ZARZĄDZENIE NR 75/2018

REKTORA UNIWERSYTETU SZCZECIŃSKIEGO

z dnia 1 października 2018 r.

w sprawie wprowadzenia Polityki ochrony danych osobowych
w Uniwersytecie Szczecińskim

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r., poz. 1668) w związku z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000) oraz ogólnym rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.) zarządza się, co następuje:

§ 1.

1. W Uniwersytecie Szczecińskim przetwarzane są dane osobowe w rozumieniu ustawy o ochronie danych osobowych i ogólnego rozporządzenia o ochronie danych osobowych. Dane osobowe przetwarzane są wyłącznie dla celów związanych z działalnością Uczelni.
2. Poprzez przetwarzanie danych osobowych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, a zwłaszcza te, które wykonuje się w systemach informatycznych takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
3. Przetwarzanie danych osobowych może odbywać się w systemie informatycznym oraz poza systemem informatycznym w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 2.

1. Administratorem danych osobowych (zwanym dalej ADO) w Uniwersytecie Szczecińskim w rozumieniu ustawy o ochronie danych osobowych jest Rektor.
2. Administrator danych osobowych przetwarzający dane zachowuje szczególną staranność w celu ochrony interesów osób, których te dane dotyczą, a w szczególności zapewnia:

1) przetwarzanie danych zgodnie z prawem, przede wszystkim ustawą Prawo o szkolnictwie wyższym,
2) zbieranie danych dla celów oznaczonych, zgodnych z prawem, i nie poddawanie ich dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem punktu 3,
3) merytoryczną poprawność i adekwatność w stosunku do celów, w jakich są przetwarzane,
4) przechowywanie w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

3. Przetwarzanie danych w celu innym niż zostały zebrane jest dopuszczalne, jeśli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych.

§ 3.

1. Rektor powierza wykonywanie obowiązków wynikających z ustawy o ochronie danych osobowych lokalnym administratorom danych osobowych, zwanym dalej LADO, którymi są:

1) **dziekani** – w zakresie podległych pracowników, doktorantów, studentów słuchaczy studiów podyplomowych i uczestników kursów dokształcających, jak i osób uczestniczących w innych formach kształcenia prowadzonych na wydziale,
2) **dyrektorzy i kierownicy jednostek międzywydziałowych i ogólnouczelnianych** – w zakresie podległych pracowników i studentów, słuchaczy studiów podyplomowych i uczestników kursów dokształcających,
3) **prorektorzy** – w zakresie pracowników podległych im komórek organizacyjnych oraz wykonywania zadań określonych w Regulaminie organizacyjnym administracji US.
4) **kanclerz** – w zakresie pracowników (wszystkich jednostek podległych kanclerzowi zgodnie z Regulaminem organizacyjnym administracji).

§ 4.

1. Rektor powołuje inspektora danych osobowych oraz administratora systemów informatycznych.

2. Obowiązek prowadzenia ewidencji wszystkich osób pełniących obowiązki lokalnych administratorów danych osobowych oraz innych osób, którym powierzone zostało wykonywanie obowiązków związanych z ochroną danych osobowych powierza się inspektorowi danych osobowych.

3. Sprawowanie funkcji kontrolnych w zakresie ochrony danych osobowych w Uniwersytecie Szczecińskim powierza się prorektorowi ds. nauki i współpracy międzynarodowej.

§ 5.

1. Pracownicy, doktoranci, studenci i inne osoby, których dane osobowe są przetwarzane w jednostkach organizacyjnych Uniwersytetu Szczecińskiego, mają prawo do ochrony danych osobowych, do kontroli przetwarzania tych danych oraz do ich uaktualnienia, poprawienia, jak też do uzyskania wszystkich informacji o przysługujących im prawach.
2. Osoby, które zostały upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania w tajemnicy tych danych oraz sposobu ich zabezpieczenia.
3. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać również zakres odpowiedzialności tej osoby za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym uprawnieniem lub pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

§ 6.

