **Zasada celowości** – cel przetwarzania danych musi z góry być określony i informacja ta musi zostać przekazana osobie, której dane dotyczą.
3) **Zasada merytorycznej poprawności** – dane osobowe muszą być prawdziwe, kompletne i aktualne ze względu na cel jakiemu mają służyć. Nie powinno się zbierać danych osobowych ze źródeł nieznanego pochodzenia.
4) **Zasada adekwatności** – można przetwarzać tylko de dane osobowe, które są niezbędna do celu jaki administrator danych chce osiągnąć. \
5) **Zasada ograniczenia czasowego** – dane osobowe nie mogą być przetwarzane dłużej niż jest to konieczne do osiągnięcia celu, w którym zostały zebrane.
6) **Polityka czystego biurka** – należy pamiętać o konieczności usuwania wszelkich nośników danych osobowych poza zasięg wzroku i zasięg dłoni osób postronnych i ich przechowywania pod kluczem.
7) **Polityka czystego druku** – należy pamiętać o konieczności odbierania wszelkich wydruków z urządzeń drukujących niezwłocznie po ich wydrukowaniu.
8) **Polityka czystego ekranu** – należy pamiętać o konieczności blokowania komputerów nawet przed krótkotrwałym opuszczeniem stanowiska pracy (WIN+L). Dodatkowo należy uniemożliwiać wgląd w treści wyświetlane na monitorach osobom nieupoważnionym – odpowiednia ustawienie ekranu.
9) **Procedura niszczenia** – należy pamiętać o konieczności niszczenia dokumentów zawierających dane osobowe z wykorzystaniem niszczarek lub pojemników do utylizacji dokumentacji poufnej, gdy już staną się nie potrzebne.
10) **Polityka haseł** – należy pamiętać o konieczności zmiany hasła w cyklach nie rzadszych niż 90 dni oraz o zakazie współdzielenie dostępów do systemów informatycznych z wykorzystaniem jednego identyfikatora/loginu.
11) **Procedura korzystania z urządzeń mobilnych** – należy pamiętać o konieczności zabezpieczania sprzętu informatycznego (laptopy, smartfony, tablety, pendrive) w trakcie ich wynoszenia poza obszar pracy (obszar przetwarzania danych) – hasło , PIN, technologia biometryczna)

12) **Procedura korzystania z internetu** – należy pamiętać o zakazie stosowania zapamiętywania haseł w przeglądarkach internetowych oraz historii wyszukiwania – okresowo należy czyścic historię przeglądania lub wyłączyć jej zapamiętywanie.
13) **Procedura korzystania z poczty elektronicznej** – należy pamiętać o weryfikacji w procesie wysyłania tak aby adresacja była prawidłowa – w szczególności należy weryfikować opcje kopia ukryta/kopia jawna. Dodatkowo nie wolno korzystać z odnośników znajdujących się w mailach nieznanego pochodzenia.

31. Monitoring wizyjny.

1. Przetwarzanie danych osobowych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ZUT , w tym w celu zapewnienia bezpieczeństwa osób i ochrony mienia. Podstawę prawną przetwarzania danych osobowych stanowi art. 6 ust. 1 lit. c RODO w związku z art. 22^2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917 z późn. zm.).
2. Monitoring obejmuje zewnętrzny oraz wewnętrzny teren obiektów.
3. Dane mogą być przekazywane podmiotom przetwarzającym dane osobowe na zlecenie administratora danych, a także innym podmiotom uprawnionym na podstawie przepisów prawa.
4. Nagrania obrazu będą przetwarzane wyłącznie do celów, dla których zostały zebrane i będą przechowywane przez okres nieprzekraczający 3 miesięcy od dnia nagrania.
5. Osobie, której dane dotyczą przysługuje prawo:
- dostępu do danych osobowych,
- żądania ich sprostowania,
- ograniczenia przetwarzania, w przypadkach wymienionych w RODO,
- usunięcia danych, w przypadku, gdyby dane były przetwarzane niezgodnie z prawem.
6. W związku z tym, że przetwarzanie danych osobowych odbywa się na podstawie art. 6 ust. 1 lit. c RODO, osobie której dane dotyczą nie przysługuje prawo do przenoszenia danych ani prawo do złożenia sprzeciwu.
7. Przetwarzanie danych osobowych utrwalonych na nagraniach obrazu jest dla ZUT niezbędne do zapewnienia bezpieczeństwa studentów, pracowników, ochrony mienia.

WZORY DOKUMENTÓW

Załącznik nr 1

Data nadania upoważnienia: …….

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
w celu spełnienia wymogów art. 29 (RODO)

1. Upoważniam Panią/Pana

.....
Zatrudnioną/-ego na stanowisku.....
w.....

do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
- .....
- .....
- .....
- .....
- .....

2. Identyfikator/Login .....
3. Okres trwania upoważnienia:.....

Wystawił……..
(podpis i pieczątka)

Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej:…….

Załącznik nr 2

Klauzula informacyjna dotycząca przetwarzania danych osobowych

Zgodnie z art. 13 ust 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych 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) informuje się, że:

1. Administratorem Pani/Pana danych osobowych jest Zachodniopomorski Uniwersytet Technologiczny w Szczecinie z siedzibą w Szczecinie al. Piastów 17, tel. 091 449 4015,

e-mail rektor@zut.edu.pl

2. Inspektorem ochrony danych w ZUT jest mgr Artur Kurek, z którym kontakt możliwy jest

   - pisemnie: na adres 70-311 Szczecin al. Piastów 17 lub e-mail IOD.kurek@zut.edu.pl

   - telefonicznie 091 449 4924,

3. Pani/Pana dane osobowe przetwarzane w celu realizowania ……
4. Odbiorcą Pani/Pana danych osobowych będzie Zachodniopomorski Uniwersytet Technologiczny w Szczecinie.
5. Pani/Pana dane osobowe będą przechowywane przez okres ……, a po jego zakończeniu przez okres zgodny z przepisami prawa obowiązującymi w tym zakresie.
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody).
7. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych (PUODO) – gdy uzna Pani/Pan, iż przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych.

8. Podanie przez Pani/Pana danych osobowych jest konieczne z uwagi na ……..

9. Dane udostępnione przez Panią/Pana nie będą podlegały udostępnieniu podmiotom trzecim.

10. Dane udostępnione przez Panią/Pana nie będą podlegały profilowaniu.

11. Administrator danych nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Załącznik nr 3

Klauzula informacyjna dotycząca monitoringu wizyjnego

Zgodnie z art. 13 ust 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych 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) informuje się, że:

1. Administratorem Pani/Pana danych osobowych jest Zachodniopomorski Uniwersytet Technologiczny w Szczecinie z siedzibą w Szczecinie al. Piastów 17,
2. Inspektorem ochrony danych w ZUT jest mgr Artur Kurek, z którym kontakt możliwy jest

- pisemnie: na adres 70-311 Szczecin al. Piastów 17 lub e-mail IOD.kurek@zut.edu.pl
- telefonicznie 091 449 4924,.

3. Przetwarzanie danych osobowych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ZUT , w tym w celu zapewnienia bezpieczeństwa osób i ochrony mienia. Podstawę prawną przetwarzania danych osobowych stanowi art. 6 ust. 1 lit. c RODO w związku z art. 22^2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917 z późn. zm.).
4. Monitoring obejmuje zewnętrzny oraz wewnętrzny teren obiektów.
5. Dane mogą być przekazywane podmiotom przetwarzającym dane osobowe na zlecenie administratora danych, a także innym podmiotom uprawnionym na podstawie przepisów prawa.
6. Dane nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowej.
7. Nagrania obrazu będą przetwarzane wyłącznie do celów, dla których zostały zebrane i będą przechowywane przez okres nieprzekraczający 3 miesięcy od dnia nagrania.
8. Osobie, której dane dotyczą przysługuje prawo:

- dostępu do danych osobowych,
- żądania ich sprostowania,
- ograniczenia przetwarzania, w przypadkach wymienionych w RODO,

- usunięcia danych, w przypadku, gdyby dane były przetwarzane niezgodnie z prawem.

9. W związku z tym, że przetwarzanie danych osobowych odbywa się na podstawie art. 6 ust. 1 lit. c RODO, osobie której dane dotyczą nie przysługuje prawo do przenoszenia danych ani prawo do złożenia sprzeciwu.

10. Informuję się, że osobie, której dane dotyczą przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa).

11. Przetwarzanie danych osobowych utrwalonych na nagraniach obrazu jest dla ZUT niezbędne do zapewnienia bezpieczeństwa studentów, pracowników ,ochrony mienia.

12. W trakcie przetwarzania danych nie będzie dochodziło do zautomatyzowanego podejmowania decyzji ani do profilowania.

Załącznik nr 4

KLAUZULA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH.

Zgodnie z art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (RODO) wyrażam zgodę na przetwarzanie moich danych osobowych…(*wskazać jakich*, np. *zawartych w mojej ofercie pracy, zawartych w formularzu, lub przez wskazanie konkretnych danych, które będą przetwarzane np. w postaci imienia i nazwiska, adresy zamieszkania itp*.) w celu……..(*wskazać cel przetwarzania: np. udziału w procesie rekrutacji, udziału w konkursie XYZ, w celach marketingowych itd*.) przez…(*wskazać nazwę podmiotu, który będzie przetwarzać dane osobowe*).

data i podpis osoby wyrażającej zgodę: …….

