UNIWERSYTET JAGIELLOŃSKI
W KRAKOWIE

75.0200.35.2018

Zarządzenie nr 38
Rektora Uniwersytetu Jagiellońskiego
z 30 maja 2018 roku

w sprawie: ochrony danych osobowych w Uniwersytecie Jagiellońskim

Na podstawie § 27 ust. 4a Statutu Uniwersytetu Jagiellońskiego, w celu stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE.L.2016.119.1), zwanego dalej „RODO", oraz na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000), zwanej dalej „UODO", zarządzam, co następuje:

§ 1

1. Przetwarzanie danych osobowych w Uniwersytecie Jagiellońskim służy realizacji zadań wynikających z ustawy o szkolnictwie wyższym oraz ze Statutu Uniwersytetu Jagiellońskiego.
2. 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.
3. Przetwarzanie danych osobowych w Uniwersytecie Jagiellońskim może odbywać się w systemie informatycznym, a także w dokumentacji papierowej, wyłącznie w celu realizacji zadań, o których mowa w ust. 1.

§ 2

1. Administratorem Danych jest Uniwersytet Jagielloński reprezentowany przez Rektora UJ.
2. Zadania i obowiązki Administratora Danych określa załącznik nr 1 do niniejszego zarządzenia.

§ 3

Obowiązki wynikające z RODO powierza się następującym osobom:
1) Inspektorowi Ochrony Danych;
2) Specjalistom ds. ochrony danych i ich zastępcom, jeżeli zostaną wyznaczeni.

§ 4

1. Inspektora Ochrony Danych wyznacza Rektor UJ.

2. Inspektor Ochrony Danych, zwany dalej „IOD”, podlega bezpośrednio Rektorowi UJ.
3. W celu realizacji przez IOD powierzonych zadań Administrator Danych zapewnia:
   1) właściwe i niezwłoczne włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych w Uniwersytecie Jagiellońskim;
   2) środki niezbędne do ich wykonania oraz dostęp do danych osobowych i operacji przetwarzania danych, a także środki niezbędne do utrzymania jego wiedzy fachowej;
   3) niezależność IOD w zakresie wykonywanych przez niego zadań.
4. Administrator Danych nie może odwołać ani karać IOD za wypełnianie jego zadań zgodnie z obowiązującymi regulacjami prawnymi, w tym niniejszym zarządzeniem.
5. Osoba pełniąca w dniu 24 maja 2018 r. funkcję Administratora Bezpieczeństwa Informacji staje się Inspektorem Ochrony Danych i pełni swoją funkcję do dnia 1 września 2018 r., a po tej dacie, jeżeli do tego dnia Administrator Danych zawiadomi Prezesa Urzędu Ochrony Danych Osobowych, zwanego dalej „Prezesem Urzędu”, o jej wyznaczeniu w sposób określony w art. 10 UODO.
6. Administrator Danych niezwłocznie po wyznaczeniu IOD podaje jego dane na stronie internetowej UJ.
7. Administrator Danych zawiadamia Prezesa Urzędu o każdej zmianie danych zgłoszonych zgodnie z UODO oraz o odwołaniu IOD, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.
8. Szczegółowy zakres zadań i obowiązków IOD stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 5

1. Specjalistami ds. ochrony danych są:
   1) Dziekani – odpowiedzialni za przetwarzanie danych osobowych na wydziałach;
   2) Prorektorzy, Kanclerz, zastępcy Kanclerza, Kwestor, zastępcy Kwestora – odpowiedzialni za przetwarzanie danych osobowych w podporządkowanych im jednostkach organizacyjnych UJ, z wyłączeniem bibliotek UJ i UJ CM;
   3) Dyrektor Biblioteki Jagiellońskiej – odpowiedzialny za przetwarzanie danych osobowych we wszystkich bibliotekach UJ i UJ CM.
2. Prorektor UJ ds. Collegium Medicum koordynuje działanie specjalistów ds. ochrony danych działających w Uniwersytecie Jagiellońskim – Collegium Medicum.
3. Szczegółowy zakres zadań i obowiązków Specjalistów ds. ochrony danych i ich zastępców stanowi załącznik nr 3 do niniejszego zarządzenia.