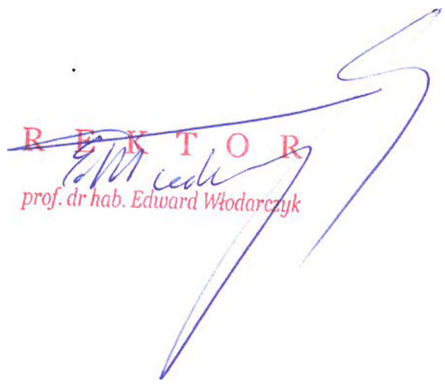
Wprowadza się Politykę ochrony danych osobowych Uniwersytetu Szczecińskiego stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 7.

Traci moc zarządzenie nr 30/2018 Rektora Uniwersytetu Szczecińskiego z dnia 25 maja 2018r. w sprawie wprowadzenia Polityki ochrony danych osobowych w Uniwersytecie Szczecińskim

§ 8.

Zarządzenie wchodzi w życie z dniem podpisania.



załącznik do
zarządzenia nr 75/2018
Rektora Uniwersytetu Szczecińskiego

POLITYKA OCHRONY DANYCH OSOBOWYCH

W UNIWERSYTECIE SZCZECIŃSKIM

§ 1.

Dane osobowe w Uniwersytecie Szczecińskim przetwarzane są w celu realizacji obowiązków oraz uprawnień określonych przepisami prawa, w szczególności statutowych celów szkoły wyższej. W szczególności dane osobowe przetwarza się:

1) dla zabezpieczenia prawidłowego toku realizacji zadań dydaktycznych, naukowych i organizacyjnych Uniwersytetu Szczecińskiego wynikających z przepisów ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (tekst jedn. Dz. U. z 2017 r. poz. 2183, ze zm.);
2) w celu zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni, polityki personalnej oraz bieżącej obsługi pracy, a także innych stosunków pracy nawiązywanych przez Uczelnię działającą jako pracodawca w rozumieniu art. 3 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn. z 2017 r., poz. 108) lub strona innych stosunków zatrudnienia;
3) dla realizacji innych celów i zadań Uniwersytetu Szczecińskiego, z poszanowaniem praw i wolności osób powierzających Uczelni swoje dane.

§ 2.

1. Politykę bezpieczeństwa w zakresie ochrony danych osobowych w Uniwersytecie Szczecińskim stosuje się do danych osobowych przetwarzanych w:

1) zbiorach danych tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach, archiwaliach i innych zbiorach ewidencyjnych;
2) systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych. Politykę ochrony danych osobowych stosuje się w szczególności do: baz danych, zbiorów plików, poczty elektronicznej, zawartości stron www, skanów dokumentów i dokumentów elektronicznych, archiwaliów elektronicznych.

2. Podstawowe zbiory danych osobowych w Uniwersytecie Szczecińskim, to zbiory obejmujące dane: kandydatów na studia, studentów, doktorantów, absolwentów, kandydatów na pracowników, pracowników, byłych pracowników, członków związków i organizacji, stron umów cywilnoprawnych, kontrahentów, uczestników studiów podyplomowych, uczestników projektów europejskich realizowanych, uczestników kursów, szkoleń i konferencji, osób korzystających z Biblioteki Głównej Uniwersytetu Szczecińskiego, osób prowadzących postępowania o uzyskanie stopnia naukowego lub o nadanie tytułu naukowego, osób otrzymujących tytuł doktora honoris causa Uniwersytetu Szczecińskiego,

osób wobec których przeprowadzone zostało postępowanie odnowienia doktoratu, i którym przyznano Medal Uniwersytetu Szczecińskiego.

§ 3.

1. Realizując Politykę danych osobowych Uniwersytet Szczeciński wyznacza osoby odpowiedzialne za bieżącą realizację postanowień polityki na terenie Uczelni oraz jej jednostek.

   Wyznaczeni zostają w szczególności:

   1) inspektor ochrony danych,
   2) administrator bezpieczeństw informatycznego,
   3) lokalni administratorzy danych osobowych, odpowiedzialni za nadzór nad przetwarzaniem danych osobowych w jednostkach podległych (kierownicy podstawowych jednostek organizacyjnych, kierownicy jednostek ogólnouczelnianych i międzywydziałowych, kierownicy poszczególnych pionów administracji centralnej zgodnie ze schematem organizacyjnym).

2. Rejestr osób, o których mowa w ust. 1 pkt. 1, 2,3 prowadzi inspektor ochrony danych.

§ 4.

1. Uniwersytet Szczeciński realizując politykę ochrony danych osobowych spełnia wymagane obowiązki informacyjne wobec osób, których dane dotyczą oraz zachowuje szczególną staranność w celu ochrony ich interesów, a szczególności zapewnia, aby dane te były:

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

przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

2. Przetwarzanie danych osobowych w Uniwersytecie Szczecińskim prowadzone jest zgodnie z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:

1) *osoba*, której dane dotyczą wyraziła zgodę na *przetwarzanie* swoich *danych osobowych* w jednym lub większej liczbie określonych celów;

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.

Akapit pierwszy pkt.6 nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

3. Obowiązek informacyjny. Uczelnia zapewnia rzetelność i przejrzystość przetwarzania danych osobowych poprzez informowanie osób, których dane dotyczą, o wykorzystywaniu ich danych osobowych (prowadzeniu operacji przetwarzania) poprzez klauzule informacyjne.

§ 5.

Upoważnienia

1. Upoważnienia do przetwarzania danych osobowych nadawane są pracownikom Uniwersytetu Szczecińskiego w zakresie powierzonych im obowiązków.
2. Kierownik jednostki wypełnia i podpisuje wniosek (załącznik nr 1 do niniejszej Polityki) o nadanie upoważnienia do przetwarzania danych osobowych w Uniwersytecie Szczecińskim.
3. Kierownik jednostki przekazuje wniosek wraz z podpisanym przez pracownika oświadczeniem (załącznik nr 2 do niniejszej Polityki) do LABI.
4. LABI po podpisaniu upoważnienia (załącznik nr 3 do niniejszej Polityki) przekazuje upoważnienie do Działu Spraw Osobowych w celu umieszczenia jej w aktach osobowych upoważnionego pracownika oraz w ewidencji osób upoważnionych, a kopię upoważnienia do inspektora ochrony danych.
5. Upoważnienia do przetwarzania danych osobowych udzielne na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. z 2016 r. poz. 922 ze zm.) zachowują moc w dniu wejścia w życie ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. oraz rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 26 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.
7. Ewidencja osób, którym zostały nadane upoważnienia do przetwarzania danych osobowych prowadzona jest, w poszczególnych jednostkach organizacyjnych, przez LABI lub osoby przez nich upoważnione. (załącznik nr 4 do niniejszej Polityki).
8. Podmioty i organy, którym przepisy szczegółowe umożliwiają dostęp do przetwarzania danych osobowych na podstawie odrębnych upoważnień, zobowiązane są do złożenia pisemnego wniosku i wskazania przepisu szczególnego dającego im takie prawo lub do wskazania przepisów umożliwiających wykorzystanie innej drogi dostępu do danych osobowych.

§ 6.

Zabezpieczenie danych osobowych

1. Uniwersytet Szczeciński realizując politykę ochrony danych osobowych stosuje odpowiednie środki fizyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w innych sposób przechowywanych.

2. Uwzględniając kategorie przetwarzanych danych oraz ich zagrożenia, Uniwersytet Szczeciński stosuje podstawowy, podwyższony lub wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

§ 7.

Ogólne zasady polityki bezpieczeństwa

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

1. W budynkach, pomieszczeniach i częściach pomieszczeń tworzących obszar Uniwersytetu Szczecińskiego, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę przetwarzania i ochrony tych danych.
2. Osoby nie posiadające upoważnienia do przetwarzania danych osobowych, a mające interes prawny lub faktyczny w uzyskaniu dostępu do danych oraz osoby wykonujące inne czynności niezwiązane z dostępem do danych osobowych, w szczególności takie, jak: sprzątanie, remonty, ochrona budynku, mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wyłącznie w obecności upoważnionego pracownika Uniwersytetu Szczecińskiego lub na podstawie wydanego przez administratora danych osobowych dokumentu zezwalającego i określającego warunki przebywania w miejscach przetwarzania danych osobowych. Zezwolenie na przebywanie w w/w miejscach i warunki przebywania mogą wynikać z umowy z podmiotem wykonującym określone usługi dla Uniwersytetu Szczecińskiego.