Załącznik nr 5

Miejscowość, data

(Imię i nazwisko wnioskodawcy)

……
(Adres wnioskodawcy,)
tel. kontaktowy

……
(Pełna nazwa administratora danych)

……
(Adres siedziby administratora danych)

Wniosek o cofnięcie zgody na przetwarzanie

Zgodnie z art. 7 pkt. 3 Rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r. informuję o wycofaniu zgody na przetwarzanie moich danych osobowych.

Uzasadnienie wniosku:

……
(podpis wnioskodawcy)

Załącznik nr 6

Miejscowość, data

……
(Imię i nazwisko wnioskodawcy)

……
(Adres wnioskodawcy)
tel. kontaktowy

……
(Pełna nazwa administratora danych)

……
(Adres siedziby administratora danych)

Wniosek o przeniesienie danych

Zgodnie z art. 20 pkt. 1,2,3,4 Rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r. wnioskuję o dokonanie przeniesienia moich danych osobowych do wskazanego administratora.

Uzasadnienie wniosku:

……
(podpis wnioskodawcy)

Załącznik nr 7

Miejscowość, data

……
(Imię i nazwisko wnioskodawcy)

……
(Adres wnioskodawcy)
tel. kontaktowy

……
(Pełna nazwa administratora danych)

……
(Adres siedziby administratora danych)

Żądanie sprostowania danych

Zgodnie z art. 16 Rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r. żądam sprostowania moich danych osobowych, które są nieprawidłowe.

Uzasadnienie żądania:

……
(podpis wnioskodawcy)

Załącznik nr 8

Miejscowość, data

……
(Imię i nazwisko wnioskodawcy)

……
(Adres wnioskodawcy)
tel. kontaktowy

……
(Pełna nazwa administratora danych)

……
(Adres siedziby administratora danych)

Żądanie usunięcia danych osobowych

Zgodnie z art. 17 pkt. 1,2,3 Rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r. żądam niezwłocznego usunięcia danych osobowych dotyczących mojej osoby.

Uzasadnienie żądania:

……
(podpis wnioskodawcy)

Załącznik nr 9

……
(miejscowość, data)

WNIOSEK W SPRAWIE UPRZEDNICH KONSULTACJI**

Niniejszym w trybie art. 36 ogólnego rozporządzenia o ochronie danych wnoszę o przeprowadzenie konsultacji w związku z planowanym przetwarzaniem mogącym nieść wysokie ryzyko naruszenia praw lub wolności osób fizycznych

Obowiązki administratora*	
Obowiązki współadministratorów*	
Dane kontaktowe inspektora ochrony danych	
Obowiązki podmiotów przetwarzających*	
Cele i sposoby zamierzonego przetwarzania	
Opis środków i zabezpieczeń mających chronić prawa i wolności osób, których dane dotyczą	

……
(czytelny podpis administratora danych)

*- we wniosku należy również wskazać odpowiednie obowiązki administratora, współadmistratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw .

**- Do wniosku należy załączyć ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Załącznik nr 10

OCENA SKUTKÓW DLA OCHRONY DANYCH

Lp.	Opis planowanych operacji i celów przetwarzania	Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów	Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą*	Planowane środki w celu zaradzenia ryzyku, w tym zabezpieczenia, oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia z uwzględnieniem praw prawnie uzasadnionych, interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy
1.				
2.				
3.				
4.				

Załącznik nr 11

Szanowny/a Pan/Pani ……

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ
O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

W związku z art. 34 ust. 1 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), informuję o naruszeniu ochrony Pana/i danych osobowych przetwarzanych przez …….

Charakter naruszenia ochrony danych osobowych	
Możliwe konsekwencje naruszenia ochrony danych osobowych	
Środki zastosowane/proponowane w celu zaradzenia naruszeniu ochrony danych / zminimalizowania negatywnych skutków*	
Imię i nazwisko inspektora ochrony danych / punkt kontaktowy	

**W zależności od przypadku, który wystąpił.*

Załącznik nr 12

……
(miejscowość, data)

ZGŁOSZENIE W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu…….....
.....

1.	Charakter naruszenia ochrony danych:	
2.	Kategoria i przybliżona liczba osób, których dane dotyczą:	
3.	Liczba rekordów, których dotyczy naruszenie:	
4.	Możliwe konsekwencje naruszenia ochrony danych:	
5.	Środki zastosowane lub proponowane w celu zaradzenia	

	naruszeniom ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenie ochrony danych.	
6.	Dane inspektora ochrony danych*	

……

……

……**

……..……..……..

(czytelny podpis administratora danych)

*- w przypadku niepowołania należy wskazać inny punkt kontaktowy

**- w przypadku zgłoszeni przekazanego organowi nadzorczemu po upływie 72 godzin, administrator danych zobowiązany jest do złożenia wyjaśnień w przedmiocie przyczyn opóźnienia.

załącznik nr 13

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko/komórka organizacyjna	Zakres *(określenie, do jakich zbiorów dana osoba ma dostęp)*	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/Login w danym systemie informatycznym
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Załącznik nr 14

WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

L.p.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				
7.				

(wszystkie miejsca, pomieszczenia, pokoje, w których dokonuje się operacji na danych osobowych)
(S) - serwer, (K) - miejsce przechowywania kopii bezpieczeństwa, (P) – pomieszczenie, w którym przetwarza się dane osobowe, (AP) - archiwum zbiorów papierowych (KR) - kraty w oknach, (A) - alarm, (W) - wzmocnione drzwi, (B) - brak

nazwa jednostki organizacyjnej

Lista kontrolna zgodności z RODO

Zasady przetwarzania danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówka**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
1.	art. 5 ust. 1 lit. a	Przetwarzanie zgodnie z prawem i w sposób przejrzysty dla osoby, której dane dotyczą.	Wszystkie komunikaty dot. przetwarzania danych osobowych powinny być łatwo dostępne i zrozumiałe.	1. Czy przetwarzane w jednostce organizacyjnej dane osobowe przetwarzane są w sposób legalny?	
2.	art. 5 ust. 1 lit. b	Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami. Zbieranie danych w celach archiwalnych, badań naukowych, historycznych lub statystycznych nie jest uznawane za niezgodne z celem pierwotnym.	Cele przetwarzania danych osobowych na określa ustawa prawo o szkolnictwie wyższym. Jeżeli cel przetwarzania wykracza poza sferę obowiązków wynikających z przepisów, należy także zakomunikować inny cel zbierania danych.	2. Czy dane przetwarzane w jednostce organizacyjnej są przetwarzane w sposób rzetelny?	
3.	art. 5 ust. 1 lit. c	Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, dla których są przetwarzane (minimalizacja danych).	Ukształtowanie zakresu przetwarzania danych, w taki sposób. by zbierane były tylko dane niezbędne, które pozwolą na osiągnięcie zamierzonego celu.	3. Czy zakres przetwarzanych danych osobowych jest adekwatny do celu ich przetwarzania?	
4.	art. 5 ust. 1 lit. d	Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane, należy podjąć wszelkie rozsądne działania, aby dane	Dane zbierane w procesie przetwarzania powinny być zgodne z prawdą, pełne (kompletne) oraz powinny odpowiadać aktualnemu stanowi rzeczy. Należy	4. Czy zapewniono merytoryczną poprawność danych osobowych?	

		osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.	zadbać o merytoryczną poprawność zbieranych danych osobowych.		
5.	art. 5 ust. 1 lit. e	Dane należy przechowywać w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane.	Zasada ograniczenia przechowywania danych zabezpiecza osobę, której dane dotyczą, przed przetwarzaniem przez nieograniczony okres. Przechowywanie w celach archiwalnych, badań naukowych, historycznych lub celów statystycznych jest dozwolone.	5. Czy dane przetwarzane są przez czas niezbędny do realizacji celu?	
6.	art. 5 ust. 1 lit. f	Dane powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych w tym ochronę danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.	Zapewnienie bezpieczeństwa polega na wdrożeniu odpowiednich środków technicznych i organizacyjnych adekwatnych do określonego poziomu ryzyka.	6. Czy dane osobowe są zabezpieczone i przechowywane w sposób adekwatny do ryzyka przetwarzania danych?	
7.	art. 5 ust. 2	Administrator danych jest odpowiedzialny za przestrzeganie przepisów dotyczących zasad przetwarzania danych, musi być w stanie wykazać ich przestrzeganie („rozliczalność”).	Przez zapewnienie rozliczalności należy rozumieć obowiązek administratora danych do przestrzegania zasad ochrony danych osobowych i umiejętność wykazania przestrzegania tych przepisów – pomocny w tym jest rejestr czynności przetwarzania.	7. Czy w jednostce organizacyjnej wykonuje się nałożone na nią obowiązki wynikające z przepisów regulujących ochronę danych osobowych?	

