Załącznik
do Zarządzenia Nr 61/0101/2020 Rektora AJP
z dnia 1 września 2020 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w Akademii im. Jakuba z Paradyża

Rozdział I.
Przepisy ogólne
§ 1.

1. Niniejsza Polityka Bezpieczeństwa Informacji wdrażana jest przez Akademię im. Jakuba z Paradyża, zwaną dalej Administratorem Danych Osobowych (ADO). Jej opracowanie ma miejsce w związku z wejściem w życie 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, dalej zwane RODO.
2. ADO, będąc świadomym, iż jest zwolniony z obowiązku rejestracji zbiorów danych, a także posiadania samej Polityki Bezpieczeństwa Informacji, zwanej dalej PBI, postanawia wdrożyć niniejszy dokument przy zachowaniu wszelkich standardów wymaganych prawem dla przetwarzania danych osobowych. Opracowanie niniejszego dokumentu wynika ze zrozumienia znaczenia bezpieczeństwa danych we współczesnym świecie.
3. Głównym celem wprowadzenia PBI jest zapewnienie bezpieczeństwa przetwarzanych danych w strukturze podległej ADO oraz dostosowanie organizacji do standardów RODO, ustawy o ochronie danych osobowych z 2018 r. oraz aktów wykonawczych.
4. PBI została opracowana w oparciu o wytyczne zawarte w następujących aktach prawnych:
    1) RODO;
    2) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.), zwana dalej Ustawą.

§ 2.

Sformułowania użyte w niniejszym dokumencie należy rozumieć w sposób następujący:

1) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
2) dane istotne – wszelkie dane, które zdaniem ADO zasługują na szczególną ochronę oraz wobec których powinny być podjęte kroki w celu zapobieżenia ujawnieniu osobom trzecim. Są to dane takie jak umowy handlowe, dokumenty finansowe etc.;
3) dane wrażliwe – dane szczególnie chronione przez przepisy prawa. Zgodnie z RODO są to:
    a) dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych,
    b) dane genetyczne,
    c) dane biometryczne,
    d) dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
    e) dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;
4) przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych lub danych istotnych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie,

zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

5) poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
6) Instrukcje zarządzania systemami informatycznymi – zespół norm oraz zasad obowiązujących w systemach informatycznych ADO, służące m.in. zapewnieniu bezpieczeństwa oraz poufności danych.

Rozdział II.
Zakres informacji objętych Polityką Bezpieczeństwa Informacji oraz zakres zastosowania

§ 3.

1. PBI opisuje zasady i procedury przetwarzania danych osobowych i danych istotnych oraz zabezpieczenia ich przed nieuprawnionym dostępem.
2. PBI składa się z następujących elementów:
   1) zadań i obowiązków ciążących na ADO oraz Inspektorze Ochrony Danych Osobowych, zwany dalej IODO;
   2) określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych;
   3) wzorów dokumentów stosowanych przez ADO.

Rozdział III.
Osoby odpowiedzialne za ochronę danych osobowych

§ 4.

1. Osobami odpowiedzialnymi za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, RODO, PBI oraz Instrukcji zarządzania systemami informatycznymi, stanowiącej załącznik nr 1 do PBI, są:
   1) ADO;
   2) IODO;
   3) osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz ADO.
2. Osoby, o których mowa w ust. 1 pkt 3, uzyskują stosowne upoważnienie do przetwarzania danych osobowych.
3. Wzór upoważnienia, o którym mowa powyżej stanowi załącznik nr 2 i 3 do PBI – dopuszczalne jest stosowanie innego dokumentu zawierającego niezbędne zapisy.

§ 5.

1. ADO jest Akademia im. Jakuba z Paradyża.
2. ADO ma świadomość, że przetwarza dane osobowe w związku z realizacją czynności niezbędnych do wykonania umowy o świadczenie usług edukacyjnych, zatrudnieniem u niego (lub świadczeniem u niego usług na podstawie umów cywilnoprawnych) lub wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej.
3. ADO przetwarza dane osobowe na podstawie zgody osób których dane są przetwarzane, ale również w swoim prawnie uzasadnionym interesie jakim jest konieczność przetwarzania danych osobowych osób zatrudnionych, studentów, świadczących usługi oraz kontrahentów.

§ 6.