§ 6

1. Administrator Danych uwzględniając charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych odbywało się zgodnie z RODO.
2. Administrator Danych ponosi ciężar dowodu przetwarzania danych osobowych w UJ zgodnie z prawem.
3. Środki techniczne i organizacyjne, o których mowa w ust. 1, obejmują wdrożenie przez Administratora Danych odpowiednich polityk ochrony danych.

§ 7

1. Administrator Danych wprowadza „Politykę Bezpieczeństwa w Uniwersytecie Jagiellońskim”, stanowiącą załącznik nr 4 do niniejszego zarządzenia, zwaną dalej

„Polityką Bezpieczeństwa”. W przypadku realizacji projektów (jeżeli wynika to z umów projektowych), tworzy się na potrzeby ich realizacji indywidualne polityki bezpieczeństwa zgodne z Polityką Bezpieczeństwa.
2. Administrator Danych wprowadza „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Jagiellońskim”, stanowiącą załącznik nr 5 do niniejszego zarządzenia, zwaną dalej „Instrukcją Zarządzania Systemem Informatycznym”. W przypadku realizacji projektów (jeżeli wynika to z umów projektowych), tworzy się na potrzeby ich realizacji indywidualne instrukcje zarządzania systemem informatycznym zgodne z Instrukcją Zarządzania Systemem Informatycznym.

§ 8

1. Osoby, których dane są przetwarzane w jednostkach organizacyjnych UJ, mają prawo do ochrony danych ich dotyczących, ich uaktualnienia lub poprawiania, zgłaszania sprzeciwu wobec przetwarzania na zasadach określonych w RODO, jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.
2. Administrator Danych w celu wypełnienia obowiązku informacyjnego wobec osób, których dane osobowe są przetwarzane w UJ, jest zobowiązany do podania osobie, której dane dotyczą, wszystkich informacji wymaganych zgodnie z RODO (tzw. klauzula informacyjna). Wzory klauzul informacyjnych określa IOD.
3. Klauzule informacyjne dla poszczególnych przypadków mogą być tworzone przez pracowników jednostek organizacyjnych UJ lub UJ CM na potrzeby konkretnych przypadków zgodnie ze wzorami określonymi przez IOD, jednak są oni zobowiązani do konsultowania treści klauzul z IOD. Wzór klauzuli informacyjnej określa załącznik nr 6 do niniejszego zarządzenia.
4. 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.

§ 9

1. Osoba, której dane dotyczą, ma prawo otrzymać od Administratora Danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora Danych, jeżeli:
   1) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy;
   2) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądać przesłania przez Administratora Danych jej danych osobowych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

§ 10

1. Osoba, której dane dotyczą, ma prawo żądać od Administratora Danych niezwłocznego usunięcia dotyczących jej danych osobowych („prawo do bycia zapomnianym”), a Administrator Danych ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   1) dane osobowe nie są już niezbędne do celów, dla jakich zostały zebrane lub w inny sposób przetwarzane;

2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania tych danych;
3) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych osobowych z przyczyn związanych z jej szczególną sytuacją i nie występują nadrzędne, prawnie uzasadnione podstawy przetwarzania tych danych;
4) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych na potrzeby marketingu bezpośredniego;
5) dane osobowe były przetwarzane niezgodnie z prawem;
6) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa polskiego, któremu podlega Administrator Danych;
7) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w RODO.

2. „Prawo do bycia zapomnianym" nie ma zastosowania w UJ w zakresie, w jakim przetwarzanie danych osobowych jest niezbędne:
1) do wywiązania się przez Administratora Danych z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa polskiego;
2) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
3) do celów ustalenia, dochodzenia roszczeń lub ochrony praw.

§ 11

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy spełniającej warunki określone w RODO, przetwarzanie danych osobowych w tym podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w tej umowie. Podmiot, któremu powierzono przetwarzanie danych osobowych odpowiada za należyte ich przetwarzanie solidarnie z Administratorem Danych.

