Załącznik nr 1
do Zarządzenia nr 4/2021
Rektora ChAT
z dnia 15.02.2021 r.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Chrześcijańskiej Akademii Teologicznej w Warszawie

Warszawa, 2021

Spis treści

§ 1 Cel polityki bezpieczeństwa w zakresie ochrony danych osobowych.

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane w Chrześcijańskiej Akademii Teologicznej (dalej: Akademia). Celem niniejszego dokumentu jest określenie jednolitych standardów ochrony danych osobowych w Akademii.
2. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Akademii (dalej: Polityka) określa strukturę organizacyjną zapewniającą podział i koordynację zadań oraz odpowiedzialności związanych z zapewnieniem ochrony danych osobowych administrowanych przez Akademię.
3. Przetwarzanie danych osobowych w Akademii służy realizacji zadań wynikających z ustawy o szkolnictwie wyższym oraz ze Statutu Akademii.
4. Przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
5. Przetwarzanie danych osobowych w Akademii może odbywać się w systemie informatycznym, a także w dokumentacji papierowej, wyłącznie w celu realizacji zadań, o których mowa w § 1 ust. 3.
6. Polityka odnosi się do danych osobowych przetwarzanych w:
   1) zbiorach danych tradycyjnych, na papierowych nośnikach danych (dokumentacja papierowa, np. kartoteki, księgi, wykazy, listy itp.),
   2) systemach informatycznych i na nośnikach cyfrowych,
   3) systemach dozoru wizyjnego (monitoring).
7. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w Akademii, odpowiadają:
   1) Administrator Danych Osobowych (ADO);
   2) Inspektor Ochrony Danych (IOD);
   3) Administrator Systemów Informatycznych (ASI);
   4) Osoby upoważnione do przetwarzania danych osobowych na podstawie udzielonych im upoważnień.
8. Polityka obowiązuje we wszystkich, komórkach organizacyjnych i stanowiskach pracowniczych Akademii. Odnosi się do wszystkich chronionych danych osobowych przetwarzanych w Akademii, niezależnie od formy, celu oraz zakresu ich przetwarzania (tradycyjnego i elektronicznego).
9. Procedury i zasady określone w Polityce mają zastosowanie do wszystkich osób wykonujących prace związane z działalnością Akademii lub na rzecz Akademii (niezależnie od formy współpracy, czy rodzaju umowy) w szczególności pracowników, zleceniobiorców oraz osób realizujących umowy o dzieło.
10. Polityka została opracowana w celu spełnienia wymogów wynikających z przepisów prawa, w szczególności:
    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 (Dz. Urz. UE L 119);
    2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
    3) Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r. poz. 113).

§ 2 Podstawowe pojęcia i definicje.

1. **ADO** - Administrator Danych Osobowych – Chrześcijańska Akademia Teologiczna w Warszawie reprezentowana przez Rektora.
2. **Anonimizacja danych osobowych** - Anonimizacja polega na pozbawieniu danych osobowych cech informacji pozwalających na identyfikację konkretnej osoby fizycznej, której dane te dotyczą.

3. **ASI** - Administrator Systemów Informatycznych wyznaczona osoba przez ADO, odpowiadającą za poszczególne systemy informatyczne służące do przetwarzania danych, w tym odpowiedzialną za bezpieczeństwo informacji przetwarzanych w systemie, w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu oraz podejmowanie odpowiednich działań.
4. **Dane osobowe** - 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, dane o lokalizacji, dane dotyczące zdrowia, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
5. **Dane szczególne** - informacje dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, przynależności do związków zawodowych, stanu zdrowia, orientacji seksualnej oraz dane genetyczne i biometryczne.
6. **Informacja** - niestanowiąca tajemnicy państwowej wiadomość, z którą zobowiązany Polityką zapoznał się w związku z wykonywaną pracą, a której ujawnienie może narazić na szkodę uzasadniony interes Akademii, interes publiczny lub prawnie chroniony interes obywateli, z wyłączeniem informacji niejawnych, których zasady ochrony normowane są odrębnie.
7. **IOD** - Inspektor Ochrony Danych - wyznaczona osoba w Akademii pełniąca nadzór nad ochroną danych osobowych oraz monitorująca wypełnienie mających zastosowanie obowiązków wynikających z regulacji prawnych w obszarze danych osobowych w Akademii.
8. **Kategoria osób**, których dane dotyczą - kategoria / grupa osób, których dane osobowe są przetwarzane w Akademii (m.in. pracownicy, kontrahenci, współpracownicy).
9. **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.
10. **Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem Państwa Członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne powinno być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosownie do celów przetwarzania.
11. **Ograniczenie przetwarzania** - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
12. **Organ nadzorczy** - Prezes Urzędu Ochrony Danych Osobowych.
13. **Osoba przetwarzająca dane** - osoba, która świadczy pracę/usługi na rzecz Akademii, bez względu na podstawę prawną (w tym umowa cywilno-prawna, staż, praktyki lub inna forma).
14. **Państwo trzecie** - Państwo, które nie wchodzi w skład EOG (Europejskiego Obszaru Gospodarczego).
15. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO.
16. **Podmiot zewnętrzny** - to osoba fizyczna, jednostka organizacyjna nieposiadająca osobowości prawnej lub osoba prawna z siedzibą w Polsce lub za granicą, organ administracji publicznej, oraz inne podmioty wykonujące zadania na rzecz Akademii.
17. **Pracownik** - osoba zatrudniona w Akademii w oparciu o umowę o pracę, akt mianowania lub realizująca zlecone czynności na podstawie umowy cywilnoprawnej.
18. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
19. **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

20. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
21. **Strona trzecia** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, ADO, podmiot przetwarzający czy osoby, które z upoważnienia ADO lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe.
22. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
23. **Ustawa** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
24. **Użytkownik** – osoba posiadająca upoważnienie do przetwarzania danych osobowych w zbiorach tradycyjnych lub/i w systemach informatycznych, w zakresie wskazanym w upoważnieniu, może nim być pracownik lub osoba wykonująca pracę na podstawie umowy cywilnoprawnej.
25. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
26. **Zgoda** - zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3 Deklaracja zgodności.