Przesłanki legalności przetwarzania danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówka**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
8.	art. 6 ust. 1 lit. a	Przetwarzanie danych osobowych jest dopuszczalne, gdy: osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.	Należy potrafić udowodnić, iż jednostka pozyskała stosowne zgody na przetwarzanie danych osobowych. Np. w przypadku procesu rekrutacji na studia zgoda pobierana jest od kandydata w systemie i za pomocą formularza papierowego. Zgodę należy zbierać np. od studentów w przypadku, gdy ich dane będą przetwarzane w celu innym niż związane z tokiem studiów z wyłączeniem marketingu/ofert oferowanych przez jednostkę. Zgoda wymagana jest zawsze od osób, które chcą wziąć udział np. w konkursie, seminarium, konferencji itp. Dowodem udzielenia zgody może być np.: − podpis osoby pod klauzulą zgody, − mail z klauzulą zgody w treści, − checkbox z zaznaczeniem zgody. Klauzula zgody musi mieć wyraźnie określony cel lub cele. Zgodnie z przepisami RODO konieczne jest pozyskanie odrębnej zgody na każdy z celów. Należy zachować treść udzielonych zgód.	8. Jeżeli podstawą prawną przetwarzania danych osobowych jest zgoda osoby której dane dotyczą, to czy jest ona udokumentowana? 9. Czy klauzula zgody ma precyzyjnie określone cele? 10. Czy zachowana jest treść udzielonych zgód z przypisaniem do osoby, która udzieliła zgody?	
9.	art. 6 ust. 1 lit. b	Przetwarzanie danych jest dopuszczalne, gdy przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą.	Należy posiadać lub potrafić wskazać miejsce przechowywania zawartej umowy z osobą, której dane dotyczą.	11. Jeżeli przetwarzanie odbywa się na podstawie umowy z osobą, której dane dotyczą, to czy taka umowa jest	

				przechowywana?	
10.	art. 6 ust. 1 lit. c	Przetwarzanie danych jest dopuszczalne, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.	Należy umieć wykazać podstawę prawną przetwarzania danych osobowych np.: – ustawa Prawo o szkolnictwie wyższym, – ustawa Kodeks pracy.	12. Gdy przetwarzanie odbywa się na podstawie przepisu prawa, to czy wskazano podstawę prawną?	
11.	art. 6 ust. 1 lit. d	Przetwarzanie danych osobowych jest dopuszczalne, gdy przetwarzanie jest	Żywotne interesy to interesy o dużym znaczeniu dla osoby, której dane	13. Czy w jednostce organizacyjnej	

Obowiązek informacyjny

Lp.	Przepis	Zagadnienie	Wskazówki	Pytania kontrolne	Czy jednostka spełnia wymaganie T/N/Uwagi
14.	art. 13 ust. 1	Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych	W celu spełnienia obowiązku informacyjnego należy poinformować osobę, której dane dotyczą o:	15. Czy jednostka organizacyjna wykonuje obowiązek informacyjny?	

		podaje jej wszystkie następujące informacje: a) swoją tożsamość i dane kontaktowe oraz gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych osobowych oraz podstawę prawną przetwarzania; c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania; d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.	− nazwie administratora danych, adresie i danych kontaktowych, − danych kontaktowych inspektora ochrony danych osobowych, − celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania (np. zgoda, przepis prawa), − jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f (do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią) – należy poinformować o prawnie uzasadnionych interesach realizowanych przez administratora, − odbiorcach danych lub kategoriach odbiorców danych, jeżeli istnieją, − gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, − okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu, − prawie żądania od administratora dostępu do danych osobowych osoby, której dane dotyczą, − prawie do cofnięcia zgody w dowolnym momencie (cofnięcie zgody w przypadku studentów odbywających tok studiów cofnięcie zgody nie jest możliwe, z uwagi na	16. Czy stosowane klauzule informacyjne są zgodne z przepisami określonymi w RODO? 17. Czy obowiązek informacyjny jest spełniony przed rozpoczęciem przetwarzania danych osobowych?	
	art. 13 ust. 2	Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych			

			to, że dane przetwarzane są na		
		osobowych administrator podaje osobie, której one dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania: a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu; b) informacje o prawie żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; d) informacje o prawie wniesienia skargi do organu nadzorczego; e) informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jet zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;	podstawie przepisów prawa), − prawie wniesienia skargi do organu nadzorczego, − obowiązku ustawowym lub umownym lub warunku zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ew. konsekwencje niepodania danych, − (gdy ma to zastosowanie) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu. W przypadku zbierania danych, nie od osoby, której dane dotyczą (art. 14 ust. 2 lit. f), należy poinformować tę osobę dodatkowo o: − źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. **Obowiązek informacyjny należy spełnić przed rozpoczęciem zbierania danych osobowych.** Obowiązek informacyjny można spełnić przez wprowadzenie tzw. klauzul informacyjnych. Klauzula informacyjna może przyjąć postać informacji np.: − zamieszczonej w formularzu, − zamieszczonej w regulaminie, − zamieszczonej w mailu,		
		f) informacje o zautomatyzowanym			

		podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.	− zamieszczonej na stronie internetowej.		