§ 12

1. Udostępnianie danych osobowych instytucjom i osobom trzecim może następować tylko za pośrednictwem Specjalistów ds. ochrony danych, chyba że odbywa się na podstawie pisemnej umowy między Uniwersytetem Jagiellońskim a odbiorcą lub podmiotem przetwarzającym.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
3. Specjalista ds. ochrony danych prowadzi ewidencję udostępniania danych osobowych. Ewidencja nie obejmuje tych udostępnień, o których informacje można uzyskać w każdym czasie bezpośrednio z systemu informatycznego.
4. Specjalista ds. ochrony danych przekazuje IOD ewidencję, o której mowa w ust. 3, w terminie do 15 stycznia danego roku za rok poprzedni.
5. Udostępnienie danych osobowych przez Administratora Danych osobom trzecim, jeżeli obowiązek udostępnienia nie wynika z przepisów prawa, musi być uprzednio zaakceptowane przez IOD albo Pełnomocnika Rektora UJ ds. prawnych lub Współpracownika Pełnomocnika Rektora UJ ds. prawnych, bądź w odniesieniu do danych osobowych udostępnianych w ramach UJ CM – przez radcę prawnego UJ CM.

§ 13

1. Do przetwarzania danych osobowych w UJ dopuszczone są wyłącznie osoby upoważnione przez Administratora Danych.
2. Z dniem 1 stycznia 2019 roku wygasają wydane na podstawie dotychczas obowiązujących przepisów upoważnienia do przetwarzania danych osobowych i oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych, a także uprawnienia dostępu do systemów informatycznych USOS oraz SAP.
3. Upoważnienia do przetwarzania danych osobowych zgodne z nowym wzorem, a także nowe uprawnienia dostępu do systemów informatycznych USOS oraz SAP należy nadać do 31 grudnia 2018 roku. Podstawą ponownego przyznania uprawnień dostępu do systemów SAP oraz USOS jest nowe upoważnienie do przetwarzania danych osobowych.

§ 14

Tracą moc:

1) zarządzenie nr 14 Rektora Uniwersytetu Jagiellońskiego z 10 lutego 2006 roku w sprawie ochrony danych osobowych przetwarzanych w Uniwersytecie Jagiellońskim (z późn. zm.);
2) zarządzenie nr 22 Rektora Uniwersytetu Jagiellońskiego z 9 marca 2006 roku w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych przetwarzanych w Uniwersytecie Jagiellońskim;
3) zarządzenie nr 29 Rektora Uniwersytetu Jagiellońskiego z 24 marca 2006 roku w sprawie wprowadzenia Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie Jagiellońskim.

§ 15

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

Prof. dr hab. med. Wojciech Nowak

Zadania i obowiązki Administratora Danych

Administrator Danych ustala cele i sposoby przetwarzania danych osobowych w Uniwersytecie Jagiellońskim, jak również zapewnia bezpieczeństwo przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych:

1. Administrator Danych wdraża i wprowadza do stosowania w Uniwersytecie Jagiellońskim polityki i procedury z zakresu ochrony danych osobowych, a także może wdrożyć kodeksy postępowania zatwierdzone przez Prezesa Urzędu Ochrony Danych Osobowych.
2. Administrator Danych wdraża w Uniwersytecie Jagiellońskim rekomendacje Prezesa Urzędu Ochrony Danych Osobowych.
3. Administrator Danych we współpracy z IOD prowadzi rejestr czynności przetwarzania danych (załącznik nr 1 do Polityki Bezpieczeństwa), a także rejestr kategorii czynności przetwarzania (załącznik nr 2 do Polityki Bezpieczeństwa) w razie przetwarzania danych osobowych w imieniu i na rzecz innego administratora danych osobowych.
4. Administrator Danych, po konsultacji z IOD, dokonuje oceny skutków dla ochrony danych (załącznik nr 3 do Polityki Bezpieczeństwa). Ocenę skutków dla ochrony danych wykonuje się przed rozpoczęciem przetwarzania danych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele, z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Wykonując ocenę skutków dla ochrony danych, Administrator Danych bierze pod uwagę rodzaj zagrożenia określony w Wykazie typowych zagrożeń (ryzyka) stanowiącym załącznik nr 4 do Polityki Bezpieczeństwa oraz podatność danych na zagrożenia (ryzyko), której przykłady określa załącznik nr 5 do Polityki Bezpieczeństwa.