1. ADO deklaruje, że przetwarzanie danych osobowych w Akademii jest zgodne z mającymi zastosowanie wymaganiami prawnymi.
2. Deklaracja ta opiera się w szczególności na zapewnieniu, że dane osobowe są:
   1) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane, prawidłowe i w razie potrzeby uaktualniane;
   2) 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;
   3) 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;
   4) przetwarzane są rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
3. Filarami ochrony danych osobowych w Akademii są:
   1) legalizm - Akademia dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
   2) bezpieczeństwo – Akademia zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;
   3) prawa jednostki - Akademia umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
   4) rozliczalność - Akademia dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z RODO.

§ 4 Podział obowiązków w zakresie ochrony danych osobowych w Akademii.

1. **ADO** - realizuje zadania w sprawach z zakresu ochrony danych osobowych. Do najważniejszych obowiązków należy:
   1) zapewnienie przetwarzania danych zgodnie z prawem oraz uregulowaniami Polityki i innymi dokumentami wewnętrznymi;
   2) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z przepisami powszechnie obowiązującymi;
   3) powołanie ASI oraz wprowadzenie „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Akademii";
   4) powoływanie IOD oraz wspieranie IOD w wypełnianiu przez niego zadań;
   5) nadzorowanie działań IOD oraz ASI oraz wydawanie im zaleceń, co do sposobu wykonywania obowiązków wynikających z Polityki.

6) wyrażanie zgód oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania IOD oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.
7) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w formie papierowej lub elektronicznej, która odzwierciedla aktualny stan nadanych i odwołanych upoważnień do przetwarzania danych;
8) wydawanie i cofanie upoważnień do przetwarzania danych osobowych;
9) uwzględnienie ochrony danych w fazie projektowania zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania (wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą);
10) wdrażanie odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych).

2. **IOD** podlega bezpośrednio Rektorowi Akademii jest on odpowiedzialny za:
1) informowanie ADO, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych powszechnie obowiązujących przepisów o ochronie danych i doradzanie im w tej sprawie;
2) konsultowanie merytoryczne umów powierzenia przetwarzania danych osobowych;
3) kontrola działań jednostek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
4) nadzór nad bezpieczeństwem danych osobowych;
5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
6) kontakty z właściwym organem administracji publicznej ds. ochrony danych osobowych związane ze składaniem wyjaśnień oraz współpracą w przypadku kontroli przeprowadzanej przez inspektorów organu nadzorczego;
7) monitorowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
8) organizowanie szkoleń dla pracowników ADO uczestniczących w operacjach przetwarzania danych
9) nadzorowanie opracowania, tworzenie i aktualizację wewnętrznych aktów normatywnych (niniejsza Polityka, procedury, instrukcje, regulaminy i inne dokumenty) dotyczących ochrony danych osobowych oraz nadzór nad ich przestrzeganiem;
10) prowadzenie dokumentacji przetwarzania danych osobowych wymaganych przez mające zastosowanie regulacje prawne;
11) utrzymywanie aktualnego rejestru czynności przetwarzania danych osobowych.

3. **ASI** jest odpowiedzialny za:
1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
2) identyfikowanie i zgłaszanie do IOD ewentualnych problemów z zakresu bezpieczeństwa i ochrony danych osobowych;
3) instalację i konfigurację sprzętu i oprogramowania;
4) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem;
5) kontrolowanie przestrzegania zasad przetwarzania danych osobowych na stacjach roboczych użytkowników;
6) nadzór nad procesem administracji, uprawnieniami nadawanymi/ modyfikowanymi/ odbieranymi do systemów informatycznych przetwarzających dane osobowe;
7) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
8) optymalizacja wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego;

9) planowanie i realizację, w porozumieniu z IOD, działań podnoszących bezpieczeństwo systemów informatycznych, w tym inicjowanie, wdrażanie i koordynowanie wdrożenia nowych rozwiązań informatycznych;
10) prowadzenie ewidencji użytkowników z uprawnieniami dostępu do systemów informatycznych;
11) prowadzenie profilaktyki antywirusowej;
12) przeciwdziałanie próbom naruszenia bezpieczeństwa systemów informacji poprzez analizę dokonanych naruszeń i próbę zapobiegnięciu im w przyszłości;
13) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego;
14) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie;
15) zarządzanie licencjami i procedurami ich dotyczącymi.

4. Wszystkie osoby upoważnione do przetwarzania danych osobowych w Akademii są odpowiedzialne za:
   1) przetwarzanie danych osobowych zgodnie z przyjętą Polityką oraz zapisami RODO i Ustawy;
   2) bezzwłoczne zgłaszanie kierownikowi komórki organizacyjnej oraz IOD wszelkich incydentów, nieprawidłowości i dostrzeżonych zagrożeń związanych z bezpieczeństwem danych osobowych;
   3) dołożenie szczególnej staranności podczas przetwarzania danych osobowych, aby proces przetwarzania odbywał się zgodnie z prawem, dane osobowe były merytorycznie poprawne, a ich przetwarzanie odbywało się wyłącznie w celu i zakresie, dla którego zostały zebrane;
   4) informowanie IOD o zamiarze powierzenia przetwarzania danych osobowych lub ich udostępnienia innemu podmiotowi oraz konsultowanie z IOD umowy o powierzeniu przetwarzania danych osobowych;
   5) niezwłoczne usunięcie / zaprzestanie przetwarzania danych osobowych w momencie ustania celu ich przetwarzania;
   6) przestrzeganie zasad ochrony danych osobowych określonych w Polityce i Instrukcji zarządzania systemami informatycznymi przetwarzającymi dane osobowe oraz dokumentach z nimi związanych. W tym celu każdy użytkownik zobowiązany jest zapoznać się przed dopuszczeniem do przetwarzania danych z wyżej wymienionymi dokumentami oraz złożyć stosowne Oświadczenie w formie zobowiązania pracownika lub współpracownika do zachowania w tajemnicy danych osobowych i informacji oraz sposobów ich zabezpieczenia. W przypadku pracowników zewnętrznych zapisy dotyczące zobowiązania do poufności zawarte są w umowie;
   7) uczestniczenie w obowiązkowym szkoleniu z zakresu ochrony danych osobowych,
   8) wnioskowanie, za pośrednictwem kierownika komórki organizacyjnej do IOD (po wcześniejszym uzgodnieniu z IOD) o potrzebie uzupełnienia lub uaktualnienia Rejestru czynności przetwarzania danych osobowych, potrzebie dokonania zmian w procesie przetwarzania danych osobowych oraz informowanie o ustaniu celu przetwarzania tych danych.