3. Obszar, w którym przetwarzane są dane osobowe obejmuje miejsca, w których wykonuje się wszelkie operacje na danych osobowych, jak również miejsca, w których przechowuje się wszelkie nośniki informacji zawierające dane osobowe (m.in. szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, w których dane osobowe przetwarzane są na bieżąco).
4. Do obszaru przetwarzania danych należy również zaliczyć pomieszczenia, w których są składowane uszkodzone nośniki komputerowe (taśmy, dyski, komputery, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami zawierającymi dane osobowe.
5. Do obszarów przetwarzania danych osobowych administrator może zaliczyć miejsca wykorzystywane do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych.
6. Pomieszczenia, w których przetwarzane są dane osobowe należy zabezpieczyć przed dostępem osób nieuprawnionych na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.
7. Zabrania się przetwarzania danych osobowych poza obszarem ich przetwarzania (na przenośnych urządzeniach komputerowych). Zabrania się również wynoszenia danych osobowych poza obszar ich przetwarzania na nośnikach elektronicznych.
8. Postanowienia, o którym mowa powyżej nie mają zastosowania w przypadku procedur określonych w innych przepisach.
9. Prowadzenie ewidencji danych dotyczących wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, należy do obowiązków LABI.
10. Ewidencja, o której mowa w ust. 9 prowadzona jest na formularzu, którego wzór stanowi załącznik nr 4 do niniejszej Polityki.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych:

1. Prowadzenie ewidencji danych dotyczących nazwy zbiorów danych oraz stosownych nazw używanych do przetwarzania programów komputerowych należy do obowiązków LABI.
2. W ewidencji danych dotyczących nazwy danych zbiorów danych podawane są informacje z zakresu dokładnej lokalizacji miejsca (budynek, nazwa komputera lub innego urządzenia), w którym znajdują się zbiory danych osobowych. Ewidencja prowadzona jest na formularzu, którego wzór stanowi załącznik nr 5 do niniejszej Polityki.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania miedzy nimi:

1. Każdy z systemów informatycznych funkcjonujących na Uniwersytecie Szczecińskim powinien posiadać dokumentację techniczną dostarczoną przez jego autorów.
2. Dokumentacja, o której mowa w ust. 1 powinna spełniać wymagania dotyczące struktur baz danych oraz funkcjonalności zarządzających nimi aplikacji zgodnie z ustawą o ochronie danych osobowych.
3. Nowe systemy informatyczne powinny spełnić wymaganie, o którym mowa w ust. 2 przed dopuszczeniem ich do użytkowania.

4. Każdy zidentyfikowany zbiór danych powinien posiadać opis struktury zbioru i zakres informacji gromadzonych w tym zbiorze.
5. Opis poszczególnych pól informacyjnych w strukturze zbioru danych powinien jednoznacznie wskazywać, jakie kategorie są w nich przechowywane.
6. W przypadkach, gdy nie jest możliwa jednoznaczna interpretacja zawartości pola, jego opis powinien wskazywać nie tylko na kategorie danych, ale również na format ich zapisu i określać w danym kontekście ich znaczenie.

Sposób przepływu danych pomiędzy poszczególnymi systemami:

1. Sposób przepływu danych pomiędzy poszczególnymi systemami powinien zostać opisany w dokumentacji technicznej tych systemów, lub dokumentacji technicznej połączenia systemów.
2. Dokumentacja techniczna systemów powinna zawierać również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych) lub za pomocą teletransmisji wykonywanych w określonych odstępach czasu.
3. W bazach danych, które zlokalizowane są w różnych obiektach Uniwersytetu Szczecińskiego i zawierają różne zakresy danych osobowych, należy wskazać zakres przesyłanych danych, podmiotu lub kategorii podmiotów, do których dane są przekazywane oraz ogólne informacje na temat sposobu przesyłania danych. Sposób przesyłania danych np. przez Internet, pocztą elektroniczną, innym sposobem, powinien decydować o rodzaju narzędzi niezbędnych do zapewnienia bezpieczeństwa podczas ich przesyłania.