Zadania i obowiązki Inspektora Ochrony Danych (IOD)

1. Inspektor Ochrony Danych (IOD) wypełnia swoje zadania z uwzględnieniem ryzyka związanego z operacjami przetwarzania danych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
2. Do zadań IOD należy:
   1) informowanie Administratora Danych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   2) monitorowanie przestrzegania RODO, innych przepisów Unii Europejskiej lub prawa polskiego o ochronie danych oraz polityk Administratora Danych lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość w zakresie ochrony danych;
   3) prowadzenie szkoleń dla osób uczestniczących w operacjach przetwarzania danych osobowych, w tym: szkolenie wstępne pracowników przed przyjęciem do pracy oraz szkolenia organizowane w poszczególnych jednostkach organizacyjnych UJ i UJ CM, szkolenia stanowiskowe w trakcie audytów i sprawdzeń dokonywanych przez IOD, szkolenia doraźne, publikowanie newslettera dla pracowników, szkolenia e-learningowe;
   4) wykonywanie kontroli i audytów minimum dwa razy w roku w wybranych jednostkach organizacyjnych UJ i UJ CM oraz udokumentowanie ich raportami do Administratora Danych;
   5) kontrolowanie przestrzegania przetwarzania danych osobowych oraz prowadzenia dokumentacji we wszystkich jednostkach organizacyjnych UJ i UJ CM, raportowanie stanu faktycznego wraz z rekomendacjami do Administratora Danych;
   6) udzielanie na żądanie Administratora Danych zaleceń co do oceny skutków przetwarzania dla ochrony danych (załącznik nr 3 do Polityki Bezpieczeństwa) oraz monitorowanie ich wykonania;
   7) współpraca z Prezesem Urzędu Ochrony Danych Osobowych;
   8) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w sprawach związanych z przetwarzaniem danych, w tym w zakresie składanych przez Administratora Danych wniosków o uprzednie konsultacje, o których mowa w RODO;
   9) pełnienie funkcji punktu kontaktowego dla osób, których dane są przetwarzane w Uniwersytecie Jagiellońskim;
   10) dokonywanie w każdym czasie sprawdzenia prowadzenia i aktualizacji przez Specjalistów ds. ochrony danych ewidencji udostępniania danych osobowych w danej jednostce organizacyjnej UJ i UJ CM oraz raportowania stanu udostępnień danych do Administratora Danych;
   11) wspieranie Administratora Danych w prowadzeniu rejestru czynności przetwarzania danych (załącznik nr 1 do Polityki Bezpieczeństwa);
   12) wspieranie Administratora Danych w prowadzeniu rejestru kategorii czynności przetwarzania danych (załącznik nr 2 do Polityki Bezpieczeństwa).