1. ADO powołał IODO.
2. Do zadań IODO należą poniższe czynności:
   1) stały nadzór nad treścią PBI;
   2) aktualizacja i modyfikacja PBI;

3) informowanie ADO, podmioty przetwarzające oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach związanych z przetwarzaniem danych osobowych spoczywających na nich na mocy przepisów prawa;
4) monitorowanie przestrzegania przepisów ochrony danych osobowych poprzez dokonywanie czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
5) podejmowanie działań zwiększających świadomość ochrony danych osobowych personelu zatrudnionego u ADO uczestniczącego w operacjach przetwarzania, w tym m.in. szkolenia i audyty;
6) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych;
7) prowadzenie rejestru czynności przetwarzania, jeżeli taki obowiązek zaistnieje na podstawie przepisów prawa lub IODO uzna to za słuszne;
8) pełnienie funkcji punktu kontaktowego dla osób przetwarzanych oraz Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych;
9) udział w kontrolach prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych.

§ 7.

1. ADO powołał Administratora Systemów Informatycznych (osoba odpowiedzialna za system informatyczny), zwanego dalej ASI.
2. Do jego zadań należą poniższe czynności:
   1) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych;
   2) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
   3) zapewnienie ciągłości działania systemów informatycznych;
   4) sprawne realizowanie procedur tworzenia kopii zapasowych;
   5) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
   6) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych.

§ 8.

1. Osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, RODO, PBI oraz Instrukcji zarządzania systemem informatycznym.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
3. Każda upoważniona osoba, wraz z wydaniem dostępu do systemu informatycznego, powinna zobowiązać się do zachowania poufności zgodnie ze wzorem stanowiącym załącznik nr 4 do PBI.

Rozdział IV.
Upoważnienie do przetwarzania danych osobowych

§ 9.

1. Upoważnienie do przetwarzania danych osobowych oraz innych istotnych danych wydaje w imieniu ADO kierownik działu właściwego ds. organizacyjnych lub osoba zastępująca, na podstawie listy pracowników przedstawionej przez kierownika działu właściwego ds. kadr.

2. Przyznawanie użytkownikowi dostępu do systemów informatycznych oraz nadawania lub modyfikację uprawnień użytkownika do zasobów systemu informatycznego spoczywa na ASI.
3. Wniosek o wydanie oraz cofnięcie upoważnienia kierowany jest przez właściwego przełożonego.
4. Cofnięcie upoważnienia powinno następować wraz z ustaniem stosunku prawnego pomiędzy pracownikiem lub współpracownikiem, a ADO lub w przypadku stwierdzenia istotnego naruszenia przez osobę upoważnioną do stosowania zasad bezpieczeństwa informacji.
5. Upoważnienie wydawane jest w formie pisemnej, zgodnie ze wzorem stanowiącym załącznik nr 2 i 3 do PBI – dopuszczalne jest stosowanie innego dokumentu zawierającego niezbędne zapisy.
6. Upoważnienie zawiera zakres oraz cel przetwarzania danych.
7. Rejestr osób upoważnionych do korzystania z systemów informatycznych oraz przetwarzania zawartych w nich danych osobowych jest prowadzony w bazach danych tych systemów informatycznych.

Rozdział V.
Umowy powierzenia przetwarzania danych osobowych
§ 10.

1. W przypadku, gdy ADO zechce powierzyć przetwarzanie danych osobowych zewnętrznym podmiotom może się to obyć wyłącznie w drodze umowy powierzenia zawartej w formie pisemnej.
2. Umowa powierzenia przetwarzania powinna być przygotowana lub zatwierdzona przez IODO.
3. IODO prowadzi rejestr umów powierzenia przetwarzania danych osobowych.
4. W umowie powierzenia należy określić zbiór, który zostanie przekazany, cel tego przekazania oraz zakres planowanego przetwarzania danych przez inny podmiot, obowiązki przetwarzającego, prawo do kontroli dokonywanej przez przekazującego, zakres odpowiedzialności przetwarzającego oraz czas obowiązywania umowy. Umowa powinna zakazywać profilowania oraz przenoszenia danych osobowych poza terytorium Europejskiego Obszaru Gospodarczego.
5. W związku z ryzykiem związanym z powierzaniem przetwarzania danych osobowych zewnętrznym podmiotom należy robić to tylko gdy jest to zasadne pod względem zabezpieczenia żywotnych interesów ADO.
6. Wykaz podmiotów, którym ADO powierzył przetwarzanie danych osobowych sporządza się według wzoru stanowiącego załącznik nr 5 do PBI.

Rozdział VI.
Zasady przetwarzania danych osobowych
§ 11.