§ 5 Środki techniczne i organizacyjne ochrony danych osobowych

1. W celu zapewnienia ochrony danych osobowych przetwarzanych w Akademii stosuje się następujące zabezpieczenia organizacyjne i techniczne:
   1) do przetwarzania danych osobowych w systemie informatycznym lub w wersji papierowej dopuszcza się jedynie osoby, które uprzednio pisemnie zobowiązały się do zachowania ich w poufności i nadano im pisemne upoważnienie;
   2) pracownicy / współpracownicy mają dostęp wyłącznie do takich informacji i danych jakie się wiążą z wykonywaną przez nich pracą, której zakres został określony w umowie o pracę lub umowie cywilnoprawnej oraz w zakresie zadań / obowiązków (zasada wiedzy koniecznej);
   3) dokonuje się regularnych audytów i testów skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych;
   4) opracowano i wdrożono przez ASI Instrukcję zarządzania systemami informatycznymi przetwarzającymi dane osobowe w Akademii;
   5) przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe dopuszcza się tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
   6) przetwarzania danych osobowych dokonuje się w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych, w szczególności poprzez: kontrolę dostępu do pomieszczeń i budynków, instalację alarmową, zapewnienie środków przetwarzania danych osobowych z trwałym znaczeniem otwarcia, w których przetwarza się dane osobowe (szafy, biurka zamykane na klucz);

7) stosuje się pisemne umowy powierzenia przetwarzania danych osobowych przy współpracy z podmiotami zewnętrznymi przetwarzającymi dane osobowe;
8) zapewnia się realizację szkoleń dla wszystkich osób dopuszczonych do przetwarzania danych osobowych obejmujących zasady ich ochrony;
9) zapewnia się zdolność do możliwie szybkiego przywrócenia dostępności danych osobowych w razie incydentu fizycznego lub technicznego;
10) zapewnia się zdolność do zapewnienia poufności, integralności i dostępności danych osobowych przetwarzanych w systemach informatycznych Akademii;
11) dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi, który jest odpowiedzialny za wszystkie czynności wykonywane przy jego użyciu. Pracownik może przetwarzać dane osobowe tylko w zakresie wskazanym w nadanym przez pracodawcę upoważnieniu do przetwarzania danych osobowych;
12) rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu;
13) zapewnia się zdolność systemów informatycznych do spełnienia praw osób, których dane dotyczą.;
14) powołany jest Inspektor Ochrony Danych (IOD);
15) prowadzona jest ocena ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w związku z przetwarzaniem danych osobowych;
16) dokonywana jest ocena skutków dla ochrony danych osobowych w odniesieniu do planowanych operacji przetwarzania, w szczególności z użyciem nowych technologii – w przypadku, gdy zostanie stwierdzone, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
17) prowadzona jest kontrola dostępu do pomieszczeń, w których przetwarzane są dane osobowe oraz ścisła kontrola dostępu do pomieszczeń, w których znajdują się serwery.

§ 6 Środki organizacyjne i techniczne zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie tradycyjnym.

1. Zabezpieczenie danych osobowych i informacji:
   1) za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe i informacje odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych jednostek organizacyjnych;
   2) wszystkie dane, o których mowa w § 2 ust. 4 i 5, powinny być zabezpieczone fizycznie przed osobami nieupoważnionymi oraz przechowywane w urządzeniach gwarantujących dostęp do nich wyłącznie uprawnionych pracowników, tj. przynajmniej w pomieszczeniach zamykanych na klucz, z zastosowaniem dodatkowego zabezpieczenia w postaci szafy drewnianej zamykanej na klucz lub szafy metalowej - w odniesieniu do szczególnie istotnych dla działalności Akademii danych;
   3) klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich odpowiednie zabezpieczenie;
   4) pomieszczenia, w których przetwarzane są dane osobowe i informacje, zabezpieczone są na czas nieobecności osób zatrudnionych przy przetwarzaniu tych danych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych;
   5) dostęp do kluczy do pomieszczeń, w których przetwarzane są dane osobowe i informacje, posiadają wyłącznie osoby uprawnione przez ADO. Przed rozpoczęciem pracy, klucze pobierane są od pracownika ochrony nadzorującego ich przechowywanie, zaś po zakończeniu pracy są one zdawane również do pracownika ochrony.
2. Postępowanie z danymi osobowym i informacjami:
   1) pracownicy zobowiązani są stosować „politykę czystego biurka”. Polega ona na tym, że;
      - wszelkie dokumenty papierowe i nośniki komputerowe, kiedy nie są używane, przechowuje się w odpowiednich, zamykanych szafach lub innego rodzaju zabezpieczonych meblach, szczególnie poza godzinami pracy;

- nośniki informacji zawierających szczególne kategorie danych osobowych, jeśli nie są aktualnie wykorzystywane, zamykane są w meblach biurowych, szafkach metalowych lub sejfach, w zależności od ich ważności;
- komputery osobiste i stacje robocze nie mogą być pozostawiane bez nadzoru w stanie zarejestrowania do sieci, w sposób umożliwiający korzystanie osobom nieuprawnionym z dostępnych na urządzeniu usług;
- wydruki zawierające dane osobowe muszą być niezwłocznie zabierane z drukarki sieciowej oraz innych współdzielonych urządzeń.

2) dokumentacja zawierająca dane osobowe lub informacje podlega archiwizacji zgodnie z przepisami powszechnie obowiązującymi i aktami obowiązującymi w Akademii.

3. Pracownicy zobowiązani są porządkować dokumentację pod względem jej użyteczności. Polega ona na niszczeniu wszelkiej dokumentacji roboczej lub tymczasowej zawierającej dane osobowe lub informacje niezwłocznie po ustaniu celu przetwarzania. Niszczenie polega w szczególności na:
   1) trwałym, fizycznym zniszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy użyciu niszczarki lub innych skutecznych metod;
   2) anonimizacji danych osobowych i/lub ich zbiorów polegającej na pozbawieniu danych osobowych i/lub ich zbiorów cech pozwalających na identyfikacje osób fizycznych, których anonimizowane dane dotyczą.
4. Pracownicy zobowiązani są do przewożenia, przenoszenia i przekazywania dokumentów w sposób zapobiegający ich kradzieży, zagubieniu, utracie i dostępu osób nieupoważnionych.