Zadania i obowiązki
Specjalistów ds. ochrony danych i ich zastępców

1. Specjalista ds. ochrony danych podlega bezpośrednio Administratorowi Danych, a w zakresie merytorycznym wykonuje wytyczne IOD.
2. Do zadań Specjalistów ds. ochrony danych i ich zastępców należy:
   1) wyznaczenie i upoważnienie w kierowanych przez nich jednostkach organizacyjnych UJ maksymalnie pięciu zastępców odpowiedzialnych za przestrzeganie w tej jednostce przepisów o ochronie danych osobowych;
   2) informowanie IOD o wyznaczeniu oraz odwołaniu zastępcy lub zastępców w terminie 14 dni od daty zaistnienia zdarzenia;
   3) prowadzenie rejestru zastępców Specjalistów ds. ochrony danych oraz odnotowywanie w tym rejestrze każdej zmiany;
   4) prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych w danej jednostce organizacyjnej UJ lub UJ CM zgodnie z załącznikiem nr 11 do Polityki Bezpieczeństwa;
   5) prowadzenie Wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, zgodnie z załącznikiem nr 7 do Polityki Bezpieczeństwa, oraz dokonywanie jego aktualizacji niezwłocznie po nastąpieniu zmiany;
   6) prowadzenie Wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zgodnie z załącznikiem nr 8 do Polityki Bezpieczeństwa, oraz prowadzenie Opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, zgodnie z załącznikiem nr 9 do Polityki Bezpieczeństwa i dokonywanie ich aktualizacji niezwłocznie po nastąpieniu zmiany;
   7) prowadzenie ewidencji wniosków o udostępnianie danych osobowych instytucjom i osobom trzecim (także w przypadku przekazywania ich do państwa trzeciego zgodnie z RODO);
   8) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w podległych jednostkach organizacyjnych oraz ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem oraz prowadzenie opisu tych środków technicznych zgodnie z załącznikiem nr 13 do Polityki Bezpieczeństwa;
   9) zapewnienie dopuszczenia do przetwarzania danych wyłącznie osób posiadających upoważnienie;
   10) kontrolowanie przestrzegania zasad przetwarzania danych osobowych i stosowania w podległej jednostce organizacyjnej UJ lub UJ CM Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym;
   11) zgłoszenie IOD zamiaru stworzenia zbioru danych osobowych w celu wykonania przez Administratora Danych we współpracy z IOD szacowania i analizy ryzyka (załącznik nr 6 do Polityki Bezpieczeństwa) i ustalenia konieczności wykonania oceny skutków dla ochrony danych (załącznik nr 3 do Polityki Bezpieczeństwa) oraz przeprowadzenie w razie konieczności uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych;

12) przekazywanie upoważnień do przetwarzania danych osobowych do DSO i DSO CM w celu włączenia ich do akt osobowych pracowników oraz zarejestrowania w systemie SAP;
13) informowanie nowo przyjętych pracowników oraz pracowników, którym zmienia się zakres obowiązków, o zasadach przetwarzania danych osobowych w UJ i UJ CM;
14) przesyłanie pracownikom przetwarzającym dane drogą mailową materiałów informacyjnych dotyczących aktualizacji zarządzeń dotyczących ochrony danych osobowych, aktualizacji innych dokumentacji oraz materiałów szkoleniowych otrzymywanych od IOD;
15) nadawanie osobom przetwarzającym dane osobowe upoważnień do przetwarzania danych osobowych (formularz stanowi załącznik nr 10 do Polityki Bezpieczeństwa) i uprawnień do systemów informatycznych zgodnie z procedurą stanowiącą załącznik nr 1 do Instrukcji Zarządzania Systemem Informatycznym.

3. Specjalista ds. ochrony danych (zastępca/y) jest zobowiązany do uzupełnienia niżej wymienionej dokumentacji i poinformowania o tym IOD w następujących terminach:
   1) wykazu miejsc przetwarzania danych osobowych w swojej jednostce (załącznik nr 7 do Polityki Bezpieczeństwa) – nie później niż w terminie 30 dni od wejścia w życie niniejszego zarządzenia;
   2) wykazu zbiorów danych osobowych (załącznik nr 8 do Polityki Bezpieczeństwa) – nie później niż w terminie 30 dni od dnia wejścia w życie niniejszego zarządzenia;
   3) opisu struktury zbiorów danych (załącznik nr 9 do Polityki Bezpieczeństwa) – nie później niż w terminie 30 dni od dnia wejścia w życie niniejszego zarządzenia;
   4) ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik nr 11 do Polityki Bezpieczeństwa) – nie później niż w terminie 45 dni od dnia wejścia w życie niniejszego zarządzenia;
   5) zestawienia danych osobowych z informacją, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (załącznik nr 12 do Polityki Bezpieczeństwa) – nie później niż w terminie 45 dni od dnia wejścia w życie niniejszego zarządzenia;
   6) określenia środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (załącznik nr 13 do Polityki Bezpieczeństwa) – nie później niż w terminie 45 dni od dnia wejścia w życie niniejszego zarządzenia.
4. Po upływie terminów, o których mowa w ust. 3, IOD jest upoważniony do sprawdzenia prowadzenia ewidencji w poszczególnych jednostkach organizacyjnych UJ i UJ CM.