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
15.	art. 25 ust. 1	Uwzględnianie ochrony danych w fazie projektowania.	Zgodnie z tą zasadą należy uwzględnić odpowiednie środki techniczne i organizacyjne, które pomogą w skutecznej realizacji zasad ochrony danych osobowych. Należy posłużyć się zasadą minimalizacji danych oraz wdrożyć odpowiednie ustawienia domyślne dotyczące prywatności osób, których dane dotyczą.	18. Czy przetwarzanie danych osobowych odbywa się w sposób bezpieczny?	
16.	art. 25 ust. 2	Domyślana ochrona danych.	Rezultatem domyślnej ochrony danych jest doprowadzenie do sytuacji, w której domyślnie będą przetwarzane tylko te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania.	19. Czy jednostka organizacyjna przetwarza tylko dane niezbędne do realizacji celu, w jakim zbiera dane osobowe?	

Powierzenie przetwarzania danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
17.	art. 28	Przetwarzanie danych osobowych odbywa się w imieniu administratora z wykorzystaniem usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.	W przypadku powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu należy z tym podmiotem zawrzeć stosowną umowę powierzenia przetwarzania lub gdy przetwarzanie odbywa się na podstawie już zawartej umowy powierzenia należy dokonać sprawdzenia treści pod kątem nowych przepisów. Dowodem na spełnienie obowiązku wynikającego z art. 28 jest posiadanie umów powierzenia przetwarzania danych lub aneksów. Umowa powierzenia przetwarzania danych osobowych w szczególności powinna obejmować następujące elementy: – przedmiot i czas trwania przetwarzania, – charakter i cel przetwarzania, – rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, – obowiązki i prawa administratora danych, – wskazanie, że przetwarzanie odbywa się wyłącznie na udokumentowane polecenie administratora, – zapewnienie, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania uzyskanych danych w tajemnicy,	20. Czy w jednostce organizacyjnej zidentyfikowano podmioty zewnętrzne, z którymi podpisano lub należy podpisać umowę powierzenia przetwarzania danych osobowych? 21. Czy powierzenie przetwarzania danych osobowych ma formę pisemną? 22. Czy umowa powierzenia przetwarzania zawiera wszystkie obligatoryjne elementy wynikające z RODO?	

			– informacje o podjętych środkach bezpieczeństwa danych, – zobowiązanie podmiotu przetwarzającego do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego, – pomoc administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, – pomoc administratorowi danych w wywiązaniu się z obowiązku zapewnienia bezpieczeństwa danych, zgłaszania naruszeń ochrony danych organowi nadzorczemu, zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków przetwarzania danych osobowych, – zobowiązanie do usunięcia lub zwrotu administratorowi danych wszelkich danych osobowych oraz usunięcia wszelkich ich istniejących kopii, – zobowiązanie do udostępnienia administratorowi danych wszelkich informacji niezbędnych do spełnienia obowiązków określonych w art. 28 RODO oraz umożliwienie administratorowi danych lub upoważnionemu przez administratora danych audytorowi przeprowadzenia audytów czy inspekcji.		

Rejestrowanie czynności przetwarzania					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
18.	art. 30	Prowadzenie rejestru czynności przetwarzania danych osobowych. Rejestr może być prowadzony w wersji elektronicznej lub papierowej.	Rejestr czynności przetwarzania jest narzędziem niezbędnym przy obowiązku wykazania rozliczalności przetwarzania danych osobowych. Rejestr taki obowiązkowo powinien uwzględniać informacje takie jak: – dane administratora w tym adres, – cel przetwarzania, – opis kategorii osób, których dane są przetwarzane, oraz kategorii danych osobowych – kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, – gdy ma to zastosowanie, informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, – jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych, – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Rejestr czynności przetwarzania będzie także pomocny przy spełnieniu obowiązku dotyczącego dokonania oceny skutków dla ochrony danych osobowych.	23. Czy w jednostce organizacyjnej zidentyfikowano procesy przetwarzania danych osobowych? 24. Czy w jednostce organizacyjnej ustalono kategorie osób, których dane dotyczą? 25. Czy w jednostce organizacyjnej ustalono kategorie podmiotów, którym dane będą przekazywane?	