§ 7 Środki organizacyjne i techniczne zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym.

1. Zabezpieczenie systemów informatycznych przed osobami nieupoważnionymi:
   1) dostęp do pomieszczeń, w których odbywa się przetwarzanie danych osobowych i informacji winien być ściśle kontrolowany poprzez stosowane zabezpieczenia organizacyjne i mechaniczne;
   2) system informatyczny służący do przetwarzania danych osobowych i informacji zabezpiecza się w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
   3) system informatyczny służący do przetwarzania danych osobowych i informacji chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
   4) w przypadku zastosowania zabezpieczeń logicznych obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym wykorzystywanym w Akademii a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
   5) wszelkie urządzenia i nośniki zawierające dane osobowe lub informacje, takie jak serwery, komputery główne, urządzenia teletransmisyjne, szafy z nośnikami magnetycznymi zawierające kopie danych powinny być usytuowane w pomieszczeniach uniemożliwiających dostęp do nich osób nieupoważnionych.
   6) wyłączniki oraz zabezpieczenia zasilania elektrycznego, powinny być zabezpieczone przed dostępem osób nieupoważnionych;
2. System informatyczny służący do przetwarzania danych osobowych - z wyjątkiem systemu służącego do przetwarzania danych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - powinien zapewniać, aby możliwe było w tym systemie odnotowanie:
   1) daty wprowadzania danych osobowych do systemu, zakres wprowadzanych zmian, zakres przeglądanych danych, identyfikator użytkownika, tak aby było możliwe ustalenie kto, kiedy i w jakim zakresie pracował na danym systemie informatycznym - powyższy obowiązek nie dotyczy systemu informatycznego, do którego dostęp posiada wyłącznie jedna osoba. Powyższe odnotowania następują automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych lub zakończeniu pracy w systemie;
   2) źródła danych w przypadku zbierania danych nie od osoby, której dane dotyczą;
   3) informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie ich udostępnienia;
   4) wniesienia któregokolwiek żądania osoby, której dane dotyczą, o których mowa w § 8;

5) sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa powyżej.

3. ADO wdraża odpowiednie środki techniczne, aby witryny internetowe za pośrednictwem których uzyskuje się zgody na przetwarzanie danych osobowych odpowiadały wymogom o których mowa w § 3 ust. 2 pkt 5.
4. W przypadku wykorzystywania do przetwarzania danych osobowych lub informacji komputerów przenośnych jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i używania, w tym stosowania środków ochrony kryptograficznej. Użytkownik komputera przenośnego odpowiada za powierzone mu urządzenie oraz wszelkie operacje wykonywane przy jego użyciu.
5. Komputery przenośne wykorzystywane do przetwarzania danych osobowych lub informacji, po zakończonej pracy, powinny być przechowywane w warunkach zapewniających ich bezpieczeństwo. Za właściwe zabezpieczenie przedmiotowych urządzeń odpowiedzialni są ich użytkownicy.
6. Usytuowanie urządzeń komputerowych (komputerów typu PC, drukarek) powinno uniemożliwiać dostęp do nich osób nieuprawnionych oraz wgląd do danych wyświetlanych na monitorach komputerowych.
7. W przypadku oddalenia się pracownika od stanowiska pracy należy pozostawić system w takim stanie, aby osoby nieupoważnione nie miały do niego dostępu. W tym celu konieczne jest zablokowanie ekranu komputera oraz stosowanie chronionych hasłem wygaszaczy ekranu z odpowiednim czasem nieaktywności do ich uruchomienia (nie dłuższym niż 10 minut).
8. W przypadku naprawy sprzętu komputerowego dane osobowe lub informacje należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza jednostką, w której przetwarzane są dane osobowe, po zabezpieczeniu należy je usunąć z dysku. Gdy nie ma możliwości usunięcia danych naprawa powinna być nadzorowana przez osobę upoważnioną do przetwarzania danych.
9. Szczególnemu nadzorowi podlegają w Akademii urządzenia umożliwiające tworzenie i przenoszenie dużych ilości danych, w tym nagrywarki DVD oraz nośniki typu pendrive, a także nośniki komputerowe zawierające dane osobowe lub informacje. Do ich ochrony i zabezpieczenia zobowiązani są wszyscy ich użytkownicy.
10. W przypadku uszkodzenia nośników komputerowych, o których mowa w § 13 ust 13, użytkownicy zobowiązani są do ich przekazania do właściwych służb informatycznych w celu ich zniszczenia.
11. Uszkodzone nośniki komputerowe (w tym dyski twarde), zawierające dane osobowe lub informacje, powinny być fizyczne niszczone w sposób uniemożliwiający dostęp do danych osób nieupoważnionych. Do czasu zniszczenia nośniki komputerowe powinny być zabezpieczone przed dostępem osób nieupoważnionych.
12. Dopuszcza się ponowne wykorzystanie urządzeń i nośników komputerowych zawierających dane osobowe lub informacje dla pracowników Akademii.
13. Urządzenia i nośniki komputerowe zawierające dane osobowe i informacje, przeznaczone do ponownego wykorzystania - przed ich wykorzystaniem lub przekazaniem - pozbawić zapisu w sposób gwarantujący trwałe usunięcie danych (za pomocą specjalistycznego oprogramowania).
14. Kontrola dostępu do systemu informatycznego:
    1) system informatyczny przetwarzający dane osobowe i informacje powinien być wyposażony w mechanizmy uwierzytelniania użytkowników oraz kontroli dostępu do danych. Mechanizmy te powinny być ciągle uaktywnione;
    2) czas dostępu użytkownika do poszczególnych danych osobowych i informacji określony jest czasem wykonania zadania wynikającego z pełnionej roli;
    3) system informatyczny musi zapewniać autoryzację i rozliczalność operacji. Każde działanie w systemie informatycznym powinno być jednoznacznie przypisane do unikalnego identyfikatora;
    4) dostęp do danych osobowych i informacji w systemie informatycznym powinien być kontrolowany. Jest on możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia. Identyfikator przydzielany jest użytkownikowi na stałe. Uwierzytelnienie użytkownika następuje za pomocą indywidualnego hasła;
    5) system informatyczny powinien posiadać możliwość kontroli złożoności i długości haseł;
    6) każde nowe lub zmienione urządzenie służące do przetwarzania danych osobowych lub informacji musi zostać zweryfikowane co do zgodności z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez ASI.

15. Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym:
    1) przed uruchomieniem komputera na stanowisku pracy każdy użytkownik powinien dokonać przeglądu i sprawdzenia urządzeń komputerowych pod kątem ujawnienia okoliczności wskazujących na naruszenie dostępu do tych urządzeń lub danych zawartych na nich. W przypadku stwierdzenia naruszenia, należy postępować zgodnie z § 4 ust. 4 pkt 1;
    2) rozpoczęcie pracy w systemie komputerowym powinno być możliwe po zalogowaniu się do systemu przy użyciu indywidualnego identyfikatora oraz hasła nadanego przez ASI;
    3) użytkownik opuszczając stanowisko pracy powinien zwrócić szczególną uwagę na uniemożliwienie wykorzystywania systemu komputerowego przez osoby nieupoważnione, w szczególności na włączenie opcji wygaszacza ekranu po upływie ustalonego czasu nieaktywności użytkownika;
    4) przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i wylogować się z sieci komputerowej. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci;
    5) zabrania się wykorzystywania sprzętu służbowego do celów prywatnych;
    6) zabrania się wykorzystywania sprzętu prywatnego do przetwarzania danych, których ADO jest Akademia bez zgody Rektora;
16. Zabronione jest podejmowanie działań mogących być zagrożeniem dla systemu informatycznego, a w tym:
    1) łamanie haseł;
    2) dokonywanie włamań na konta innych użytkowników;
    3) nieprawne uzyskiwanie dostępu do kont administracyjnych;
    4) zakłócanie działania usługi;
    5) omijanie i badanie zabezpieczeń;
    6) doprowadzanie do rozprowadzania wirusów, koni trojańskich, niechcianej poczty i innego złośliwego oprogramowania;
    7) praca na koncie innego użytkownika.
17. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony.
18. Po zakończeniu pracy należy zamknąć system, wyłączyć monitor i ewentualnie drukarkę, a także zabezpieczyć stanowisko pracy, w szczególności dokumentację i wymienne nośniki danych.
19. Wymogi dotyczące haseł:
    1) użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł;
    2) hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny;
    3) hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie;
    4) w sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
    5) przy wyborze hasła obowiązują następujące zasady;
       - minimalna długość hasła - 8 znaków,
       - właściwa złożoność hasła.
20. Zakazuje się stosować haseł:
    1) które użytkownik stosował uprzednio;
    2) będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami);
    3) analogicznych jak identyfikator;
    4) zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci, itp.;
    5) stanowiące przewidywalne sekwencje znaków, np. 12345678 lub abcdef.
21. Zmiany hasła nie należy zlecać innym osobom.
22. W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
23. Tworzenie i przesyłanie plików:
    1) nie tworzy się plików o charakterze baz danych (np. pliku excel) bez powodów;
    2) przed wysłaniem pliku zawierającego dane osobowe należy go odpowiednio zabezpieczyć poprzez zaszyfrowanie hasłem. Hasło należy przesłać odbiorcy pliku inną drogą komunikacji;

3) zabrania się podłączania do służbowego sprzętu komputerowego obcych nośników danych. O znalezionym lub zgubionym wymiennym nośniku danych typu Pendrive, zawierającym dane osobowe należy powiadomić Inspektora Ochrony Danych;
4) zobowiązuje się pracowników do przesyłania elektronicznej korespondencji służbowej wyłącznie za pośrednictwem Akademickiej skrzynki pocztowej;
5) w przypadku przesyłania korespondencji elektronicznej należy ukrywać listę innych odbiorców poprzez wpisywanie adresu w polu UDW lub BCC.

§ 8 Upoważnienie do przetwarzania danych.

1. Do przetwarzania danych osobowych w systemie tradycyjnym i informatycznym mogą być dopuszczone osoby posiadające upoważnienie wydane przez ADO lub osobę przez niego upoważnioną.
2. Upoważnienia wydawane są:
   1) pracownikom - w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych;
   2) wykonawcom usług i dostawcom sprzętu lub oprogramowania - w zakresie koniecznym do realizowania danej usług lub wykonania określonych czynności w systemie.
3. Zakres upoważnienia do przetwarzania danych osobowych powinno być adekwatne do zakresu wykonywanych zadań i nie może być on szerszy niż wynika to z realizowanych czynności zleconych przez ADO.
4. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić zmiana zakresu upoważnienia do przetwarzania danych osobowych.
5. Upoważnienie wydaje się przy zatrudnianiu pracownika po odbyciu przez tę osobę szkolenia z zakresu ochrony danych osobowych oraz podpisaniu oświadczenia w którym zobowiązuje się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Tajemnica obowiązuje osobę upoważnioną przy przetwarzaniu danych osobowych, zarówno w trakcie trwania umowy, jak i po jej ustaniu.
6. Przy nadaniu, zmianie lub cofnięciu upoważnienia należy dostarczyć według właściwości do Działu Kadr lub Działu Płac oświadczenie oraz stosowne upoważnienie.
7. Nadawanie i cofnięcie upoważnienia do przetwarzania danych może nastąpić:
   1) na umotywowany wniosek bezpośredniego przełożonego;
   2) na wniosek IOD;
   3) wraz z rozwiązaniem stosunku łączącego go z ADO.
8. Cofnięcie uprawnień do systemów informatycznych nadanych użytkownikowi następuje zgodnie z brzmieniem § 8 ust. 7.
9. ASI rejestruje użytkownika w systemie i nadaje mu określone uprawnienia oraz wpisuje osobę w ewidencję użytkowników z prawami dostępu do systemów informatycznych.
12. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić modyfikacja uprawnień nadanych użytkownikowi.

§ 9 Realizacja obowiązku informacyjnego

1. Administrator Danych w celu wypełnienia obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane w Akademii, jest zobowiązany do podania osobie, której dane dotyczą, wszystkich informacji wymaganych zgodnie z RODO (tzw. klauzula informacyjna). Wzory klauzul informacyjnych określa IOD.
2. Klauzule informacyjne dla poszczególnych przypadków mogą być tworzone przez pracowników jednostek organizacyjnych Akademii na potrzeby konkretnych przypadków, jednak są oni zobowiązani do konsultowania treści klauzul z IOD.
3. Obowiązku informacyjnego nie stosuje się do wypowiedzi akademickiej, o której mowa w art. 85 ust. 2 RODO i art. 2 ust. 2 UODO. W tym przypadku Administrator Danych jest także zwolniony z wykonania na wniosek osoby, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu, jak również z obowiązku ograniczenia przetwarzania oraz obowiązku rejestrowania czynności przetwarzania dotyczących takiej wypowiedzi.

5. W przypadku, gdy dane osobowe zbierane są bezpośrednio od osoby, której dane dotyczą, należy przekazać informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i konsekwencjach niepodania danych.
6. W przypadku, gdy dane osobowe pozyskiwane są w inny sposób niż od osoby, której dane dotyczą, należy przekazać osobie, której dane dotyczą informacje zawarte w § 9 ust. 1. oraz uzupełnione o:
   1) kategorie przetwarzanych danych osobowych;
   2) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie również informacji czy pochodzą one ze źródeł publicznie dostępnych.
7. W przypadku, gdy planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, należy poinformować osobę, której dane dotyczą, o nowym celu przetwarzania oraz udzielić jej stosowanych informacji zawartych w niniejszym paragrafie.
8. Do realizacji obowiązku informacyjnego zobowiązane są wszystkie osoby przetwarzające dane w Akademii.
9. Obowiązek informacyjny w Akademii należy realizować:
   1) pisemnie - jako integralną część umowy lub innego dokumentu z podmiotem zewnętrznym zawierającego dane osobowe;
   2) w formie elektronicznej - jako informacja w systemie informatycznym przetwarzającym dane osobowe;
   3) w formie e-mail - w przypadku korespondencji e-mail.
10. Podstawowe informacje wymagane mającymi zastosowanie regulacjami prawnymi w obszarze ochrony danych osobowych udostępniane są na stronie internetowej Akademii.
11. Informacje zawarte w niniejszym punkcie nie mają zastosowania w przypadku, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami.
12. Dopuszczalne jest tzw. warstwowe spełnienie obowiązku informacyjnego polegające na umieszczeniu skróconej wersji w stopce z odwołaniem do pełnej wersji na stronie internetowej.

§ 10 Prawa osób, których dane przetwarzane są przez Akademię.

1. Prawo dostępu do danych osobowych przysługujące osobie, której dane dotyczą;
2. Każda osoba, której dane dotyczą jest uprawniona do uzyskania potwierdzenia, czy w Akademii przetwarzane są jej dane osobowe.
3. Na wniosek osoby, której dane dotyczą, należy przekazać informację o:
   1) celu przetwarzania danych osobowych;
   2) kategoriach przetwarzanych danych osobowych;
   3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w Państwach trzecich lub organizacjach międzynarodowych oraz zabezpieczeniach wykorzystywanych w związku z tym przekazaniem;
   4) prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania jej danych osobowych oraz prawie wniesienia sprzeciwu wobec takiego przetwarzania;
   5) prawie wniesienia skargi do organu nadzorczego;
   6) w miarę możliwości o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach tego okresu;
   7) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotnych zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
   8) źródle pozyskiwania danych osobowych, jeśli nie zostały zebrane od osoby, której dane dotyczą.
4. W przypadku wystąpienia przez osobę, której dane dotyczą o kopię danych osobowych, należy zgłosić taki fakt IOD.
5. IOD przekazuje osobie, której dane dotyczą kopię danych podlegających przetwarzaniu.
6. IOD podejmuje decyzję o formie, w której zostanie przekazana kopia danych oraz w uzasadnionych przypadkach o wysokościach opłat za przygotowanie danych.
7. IOD ma prawo odmowy przekazania kopii danych osobowych w przypadku, gdy może to wpłynąć na prawa i wolności innych osób.
8. Prawa do sprostowania, usunięcia, ograniczenia, przenoszenia danych osobowych oraz sprzeciwu wobec ich przetwarzania:

1) prawo do sprostowania - każda osoba, której dotyczą dane ma prawo do żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Występująca z wnioskiem osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia;
2) prawo do usunięcia danych (prawo do bycia zapomnianym) - każda osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia jej danych osobowych;
3) prawo do ograniczenia przetwarzania - każda osoba, której dane dotyczą, ma prawo żądania od ADO ograniczania przetwarzania jej danych osobowych;
4) prawo do przenoszenia danych - osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła ADO oraz ma prawo przesłać te dane osobowe innemu Administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe;
5) prawo do sprzeciwu - osoba, której dane dotyczą ma prawo wnieść sprzeciw wobec przetwarzania jej danych osobowych.

9. Zasady realizacji praw osób, których dane dotyczą:
   1) wnioski o realizację praw osób, których dane dotyczą należy kierować na adres iod@chat.edu.pl;
   2) w przypadku, gdy wniosek zostanie skierowany do pracownika Akademii, należy przekazać go niezwłocznie do IOD;
   3) IOD dokonuje analizy wniosku oraz weryfikuje zasadność realizacji prawa osoby, której dane dotyczą;
   4) przed udzieleniem odpowiedzi należy zweryfikować tożsamość osoby wnioskującej;
   5) w przypadku braku zasadności realizacji prawa, IOD zobligowany jest do niezwłocznego (nie dłużej niż w terminie jednego miesiąca) przekazania tej informacji osobie wnioskującej wraz z właściwym uzasadnieniem decyzji;
   6) w przypadku pozytywnej oceny wniosku, IOD zobligowany jest do wszczęcia postępowania mającego na celu realizację prawa osoby wnioskującej. Po zakończeniu działań związanych z realizacją prawa osoby wnioskującej, IOD informuje o tym fakcie osobę wnioskującą. W przypadku, gdy czas realizacji prawa może przekroczyć 1 miesiąc IOD przekazuje osobie wnioskującej informację wraz z planowanym terminem realizacji prawa, o które wnioskowała;
   7) w przypadku realizacji prawa osoby, której dane dotyczą, IOD ma obowiązek przekazania obowiązku realizacji tego prawa do wszystkich podmiotów, którym powierzono dane do przetwarzania;
   8) w sytuacji, w której realizacja prawa osoby, której dane dotyczą wymaga zaangażowania pracowników Akademii, na wniosek IOD pracownicy ci są zobligowani do wykonania zadań niezbędnych do realizacji prawa wnioskującego.