W oparciu o zbiory danych przeprowadzana jest analiza ryzyka przetwarzania danych osobowych.

Do środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zalicz się m.in:

1. Użytkownicy systemów informatycznych Uniwersytetu Szczecińskiego powinni zostać przeszkoleni przed rozpoczęciem pracy w systemie.
2. Identyfikatory i hasła dostępu do systemów informatycznych przekazywane są użytkownikom w formie zapewniającej poufność.
3. Systemy informatyczne użytkowane przez Uniwersytet Szczecinski powinny być wyposażone w mechanizmy zapewniające:
    a) ochronę dostępu do aplikacji użytkowych,
    b) analizę poprawności przesyłanych danych,
    c) analizę modyfikacji przesyłanych danych,
    d) kontrolę dostępu do aplikacji użytkowych,
    e) kontrolę błędów wprowadzanych danych.

Dokumentacja przetwarzania danych. Prowadzona jest dokumentacja czynności związanych z przetwarzaniem danych osobowych, w tym w szczególności:

f) jakie dane zostały pozyskane i na jakiej podstawie prawnej są przetwarzane,
g) w jaki sposób zostały spełnione obowiązki informacyjne,
h) komu i w jakich okolicznościach daną mogą być udostępnione,

i) w jaki sposób raportowane są incydenty związane z naruszeniem ochrony danych,
j) wewnętrzny rejestr czynności przetwarzania danych osobowych, w których określone są zakres przetwarzania danych, cele przetwarzania, kategorie osób, których dane dotyczą, środki bezpieczeństwa (wzór załącznik nr 6 do niniejszej Polityki).

Prowadzony jest rejestr czynności przetwarzania danych osobowych.
W rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz *dane* kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora *ochrony danych*;
b) cele *przetwarzania*;
c) opis kategorii *osób*, których *dane* dotyczą, oraz kategorii *danych osobowych*;
d) kategorie odbiorców, którym *dane osobowe* zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania *danych osobowych* do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii *danych*;
g) jeżeli jest to możliwe, *ogólny* opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

§ 8.

Privacy by design – zasada domyślnej ochrony danych

Dane osobowe przetwarzane z poszanowaniem polityki prywatności osób, których dane dotyczą. Ochrona prywatności brana jest pod uwagę i stosowana w praktyce przy przyprowadzeniu wszelkich projektów i działań tak w sferze publicznej, jak i prywatnej. Uwzględnienie ochrony dany w fazie projektowania ma z zasady umożliwić włączenie ochrony prywatności w samo tworzenie projektu, działanie jego składników oraz w zarządzanie technologiami informacyjnymi i systemami przez cały cykl życia informacji. W przypadku systemów teleinformatycznych oznacza to wbudowanie w określony system, oraz poszczególne procesy przetwarzania, które system obsługuje o np. poprzez jak najszybszą pseudonimizację danych czy też umożliwienie osobie, której dane dotyczą monitorowanie przetwarzania danych.

Privacy by defaut – ocena skutków dla ochrony danych

Ocena skutków dla ochrony danych powinna obejmować planowane operacje i cele przetwarzania, zabezpieczenia i mechanizmy mające minimalizować ryzyko. Proces oceny skutków przetwarzania prowadzi do opisania przetwarzania danych, oceny niezbędności i proporcjonalności, ma również przyczynić się do właściwego zarządzania ryzykami wynikającymi z przetwarzania danych. Ocena przeprowadzana jest w sytuacjach, w których

występuje wysokie ryzyko naruszenia prywatności osób, których dane dotyczą, np. w sytuacji:

1) gdy działania na danych wykonywane są przy użyciu nowych technologii,
2) użycia zautomatyzowanych procesów przetwarzania danych, w tym profilowania;
3) przetwarzania na dużą skalę szczególnych kategorii danych np. danych wrażliwych takich jak dane na temat stanu zdrowia.