Bezpieczeństwo danych osobowych					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
19.	art. 32	Administrator i podmiot przetwarzający zobowiązani są do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.	**Zabezpieczenia osobowe:** – świadomość odpowiedzialności karnej za naruszenie ochrony danych osobowych, – zachowanie ostrożności przy udzielaniu informacji przez telefon poza ZUT, – zachowanie ostrożności przy udzielaniu informacji osobom nieuprawnionym, – zgłaszanie incydentów naruszenia ochrony danych osobowych, – zakaz przekazywania haseł dostępu do systemu, – blokowanie dostępu do systemu podczas opuszczenia stanowiska pracy, – ustawienie monitorów w sposób uniemożliwiający odczyt wyświetlania danych, – zamykanie pomieszczeń po zakończeniu pracy, – niepozostawianie dokumentów zawierających dane osobowe po zakończeniu pracy, – niszczenie dokumentów przy pomocy niszczarki.	26. Czy pracownicy zostali zapoznani z polityką bezpieczeństwa ochrony danych osobowych? 27. Czy pracownicy posiadają upoważnienia do przetwarzania danych osobowych? 28. Czy pracownicy zachowują ostrożność przy przekazywaniu danych osobowych przez telefon poza Uniwersytet Warszawski? 29. Czy pracownicy pozwalają na przebywanie w obszarze przetwarzania danych osób nieuprawnionych bez nadzoru? 30. Czy pracownicy niszczą dokumenty papierowe zawierające dane osobowe przy użyciu niszczarki dokumentów? 31. Czy pracownik posiada dostęp do programów przetwarzających dane osobowe jedynie przez zalogowanie się przy użyciu identyfikatora oraz hasła? 32. Czy pracownicy są świadomi konieczności zgłaszania incydentów naruszenia ochrony danych osobowych?	

				33. Czy pracownicy mają świadomość, iż dokumenty	
				papierowe należy przenosić w sposób uniemożliwiający ich widoczność? 34. Czy pracownicy, przenosząc dane na nośnikach danych, szyfrują ich zawartość?	
			Zabezpieczenia organizacyjne: − sprawdzenie zgodności przetwarzania danych osobowych z przepisami RODO, − wdrożenie dokumentacji ochrony danych osobowych w jednostce, − wydanie upoważnień dla pracowników posiadających dostęp do danych osobowych, − zapewnienie szkoleń z ochrony danych osobowych, − prowadzenie ewidencji osób upoważnionych, − prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, − oświadczenia o zachowaniu poufności dla osób sprzątających, wolontariuszy itp., − określenie obszarów przetwarzania danych osobowych,	Czy powołano Lokalnego Administratora Systemów 35. Informatycznych . 36. Czy jednostka organizacyjna prowadzi ewidencję osób upoważnionych? 37. Czy pracownicy zostali zapoznani z przepisami regulującymi ochronę danych osobowych? 38. Czy w jednostce organizacyjnej określono obszary przetwarzania danych osobowych? 39. Czy w jednostce organizacyjnej wdrożono procedurę przyznawania pracownikom uprawnień do przetwarzania danych osobowych w systemach informatycznych?	

			− wdrożenie procedury przyznawania uprawnień użytkownikom systemów informatycznych, − sprawdzenie czy dokumenty przechowywane są w sposób uniemożliwiający podgląd przez osoby nieuprawnione.		
			Zabezpieczenia fizyczne: − szafy zamykane na klucz, − drzwi do pomieszczeń zamykane na klucz zwykłe lub wzmocnione lub ognioodporne, − sejfy, kasy pancerne, − zabezpieczenia okien, − system alarmowy, − system kontroli dostępu, − nadzór służby ochrony, − system przeciwpożarowy i/lub gaśnice wolnostojące.	40. Czy dane osobowe zabezpieczone są w sposób fizyczny? 41. Czy kopie zapasowe/archiwalne, na których umieszczone są dane osobowe przechowywane są w odrębnym pomieszczeniu? 42. Czy obszar przetwarzania danych osobowych zabezpieczony jest przed dostępem osób nieuprawnionych?	
			Zabezpieczenia informatyczne: − sprawdzenie, czy w systemie możliwe jest odnotowanie źródła pochodzenia danych osobowych, daty i zakresu udostępnienia danych osobowych, sprzeciwu osoby, której dane dotyczą, − sprawdzenie, czy system pozwala na tworzenie i drukowanie raportów zawierających odnotowane informacje o osobie, której dane dotyczą,	43. Czy programy przetwarzające dane osobowe automatycznie odnotowują: datę pierwszego wprowadzenia danych do systemu oraz identyfikator użytkownika wprowadzającego dane osobowe do systemu? 44. Czy system umożliwia tworzenie raportów zawierających informacje o	