§ 11 Zgody na przetwarzanie danych osobowych.

1. W każdej sytuacji, w której nie zidentyfikowano podstawy prawnej, innej niż zgoda osoby, której dane dotyczą, niezbędne jest uzyskanie takiej zgody.
2. Forma wyrażenia zgody na przetwarzanie danych osobowych jest dowolna (np. treść wiadomości e-mail, wydruk, checkbox w systemie informatycznym). Forma zgody powinna gwarantować możliwość potwierdzenia uzyskania takiej zgody.
3. Wyrażenie zgody na przetwarzanie danych osobowych nie może stanowić podstawy do odmowy wykonania umowy / świadczenia usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do ich wykonania.
4. Za uzyskanie zgody na przetwarzanie danych osobowych odpowiedzialny jest pracownik pozyskujący dane osobowe od osoby, której dane dotyczą.
5. Zgoda na przetwarzanie danych osobowych powinna zawierać, co najmniej:
   1) nazwę ADO;
   2) zamierzone cele przetwarzania, dla których dane osobowe są zbierane;
   3) fakt wyrażenia zgody;
   4) informację o możliwości wycofania zgody.
6. Nie dopuszcza się sytuacji, w których łączy się zgody na przetwarzanie danych osobowych zbieranych dla spełnienia różnych celów. W przypadku zbierania danych osobowych dla kilku celów jednocześnie, należy uzyskać indywidualną zgodę dla każdego z celów.

7. W przypadku, gdy zgoda dotyczy danych szczególnych, konieczne jest zebranie jej w formie pisemnego oświadczenia od osoby, której dane dotyczą.
8. Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać zgodę.
9. W przypadku uzyskania wniosku o wycofanie zgody na przetwarzanie danych osobowych, każdy pracownik jest zobowiązany do powiadomienia o tym fakcie IOD, który podejmuje właściwe kroki.

§ 12 Realizacja udostępnień danych osobowych.

1. Dane osobowe udostępniane są wyłącznie na pisemny, umotywowany wniosek chyba, że przepisy prawa stanowią inaczej.
2. Udostępnienia danych osobowych może dokonać wyłącznie IOD lub kierownik komórki organizacyjnej przetwarzającej określone dane osobowe w uzgodnieniu z IOD. Wszyscy pracownicy Akademii, w przypadku otrzymania wniosku o udostępnienie danych osobowych, zobligowani są do przekazania wniosku IOD.
3. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
4. Zgodę na udostępnienie danych osobowych wydaje IOD.
5. W przypadku wyrażenia zgody na udostępnienie, IOD przygotowuje udostępniane dane osobowe oraz odnotowuje fakt udostępnienia w ewidencji udostępnień.
6. W przypadku udostępniania danych z systemów informatycznych, które nie odnotowują udostępnienia automatycznie, plik przekazywanych danych jest przechowywany przez IOD wraz z dokumentem wskazującym na podstawę udostępnienia i dodatkowym opisem wskazującym datę udostępnienia danych oraz określeniem odbiorcy danych (np. nazwa i adres instytucji).

§ 13 Zasady powierzania danych osobowych.

1. Powierzenie przetwarzania danych osobowych przez Akademię podmiotom zewnętrznym następuje wyłącznie w drodze umowy powierzenia przetwarzania danych osobowych zawartej na piśmie.
2. Umowa, która zawiera zapisy o powierzeniu przetwarzania danych osobowych powinna w szczególności zawierać zapisy dotyczące:
   1) przedmiotu, charakteru, celu i czasu trwania przetwarzania danych osobowych;
   2) rodzaju danych osobowych oraz kategorii osób, których dane dotyczą, obowiązków i praw ADO;
   3) zobowiązań pracowników podmiotu przetwarzającego do zachowania powierzonych danych osobowych w poufności;
   4) zapewnienia bezpieczeństwa organizacyjnego i technicznego przetwarzania danych osobowych;
   5) zasad dalszego powierzania danych osobowych administrowanych przez Akademię;
   6) udziału w procesie udzielania odpowiedzi na żądanie osoby, które dane dotyczą, oceny skutków dla przetwarzania danych osobowych, zgłaszania incydentów;
   7) usunięciu lub zwróceniu powierzonych danych osobowych po zakończeniu świadczenia usługi;
   8) udostępniania ADO wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w mających zastosowanie przepisach prawa w obszarze ochrony danych osobowych (np. audyty drugiej strony);
   9) możliwości żądania natychmiastowego wstrzymania przetwarzania powierzonych danych osobowych w razie stwierdzenia niedostatecznej ochrony ww. danych;
   10) pracownicy Akademii mają obowiązek zasięgnąć opinii IOD w każdej sytuacji, w której ma nastąpić podpisanie umowy, której przedmiot choćby pośrednio wiąże się z powierzeniem innej firmie danych osobowych, bądź z przyjęciem przez Akademię danych osobowych do przetwarzania.
3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, nie może powierzyć do dalszego przetwarzania powierzonych mu danych bez pisemnej zgody ADO.
4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, zobowiązany jest przetwarzać powierzone mu dane wyłącznie w celach, które zostały wskazane w zawartej z nim umowie.
5. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, zobowiązany jest do spełnienia mających zastosowanie wymagań prawnych w obszarze danych osobowych.

§ 14 Naruszenia ochrony danych osobowych.

1. Za naruszenie ochrony danych osobowych uznaje się 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.
2. Każdy z pracowników Akademii, w przypadku zidentyfikowania zdarzenia mogącego stanowić naruszenie ochrony danych osobowych, jest zobowiązany do niezwłocznego przesłania wypełnionego załącznika nr 1 (będącego integralną częścią Polityki) do IOD oraz kontaktu z nim osobiście lub poprzez: e-mail: iod@chat.edu.pl.
3. Obowiązek informacyjny, o którym mowa w § 14 ust. 2, powinien zostać zrealizowany najpóźniej następnego dnia roboczego po dniu powzięcia informacji o potencjalnym lub zaistniałym naruszeniu ochrony danych osobowych.
4. W uzasadnionych przypadkach osoba, która zgłosiła naruszenie zobowiązana jest postępować zgodnie z wytycznymi IOD w zakresie zabezpieczenia materiału dowodowego i jeśli zajdzie taka potrzeba zaprzestania wykonywania obowiązków służbowych w celu nienaruszania materiałów dowodowych.
5. Wszystkie zdarzenia zakwalifikowane jako naruszenie ochrony danych osobowych IOD udokumentuje w Rejestrze naruszeń ochrony danych osobowych i bezpieczeństwa informacji.
6. W przypadku, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, należy je bez zbędnej zwłoki o tym poinformować o ile jest to technicznie możliwe.
7. Zgłoszenia zdarzeń dotyczących bezpieczeństwa, jeżeli dotyczą systemów przetwarzających dane osobowe, powinny zostać zgłoszone IOD oraz ASI.
8. Dopuszcza się możliwość przeprowadzenia postępowania wyjaśniającego przez IOD, przy czym po uzyskaniu informacji, o której mowa w § 14 ust. 2, w pierwszej kolejności ustala, czy zaistniałe zdarzenie skutkuje naruszeniem praw lub wolności osób fizycznych.
9. W ramach postępowania wyjaśniającego podejmowane są czynności mające na celu wyjaśnienie okoliczności danego zdarzenia, w szczególności:
   1) ustalenie czasu wystąpienia naruszenia, jego zakresu, przyczyn, skutków oraz wielkości szkód, które zaistniały;
   2) ustalenie osoby odpowiedzialnej za naruszenie;
   3) podjęcie działań w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości;
   4) wyciągnięcie konsekwencji w stosunku do osoby ponoszącej odpowiedzialność za zdarzenie, przy czym zgodnie z przepisami powszechnie obowiązującymi z tytułu przedmiotowych naruszeń możliwa jest odpowiedzialność dyscyplinarna, cywilna lub karna;
   5) zaopiniowanie czy ADO zobowiązany jest zgłosić sprawę organom ścigania;
   6) w przypadku, gdy zgłoszone naruszenie wystąpiło w systemie informatycznym IOD może włączyć do postępowania wyjaśniającego ASI.
10. IOD prowadząc postępowanie wyjaśniające ma prawo do pełnej swobody działania, dostępu do dokumentów, wglądu do operacji wykonywanych w systemie informatycznym, pobierania wyjaśnień od pracowników i osób mogących mieć wpływ na wyniki postępowania. Raport zawierający wyniki postępowania wyjaśniającego IOD przekazuje ADO.
11. ADO po uzyskaniu od IOD informacji o stwierdzonym naruszeniu ochrony danych osobowych lub incydencie, które skutkuje naruszeniem praw i wolności osób fizycznych albo jest wysoce prawdopodobne, w terminie 72 godzin od stwierdzenia naruszenia ochrony danych zawiadamia Prezesa Urzędu Ochrony Danych.

§ 15 Retencja danych (okres przechowywania danych osobowych).

1. Dane osobowe przetwarzane w Akademii przechowywane są przez okres nie dłuższy niż jest to niezbędne. Okres przechowywania danych dostosowywany jest do celu, w którym zostały zebrane.
2. Okres retencji może:
   1) wynikać z przepisów prawa;
   2) zostać określony przez organ nadzorczy w zakresie ochrony danych osobowych;

3) być ustalany przez komórki organizacyjne będące właścicielami przetwarzanych danych osobowych w oparciu o Rzeczowy Wykaz Akt (ustalony w uzgodnieniu z Archiwum Akt Nowych);
4) wynikać z zapisów konkretnej umowy.

3. Wskazany przez komórkę organizacyjną okres retencji jest weryfikowany i akceptowany przez IOD.
4. Okres retencji danych osobowych odnotowany jest w Rejestrze czynności przetwarzania w stosunku do określonej kategorii i celu, w jakim dane osobowe zostały zebrane.
5. W przypadku dokumentacji w formie papierowej, za zniszczenie danych po ustaniu okresu retencji odpowiedzialny jest każdy pracownik przetwarzający te dane. Dane powinny zostać zniszczone przy użyciu odpowiednie niszczarki. Proces ten może zostać zlecony na zewnątrz Akademii. Ze zniszczenia danych należy sporządzić protokół, którego treść należy uzgodnić z IOD.
6. W przypadku danych osobowych przetwarzanych w systemach informatycznych, każdy pracownik przetwarzający te dane jest odpowiedzialny, w miarę możliwości, za usunięcie tych danych po upłynięciu okresu retencji lub zgłoszenie potrzeby ich usunięcia do IOD. Na podstawie tego wniosku IOD kontaktuje się z ASI w celu usunięcia danych w wersji elektronicznej. Co najmniej raz w roku kierownicy komórek organizacyjnych w Akademii odpowiedzialni są za przeprowadzenie weryfikacji, czy cel przetwarzania danych osobowych w stosunku do danych, które przetwarzają, jest nadal aktualny oraz, czy nie przetwarzają danych dłużej aniżeli zostało to określone w Rejestrze czynności przetwarzania.
7. Wyniki przeglądu są przekazywane do IOD na jego wniosek.

§ 16 Postanowienia końcowe

1. Do kontroli stanu ochrony danych osobowych w jednostkach organizacyjnych Akademii uprawnieni są:
   1) Administrator Danych Osobowych;
   2) Kanclerz;
   3) Inspektor Ochrony Danych;
   4) Administrator Systemu Informatycznego;
   5) Pracownicy upoważnieni przez Rektora.
2. Akademia dba o zapoznanie pracowników z Polityką i jej przestrzeganie. We wszelkich sprawach związanych z interpretacją postanowień Polityki oraz przepisów powszechnie obowiązujących dotyczących ochrony danych osobowych należy zwracać się do Inspektora Ochrony Danych.
3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.