§ 9.

Bezpieczeństwo danych przetwarzanych w sposób tradycyjny

1. Zgodnie z ustawą ochronie danych osobowych zbiory danych osobowych przetwarzanych w sposób tradycyjny (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne) również podlegają ochronie.
2. Uniwersytet Szczeciński prowadzi ewidencję budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w sposób tradycyjny. Obowiązek prowadzenia i aktualizacji ewidencji, o której mowa powyżej powierza się LADO. Kopie prowadzonej ewidencji i kopie jej aktualizacji LADO przekazuje Inspektorowi Ochrony Danych. Kopie przekazywane są dokonaniu zmian w zbiorach lub ich aktualizacji.

3. Ewidencja zbiorów danych osobowych prowadzonych w sposób tradycyjny zawiera w szczególności:

a) wykaz zbiorów danych osobowych prowadzonych w sposób tradycyjny (załącznik nr 7 do niniejszej Polityki)
b) wykaz osób uprawnionych do przetwarzania danych osobowych w sposób tradycyjny (załącznik nr 8 do niniejszej Polityki),
c) określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności przetwarzanych danych.

4. Obowiązek prowadzenia oraz aktualizację ewidencji, o której mowa w pkt. 3, powierza się LADO lub osobie przez niego wyznaczonej.
5. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą administratora danych lub osoby upoważnionej do przetwarzania danych osobowych.
6. Obszar, w którym są przetwarzane dane osobowe w sposób tradycyjny zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych w sposób tradycyjny.
7. Zabrania się wynoszenia wszelkich dokumentów, kartotek, skorowidzów, ksiąg, wykazów i innych zawierających dane osobowe poza obszar ich przetwarzania.

§ 10.

Naruszenia ochrony danych

1. Obowiązkiem administratorów danych jest zgłaszanie naruszeń ochrony danych.
2. Incydenty zgłaszane są do Urzędu Ochrony Danych Osobowych.
3. Naruszenie ochrony danych 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.
4. Zgłoszenie incydentu następuje w sytuacjach, gdy skutkuje on ryzykiem naruszenia praw i wolności osób, których dane dotyczą, np. naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy tez naruszenia tajemnic prawnie chronionych.
5. W przypadkach naruszenia, o których mowa w ust.4, naruszenie należy zgłosić nie później niż 72 godziny po stwierdzeniu incydentu.
6. W sytuacji, gdy w podczas wystąpienia incydentu pojawią się ryzyka dla osób, których dane dotyczą, występuje konieczność ich zawiadomienia o naruszeniu.
7. Zgłoszenia o zajściu incydentu w Uniwersytecie Szczecińskiem dokonuje niezwłocznie kierownik jednostki, w której doszło do naruszenia ochrony danych osobowych. Formularz zgłoszenia stanowi załącznik nr 9 do niniejszej Polityki.
8. Zgłoszenie, o którym mowa w ust. 7, jest przekazywane rejestrowane przez inspektora danych osobowych i przekazywane niezwłocznie do Urzędu Ochrony Danych przez osobę upoważnioną i wskazaną do dokonania takiego zgłoszenia przez ADO.

§ 11.

Postanowienia końcowe

1. Obowiązek informacyjny, o którym mowa w ogólnym rozporządzeniu o ochronie danych osobowych z dnia 26 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)
w przypadku osób zatrudnionych w Uniwersytecie Szczecińskim na podstawie umowy o pracę, studentów Uniwersytetu Szczecińskiego, doktorantów Uniwersytetu Szczecińskiego ma zastosowanie w przypadku zawierania umów cywilnoprawnych (wzory wprowadzone zarządzeniem rektora), w których stroną jest Uniwersytet Szczeciński.

2. Zasady niniejszej polityki będą zmieniane i uzupełnianie o zapisy i regulacje dotyczące ochrony danych osobowych wprowadzanych ustawodawstwem europejskim i krajowym.

3. Czynności i działania o charakterze wykonawczym do niniejszej Polityki dotyczące realizacji obowiązków związanych z ochroną danych osobowych wydaje, w formie zaleceń, inspektor ochrony danych.