			− podłączenia serwera do UPS, − klimatyzacja w serwerowni, − systemy operacyjne lub programy zapewniają rejestrację dostępu do danych osobowych, − zapewnienie szyfrowania połączenia przez Internet (SSL, VPN), − stosowanie oprogramowania antywirusowego, − firewall do ochrony dostępu do sieci komputerowej, − aktualizacja oprogramowania, − określenie praw dostępu do danych przechowywanych w systemach informatycznych, − odrębny identyfikator dla każdego użytkownika, − wykonywanie kopii bezpieczeństwa.	osobie, której dane dotyczą, w przystępnej formie? 45. Czy systemy informatyczne zapewniają rejestrację dostępu do danych osobowych? 46. Czy użyto Firewall do ochrony dostępu do sieci komputerowej? 47. Czy serwerownia wyposażona jest w klimatyzację? 48. Czy użyto systemu IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej? 49. Czy stosowany jest NAT? 50. Czy systemy operacyjne i przeglądarki mają instalowane aktualizacje? 51. Czy zainstalowano wygaszacze ekranów chronione hasłem na stacjach roboczych? 52. Czy nośniki informacji podłączone do stacji roboczej sprawdzane są oprogramowaniem antywirusowym? 53. Czy pracownik, czasowo opuszczając stanowisko pracy, wylogowuje się z systemu? 54. Czy ekrany monitorów zostały ustawione w sposób uniemożliwiający	

				wgląd przez osoby nieupoważnione?	

Ocena skutków dla ochrony danych				
Przepis	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
art. 35	Dokonanie oceny skutków dla ochrony danych osobowych. Przed rozpoczęciem przetwarzania danych dokonuje się oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, gdy przetwarzanie danych może powodować wysokie ryzyko naruszenia praw lub wolności osób, której dane dotyczą.	Dokonanie oceny skutków dla ochrony danych osobowych jest niezbędne w celu ustalenia procesu przetwarzania danych osobowych oraz podjęcia określonych środków ochrony danych adekwatnych do poziomu ryzyka. Ocena skutków dla ochrony danych powinna polegać na: – ustaleniu procesu/ów przetwarzania danych (np. proces rekrutacji), – ustaleniu odpowiedzialności za proces, – podjęciu decyzji o konieczności wykonania oceny skutków, – uzasadnieniu decyzji, – wskazaniu interesariuszy (np. pracownicy, studenci itp.), – podjęciu konsultacji z Inspektorem Ochrony Danych, – określeniu planowanego terminu i sposobu realizacji praw i obowiązków osób, których dane dotyczą, – identyfikacji i opisie aktywów, – opracowaniu przepływu danych, – określeniu wymagań w zakresie ochrony prywatności,	55. Czy w jednostce organizacyjnej ustalono procesy przetwarzania danych osobowych? 56. Czy w jednostce organizacyjnej dokonano analizy ryzyka procesów przetwarzania danych osobowych? 57. Czy w jednostce organizacyjnej wykonano ocenę skutków dla ochrony danych osobowych?	

			− określeniu wymogów ogólnych w zakresie bezpieczeństwa danych, − wybraniu odpowiedniej metody szacowania ryzyka, − dokonaniu klasyfikacji danych, − określeniu zasad postępowania z danymi, − identyfikacji zagrożeń, − wyznaczeniu wartości ryzyka, − opracowaniu planu postępowania z ryzykiem, − określeniu poziomu ryzyka szczątkowego, − ustaleniu sposobu przeglądu i monitorowania ryzyka, − opracowaniu raportu z oceny skutków dla ochrony danych.		

Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej					
Lp.	**Przepis**	**Zagadnienie**	**Wskazówki**	**Pytania kontrolne**	**Czy jednostka spełnia wymaganie T/N/Uwagi**
21.	Rozdział V RODO	Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje, gdy administrator i podmiot przetwarzający spełnią warunki określone w Rozdziale V.	Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko, gdy spełnione zostaną warunki i unormowania wynikające z RODO przy zapewnieniu, że nie został naruszony stopień ochrony osób fizycznych wyrażony w RODO. Podstawowym warunkiem przekazania danych osobowych do państwa trzeciego jest stwierdzenie przez Komisję Europejską, że państwo trzecie lub dana organizacja międzynarodowa zapewniają	58. Czy przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej odbywa się w sposób legalny?	
			odpowiedni stopień ochrony danych osobowych. Stwierdzenie odpowiedniego stopnia ochrony następuje w postaci aktu wykonawczego zawierającego decyzję Komisji Europejskiej. Przekazanie danych osobowych do państw trzecich lub organizacji międzynarodowych, w odniesieniu do których podjęta została decyzja o zapewnieniu odpowiedniego stopnia ochrony danych nie wymaga specjalnego zezwoleni		