1. W trakcie przetwarzania danych osobowych w Akademii im Jakuba z Paradyża stosowane będą następujące zasady:
    1) zasada przejrzystości zgodnie z którą wszelkie komunikaty związane z przetwarzaniem danych osobowych były prezentowane w łatwo dostępny, zrozumiały sposób, a także jasnym i prostym językiem;
    2) zasada zgodności z prawem, która wymaga aby przetwarzanie danych osobowych było wykonywane na podstawie przesłanek legalności, tj. najczęściej zgody osoby fizycznej lub prawnie uzasadnionego interesu ADO;

3) zasada ograniczenia celu przetwarzania danych osobowych, która wymaga aby dane były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
4) zasada minimalizacji danych, która wymaga aby dane osobowe były adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum;
5) zasada prawidłowości danych, zgodnie z którą dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane;
6) zasada ograniczenia przechowywania danych, która wymaga, aby okres przetwarzania danych był ograniczony do czasu jaki jest niezbędny do tego, aby osiągnąć założony cel przetwarzania danych;
7) zasada integralności i nienaruszalności zgodnie z którą dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich.

2. Jeśli przesłanką legalności jest dobrowolna zgoda na przetwarzanie danych osobowych, która powinna mieć brzmienie zgodne z poniższym:
   1) *Wyrażam zgodę na przetwarzanie moich danych osobowych tj. ……. (np.: imię, nazwisko, adres e-mail, adres zamieszkania, numer telefonu) przez Administratora Danych Osobowych, tj. Akademii im. Jakuba z Paradyża w celu …….. Moja zgoda może zostać cofnięta, może być wniesiony sprzeciw wobec przetwarzania Państwa danych osobowych lub mogą być one przeniesione w dowolnym momencie. Aby skontaktować się z Administratorem Danych Osobowych należy wysłać wiadomość e-mail na adres iodo@ajp.edu.pl spod adresu, którego zgoda dotyczy. Informujemy, że nie jesteście Państwo profilowani, a dane nie będą udostępniane innym podmiotom. Podanie danych jest dobrowolne. Państwa dane nie będą przekazywane poza EOG ani udostępniane organizacjom międzynarodowym*.
3. W przypadku przetwarzania danych osobowych osoby niepełnoletniej wymagane jest otrzymanie zgody od ich prawnego opiekuna.
4. Osoba, której dane są przetwarzane ma prawo do: uzyskania informacji, dostępu do danych osobowych, sprostowania danych osobowych, usunięcia danych osobowych, ograniczenia przetwarzania danych osobowych, przenoszenia danych osobowych, sprzeciwu wobec przetwarzania danych osobowych, wniesienia skargi do organu nadzorczego, do zapomnienia.

Rozdział VII.
Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych oraz danych istotnych
§ 12.

1. Wprowadzenie, odpowiednich ze względu na charakter organizacji pracy ADO, ogólnych zasad bezpieczeństwa przetwarzania danych, zgodnie z wymaganiami przepisów prawnych z zakresu ochrony danych osobowych, pozwoli na prawidłowe przetwarzanie danych.
2. Za bezpieczeństwo przetwarzania danych osobowych i danych istotnych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
3. Pracownicy mający dostęp do danych osobowych i danych istotnych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.

4. W miejscu przetwarzania danych osobowych i danych istotnych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe i dane istotne w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
5. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe i dane istotne musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np.: z wykorzystaniem niszczarek.
6. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe i dane istotne poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe i dane istotne odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
7. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe lub dane istotne jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
8. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe i dane istotne w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

Rozdział VIII.
Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych i danych istotnych
§ 13.

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych w systemach informatycznych przez osobę przetwarzającą dane osobowe lub dane istotne bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych, jest zobowiązana fakt ten niezwłocznie zgłosić ASI.
2. Do czasu przybycia na miejsce naruszenia ochrony danych ASI lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
    2) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe;
    3) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
    4) udokumentować wstępnie zaistniałe naruszenie;
    5) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ASI lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia ochrony danych osobowych lub danych istotnych, ASI lub osoba go zastępująca:
    1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania;
    2) wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

4. ASI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport w ciągu 48 godzin od incydentu, według wzoru stanowiącego załącznik nr 6 do PBI.
5. Raport, o którym mowa w ust. 4, ASI niezwłocznie przekazuje IODO, a w przypadku jego nieobecności osobie wyznaczonej.
6. W ciągu 72 godzin od incydentu IODO ma obowiązek zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, ASI zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i wskazuje termin wznowienia przetwarzania danych.

Rozdział IX.
Kontrola przetwarzania i stanu zabezpieczenia danych osobowych
§ 14.

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Akademii im. Jakuba z Paradyża sprawuje IODO oraz ASI – w odniesieniu do danych osobowych i danych istotnych przetwarzanych w systemach informatycznych służących do przetwarzania tych danych.
2. Wzór protokołu z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających stanowi załącznik nr 7 do PBI.
3.

Rozdział X.
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych
§ 15.

1. Wykaz zastosowanych środków technicznych i organizacyjnych przedstawiono w załączniku nr 8 do PBI.
2. Wzór, o którym mowa w ust. 1, zawiera wykaz środków technicznych i organizacyjnych, które zostały zastosowane przez ADO w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych.