REGULAMIN
REALIZACJI ZADAŃ
INSPEKTORA OCHRONY DANYCH

§ 1.
POWOŁYWANIE IOD

1. Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, zwany dalej „Administratorem" albo „UKSW" albo „Uczelnią", jako jednostka sektora finansów publicznych, której działalność opiera się na operacjach przetwarzania danych na dużą skalę, w związku z art. 8 i art. 9 pkt 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), zwanej dalej „Ustawą", jest zobowiązany do wyznaczenia Inspektora Ochrony Danych, zwanego dalej „IOD", dla właściwego zapewnienia ochrony przetwarzania danych osobowych.
2. IOD w UKSW jest osobą fizyczną, zatrudnioną na umowę o pracę i zajmuje wyodrębnione stanowisko w strukturze organizacyjnej UKSW na mocy decyzji Rektora, utworzone w oparciu o przepisy prawa wewnętrznego Uczelni.
3. IOD w strukturze organizacyjnej podlega bezpośrednio najwyższemu kierownictwu Administratora, co oznacza Rektora lub osoby pełniące funkcje w ramach organu najwyższego kierownictwa, tj.: wyznaczeni prorektorzy.
4. Administrator powiadamia Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem UODO" lub „organem nadzorczym", o wyznaczeniu IOD, oraz aktualizuje zmiany w tym zakresie. Dane kontaktowe IOD są publikowane niezwłocznie po jego wyznaczeniu w miejscu ogólnie dostępnym, w szczególności na stronie internetowej Uczelni i w Biuletynie Informacji Publicznej.

§ 2.
ZASTĘPCA IOD

1. Administrator, w celu zachowania ciągłości pracy IOD, może wyznaczyć osobę zastępującą IOD w czasie jego nieobecności, o czym powiadamia organ nadzorczy.
2. W związku z wykonywaniem obowiązków w czasie nieobecności IOD, do osoby go zastępującej, stosuje się odpowiednio przepisy dotyczące IOD.

§ 3.
OPIS STANOWISKA I KOMPETENCJI IOD

1. IOD pełni w UKSW rolę doradczą i weryfikacyjną wobec działań Administratora oraz osób zajmujących się przetwarzaniem danych osobowych. Zadania IOD i sposób ich realizacji są ściśle powiązane z obowiązkami Administratora.
2. IOD powinien posiadać kwalifikacje zawodowe obejmujące :
   1) wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych, w szczególności znajomości przepisów rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L 119/1 z dnia 4 maja 2016 r.), zwanego dalej „RODO", przepisów sektorowych w obszarze realizacji obowiązków prawnych ciążących na Administratorze, w tym przepisów dotyczących szkolnictwa wyższego i prawa pracy;
   2) kompetencje adekwatne do charakteru, stopnia skomplikowania i ilości danych przetwarzanych

w UKSW, w zakresie znajomości:

a) procesów przetwarzania, systemów informatycznych oraz zabezpieczeń stosowanych u Administratora,

b) procedur administracyjnych i organizacyjnych funkcjonowania jednostki.

3. Do kompetencji niezbędnych w realizacji zadań IOD należą:
   1) znajomość i zrozumienie zasad legalnego przetwarzania, ograniczenia celu, minimalizacji danych, poprawności danych, ograniczonego okresu przechowywania danych oraz ich integralności, poufności i rozliczalności;
   2) umiejętność zidentyfikowania podstawy prawnej przetwarzania danych w działalności Administratora;
   3) wiedza o sposobach określania odpowiednich środków i treści informacji podawanych osobom, których dane dotyczą;
   4) umiejętność wprowadzenia procedury odbierania i zarządzania wnioskami osób, których dane dotyczą oraz wykonywania ich praw;
   5) znajomość ram prawnych dotyczących powierzenia w kontekście przetwarzania danych osobowych;
   6) umiejętność zidentyfikowania transferu danych poza Unię Europejską oraz zadecydowania, który z prawnych instrumentów przekazania należy zastosować;
   7) umiejętność opracowania polityki określającej wewnętrzne zasady w zakresie ochrony danych oraz współpracy przy wdrożeniu ich u Administratora;
   8) umiejętność zorganizowania oraz przeprowadzenia audytu dotyczącego ochrony danych;
   9) umiejętność opracowania i współpracy przy tworzeniu rejestru czynności przetwarzania, rejestru kategorii czynności przetwarzania oraz dokumentacji dotyczącej naruszeń danych, a także przygotowania dokumentacji niezbędnej do udowodnienia zgodności z przepisami o ochronie danych;
   10) umiejętność oszacowania środków ochrony danych na podstawie projektu oraz domyślnej ochrony danych dostosowanych do ryzyka i charakteru operacji przetwarzania;
   11) wiedza pozwalająca uczestniczyć w określeniu środków bezpieczeństwa dostosowanych do ryzyka oraz charakteru operacji przetwarzania;
   12) umiejętność identyfikacji naruszeń ochrony danych osobowych wymagających powiadomienia organu nadzorczego oraz poinformowania osób, których dane dotyczą;
   13) umiejętność określenia, czy konieczne jest przeprowadzenie oceny skutków dla ochrony danych (DPIA) czy też nie;
   14) umiejętność przeprowadzenia oceny skutków dla ochrony danych (DPIA);
   15) umiejętność udzielenia porady na temat oceny skutków dla ochrony danych, w szczególności w zakresie metodologii, ewentualnego powierzenia przetwarzania, środków organizacyjnych i technicznych, które należy przyjąć;
   16) umiejętność zarządzania relacjami z organami nadzorczymi poprzez udzielanie odpowiedzi na ich pytania i ułatwiając ich działanie (w szczególności badanie skarg i kontrole);
   17) wiedza o sposobie opracowania, wdrożenia, przeprowadzania szkoleń i warsztatów w zakresie ochrony danych;
   18) umiejętność zapewnienia możliwości sprawdzenia swoich działań, w szczególności za pomocą temu służących narzędzi lub zestawień rocznych i raportów.

4. Uwzględniając kompetencje, o których mowa w ust. 3, minimalne wymagania dla kandydata na stanowisko IOD mogą obejmować doświadczenie zawodowe trwające co najmniej 2 lata na stanowisku IOD oraz odbyte szkolenia z zakresu ochrony danych osobowych lub wykształcenie kierunkowe z zakresu ochrony danych osobowych i minimum 2 lata doświadczenia zawodowego, np. we współpracy z IOD.
5. IOD zobowiązany jest wypełniać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania danych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania danych w interesie Administratora, jako ekspert, a także jako niezależny, proaktywny i wiarygodny organ w dziedzinie prywatności i ochrony danych osobowych.
6. IOD powinien w swoich działaniach opierać się na rzeczywistym stanie faktycznym badanej sprawy, nie powinien ulegać żadnym naciskom i podporządkowywać swoich opinii innym osobom. Jego nadrzędnym celem w każdej sytuacji powinno być zapewnienie, że przetwarzanie danych będzie następowało zgodnie z prawem poprzez rzetelne podejście do wykonywania swoich obowiązków i wysoki poziom etyki zawodowej.

§ 4.

IOD W STRUKTURZE ORGANIZACYJNEJ UKSW

1. IOD nie może być osobą spokrewnioną z osobami, które kierują lub zarządzają Uczelnią. Przy wyznaczaniu IOD, w tym jego zastępcy konieczna jest analiza i ocena, czy określone relacje pokrewieństwa nie będą miały wpływu na wykonywanie zadań i obowiązków IOD w sposób niezależny i nie będą powodować konfliktu interesów.
2. Ze stanowiskiem IOD i zastępcy IOD nie można łączyć funkcji pełnomocnika ds. ochrony informacji niejawnych.
3. Do stanowisk niekompatybilnych z pełnieniem funkcji IOD, które powodują konflikt interesów należą funkcje i stanowiska administracyjne wchodzące w skład kadry zarządzającej jak i kierownicze niższego szczebla, o których mowa w przepisach wewnętrznych UKSW, właściwych do spraw organizacyjnych i zatrudnienia, a w szczególności: osoba pełniąca stanowisko lub funkcję w organach zarządczych Uczelni, kanclerz, kwestor, kierownik działu IT, dyrektor i kierownik jednostki właściwej do spraw kadr i płac, jak też inne stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych.

§ 5.

1. Konflikt interesów, o którym mowa w § 4 ust. 3 następuje, w sytuacji gdy nie można pogodzić prawidłowego wykonywania zadań inspektora, przypisanych mu w art. 38 ust. 4 oraz art. 39 RODO, z realizacją innych zadań, pomiędzy którymi występuje sprzeczność, uniemożliwiająca odpowiednią ich realizację. Sprzeczność może wynikać z występowania przez IOD jednocześnie w dwóch rolach lub podejmowania przez IOD działań lub decyzji, które następnie muszą podlegać jego ocenie w zakresie art. 39 ust. 1 lit. a RODO, zwłaszcza w sytuacji, gdy IOD jest obciążany obowiązkami, które przepisy nakładają na Administratora.
2. W przypadku, gdy IOD będzie wykonywał dodatkowo inne zadania i obowiązki, ponad te wynikające z RODO, Administrator powinien zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów, który może być również rezultatem nadmiaru przydzielonych obowiązków, w sytuacji, gdy musi on wybrać między obowiązkami jakie będzie realizował, a którym nie podoła z powodu braku czasu koniecznego na ich wykonanie.
3. IOD nie może podejmować się realizacji zadań, które mogą stać się w dalszej kolejności przedmiotem dokonywania przez niego czynności monitorowania, ani podejmować decyzji w zakresie celów i środków dotyczących przetwarzania i zabezpieczania danych.

§ 6.

GWARANCJA NIEZALEŻNOŚCI

1. Istotą funkcji IOD jest obiektywne i niezależne wykonywanie przez niego zadań określonych w art. 39 ust. 1 RODO.
2. Gwarancją niezależności IOD jest w szczególności:
   1) zatrudnienie IOD w bezpośredniej podległość najwyższemu kierownictwu;
   2) wspieranie IOD w wypełnianiu jego zadań;
   3) zapewnienie udziału IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych;
   4) zakaz wydawania IOD instrukcji i poleceń co do wykonywania przez niego zadań, o którym mowa w ust. 3;
   5) unikanie konfliktu interesów w związku z realizacją obowiązków IOD;
   6) zakaz odwoływania i karania IOD za obiektywnie prawidłowe wypełnianie przez niego zadań.
3. Zakaz wydawania instrukcji IOD, o którym mowa w ust. 2 pkt 4 oznacza, że w ramach wypełniania swoich zadań IOD, nie może otrzymywać poleceń dotyczących sposobu załatwienia sprawy, które określałyby sposób przekazywania wyników swojej pracy w związku z przeprowadzonym sprawdzeniem/audytem, środki jakie mają zostać podjęte, cel jaki powinien zostać osiągnięty oraz czy należy przeprowadzić konsultacje z organem nadzorczym.

§ 7.

ZADANIA I UPRAWNIENIA IOD

1. Do zadań IOD należą:
   1) zapoznawanie, w formie ustnie lub pisemnie, w postaci papierowej, elektronicznej lub za pośrednictwem środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2019 r. poz. 123 i 730), Administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami o ochronie danych osobowych, ze szczególnym uwzględnieniem przepisów określających obowiązki spoczywające na tych osobach w związku z przetwarzaniem przez nie danych osobowych i prowadzenie doradztwa w tym zakresie;
   2) monitorowanie regulaminów i polityk Administratora w dziedzinie ochrony danych osobowych oraz powiązane z tym sprawdzenia/audyty, zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektorów ochrony danych;
   3) przygotowywanie, w porozumieniu z Administratorem, dla osób, które uczestniczą w operacjach przetwarzania danych osobowych:
      a) cyklicznych lub organizowanych w zależności od bieżących potrzeb instruktaży, w tym z wykorzystaniem technologii informatycznych,
      b) udostępnianie materiałów do samokształcenia kierowanego, w tym z wykorzystaniem technologii informatycznych lub w celu realizacji samokształcenia online, przy jednoczesnym zapewnieniu konsultacji umożliwiających uzyskanie, aktualizowanie lub uzupełnianie wiedzy i umiejętności w zakresie przetwarzania danych osobowych oraz obowiązujących przepisów o ochronie danych osobowych;
   4) udzielanie, na polecenie Administratora, zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   5) współpraca z Prezesem UODO, zgodnie z artykułem 39 ust. 1 lit. d RODO;

6) pełnienie funkcji punktu kontaktowego dla Prezesa UODO w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
7) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

2. Działania, o których mowa w ust. 1 pkt 2 oznaczają:
   1) zbieranie informacji w celu identyfikacji procesów przetwarzania i stosowania środków technicznych i organizacyjnych zapewniających bezpieczeństwo ochrony danych osobowych;
   2) analizowanie i sprawdzanie zgodności przetwarzania;
   3) informowanie, doradzanie i rekomendowanie określonych działań zwiększających świadomość personelu uczestniczącego w operacjach przetwarzania, w zakresie prawidłowego sposobu wypełniania obowiązków wynikających z przepisów o ochronie danych osobowych.
3. Administrator dokonując oceny, o której mowa w ust. 1 pkt 4 powinien konsultować się z IOD w następujących kwestiach:
   1) konieczności przeprowadzenia oceny skutków dla ochrony danych;
   2) metodologii przeprowadzenia oceny skutków dla ochrony danych;
   3) konieczności przeprowadzenia wewnętrznej oceny lub zlecenia jej podmiotowi zewnętrznemu;
   4) zabezpieczeń, w tym środków technicznych i organizacyjnych, stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
   5) prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO.
4. IOD jest zobowiązany do przestrzegania wszystkich przepisów prawa krajowego i unijnego, które będą miały do niego zastosowanie i na mocy których określone informacje objęte są prawnie chronionymi tajemnicami.
5. IOD jest zobowiązany do przestrzegania tajemnicy i poufności, aby zapewnić bezpieczeństwo danych osobowych i budować zaufanie do prowadzonej działalności w związku wykonywaniem zadań, które wymagają dostępu do:
   1) danych osobowych, w tym danych osobowych, o których mowa w art. 9 ust. 1 RODO;
   2) danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 RODO;
   3) informacji dotyczących środków technicznych i organizacyjnych zapewniających przetwarzanie zgodne z przepisami RODO, w tym polityk ochrony danych.
6. Obowiązek zachowania tajemnicy oraz poufności nie uniemożliwia IOD kontaktu z Prezesem UODO i zasięgania jego opinii.
7. W ramach prowadzonych sprawdzeń, IOD gromadzi informacje od Administratora lub osób odpowiedzialnych za bezpieczeństwo przetwarzania danych osobowych, dokonuje analizy tych informacji oraz ustalania stanu realizacji zaleceń.
8. IOD jest uprawniony do uzyskania wszelkich informacji i niezbędnego wsparcia w zakresie operacji przetwarzania danych osobowych od wszystkich jednostek organizacyjnych UKSW.
9. IOD prowadzi pisemną dokumentację swoich czynności, w tym:
   1) sporządza dla Administratora pisemne sprawozdania z wykonania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych w wyniku prowadzonych sprawdzeń i analiz stanu

faktycznego przetwarzania danych osobowych;

2) przekazuje Administratorowi sprawozdanie, o którym mowa w pkt 1, nie rzadziej niż raz w roku, w sposób uniemożliwiający zapoznanie się z jego treścią osobom nieupoważnionym.

§ 8.

OBOWIĄZKI ADMINISTRATORA WOBEC IOD

1. Administrator jest zobowiązany do wspierania IOD poprzez zapewnienie mu zasobów niezbędnych do wykonania jego zadań, zgodnie z art. 38 RODO. Przez zasoby rozumie się:
   1) aktywne wsparcie IOD ze strony kadry kierowniczej (np. cykliczne spotkania);
   2) ustalenie wymiaru czasu, który umożliwi IOD wykonywanie zadań;
   3) udzielanie odpowiedniego wsparcia infrastrukturalnego (pomieszczenia, sprzęt biurowy i komputerowy, licencje na oprogramowanie, wyposażenie biurowe);
   4) zobowiązanie pracowników jednostek organizacyjnych Uczelni do udzielania IOD niezbędnych informacji i wsparcia dotyczących operacji przetwarzania danych osobowych;
   5) wspomaganie doskonalenia zawodowego przez zapewnienie zasobów finansowych, niezbędnych do utrzymania i rozwoju wiedzy fachowej;
   6) udzielanie wsparcia kadrowego, np. powołanie zespołu inspektora ochrony danych, organizacja sekretariatu.
2. Administrator ponosi odpowiedzialność za właściwie i niezwłocznie włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych od najwcześniejszego etapu, tak by ułatwić zapewnienie zgodności z RODO, a w szczególności za:
   1) zapewnienie udziału, z głosem doradczym w spotkaniach przedstawicieli kadry kierowniczej wyższego i średniego szczebla (np.: kolegium rektorskie, rada rektorska, spotkania z kierownikami jednostek) oraz uczestnictwa w podejmowaniu decyzji mających wpływ na ochronę danych;
   2) udostępnienie niezbędnych informacji odpowiednio wcześniej, umożliwiając IOD zajęcie stanowiska;
   3) uwzględnianie opinii IOD, w szczególności w ocenie ryzyka związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko;
   4) udzielanie zwrotnego pisemnego uzasadnienia w przypadku braku uwzględnienia zaleceń przekazanych przez IOD.
3. Niezwłoczna konsultacja z IOD powinna następować w sytuacji, gdy:
   1) dojdzie do stwierdzenia naruszenia ochrony danych lub innego zdarzenia związanego z danymi osobowymi;
   2) uruchamiane są nowe procesy lub systemy;
   3) dokonywane są zmiany w istniejących procesach lub systemach;
   4) zaistnienia konieczności angażowanie podmiotów przetwarzających.

§ 9.

DZIAŁANIA NIEDOZWOLONE WOBEC IOD

Przez działania niedozwolone wobec IOD rozumie się:

1) próby wywierania nacisku na IOD przez wydawanie instrukcji dotyczących wykonywania jego zadań w szczególności: instrukcji dotyczących wyników, jakie IOD ma osiągnąć, sposobu

rozpatrywania skargi lub tego, czy należy przeprowadzić konsultacje z organem nadzorczym;

2) próby obligowania IOD do przyjęcia określonego stanowiska w sprawie przepisów dotyczących ochrony danych np. określonej wykładni przepisów;
3) odwoływanie lub ukaranie IOD, o których mowa w § 6 ust. 2 pkt 6 za wypełnianie swoich zadań, np. za dokonanie zgłoszenia incydentu naruszenia ochrony danych osobowych do organu nadzorczego mimo sprzeciwu Administratora;
4) delegowanie podległości IOD na inną osobę lub jednostkę organizacyjną, niż najwyższe kierownictwo Administratora, o którym mowa w § 1 ust. 3 niniejszego Regulaminu;
5) zobowiązanie IOD do poniesienia osobistej odpowiedzialności za przypadki naruszenia przepisów RODO w uczelni.

§ 10.

OCENA DZIAŁAŃ I WSPÓŁPRACA IOD Z AUDYTOREM

1. Działania IOD, jak i audytora wewnętrznego powinny być komplementarne, gdyż wspierają kierownika jednostki w realizacji jej celów i zadań, jakimi są:
   1) monitorowanie zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa;
   2) ocena zgodności działalności jednostki z przepisami prawa (również przepisami prawa o ochronie danych osobowych) oraz procedurami wewnętrznymi, a także skuteczności i efektywności działania, ochrony zasobów oraz zarządzania ryzykiem.
2. Audytor wewnętrzny, dokonując systematycznej oceny kontroli zarządczej we wszystkich obszarach jednostki, obejmuje również działania podejmowane przez IOD w zakresie prawidłowości wykonywania przez niego obowiązków, mając na uwadze gwarancję niezależności IOD, o której mowa w § 6 ust. 2 pkt 4 Regulaminu.
3. Ostateczną decyzję co do oceny wyników audytu podejmuje Administrator. IOD musi mieć możliwość przedstawienia swojego stanowiska w zakresie, o którym mowa w zdaniu 1. Racje obu stron powinny zostać uzasadnione i udokumentowane w celach dowodowych.

§ 11.

OBSŁUGA ADMINISTRACYJNA ZGŁOSZEŃ

1. W zakresie działalności związanej z wykonaniem przepisów o ochronie danych osobowych nie nadaje się biegu skargom i zgłoszeniom anonimowym, w przypadku ich oczywistej bezzasadności stwierdzonej w wyniku wstępnej weryfikacji.
2. Rozpatruje się zgłoszenia złożone w formie pisemnej, w tym w formie elektronicznej (mailowo lub za pomocą dedykowanego formularza dostępnego na stronie internetowej Uczelni), w języku urzędowym, które zawierają szczegółowe informacje, biorąc pod uwagę:
   1) charakter i wagę zarzucanych naruszeń zasad ochrony danych;
   2) znaczenie szkody, jaką poniósł lub mógł ponieść jeden lub więcej podmiotów danych w wyniku naruszenia;
   3) prawdopodobieństwo ustalenia, że doszło do naruszenia;
   4) dokładną datę, w której miały miejsce dane zdarzenia, dane zachowanie przestało wywoływać skutki, skutki zostały usunięte lub zapewniono odpowiednią gwarancję takiego usunięcia.
3. Nie ujawnia się tożsamość skarżącego. Tożsamość skarżącego ujawnia się wyłącznie w zakresie niezbędnym do właściwego rozpatrzenia zgłoszenia, w szczególności na wniosek podmiotów

upoważnionych przez przepisy prawa.

4. Nie ujawnia żadnych dokumentów związanych z naruszeniem, z wyjątkiem anonimowych fragmentów lub streszczeń ostatecznej decyzji, chyba że dana osoba wyrazi zgodę na takie ujawnienie.
5. Jeżeli wymagają tego okoliczności skargi, IOD współpracuje z właściwymi organami nadzoru, działającymi w ramach swoich prawnie uzasadnionych kompetencji.
6. Po otrzymaniu zgłoszenia o naruszeniu, niezwłocznie powiadamia się skarżącego o wyniku postępowania dotyczącego skargi i podjętych działaniach.