ul. Bartycka 18, 00-716 Warszawa
tel: (22) 841 00 41, (22) 3296 100
fax: (22) 841 00 46
email: camk@camk.edu.pl
http://www.camk.edu.pl

CENTRUM ASTRONOMICZNE IM. MIKOŁAJA KOPERNIKA PAN

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 1

Niniejszym Centrum Astronomiczne im. M. Kopernika PAN ustanawia politykę bezpieczeństwa danych osobowych (PBDO, Polityka), która określa cele i zasady jakim podlega bezpieczeństwo danych osobowych w instytucie zgodnie z przepisami 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 osobowych), zwanego dalej Rozporządzeniem.

§ 2
Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć osobę wyznaczoną przez ADO, odpowiedzialną za nadzór nad przestrzeganiem zasad ochrony danych osobowych w instytucie;

2) **administratorze danych osobowych (ADO)** – należy przez to rozumieć Centrum Astronomiczne im. M. Kopernika PAN;

3) **analizie ryzyka** – należy przez to rozumieć proces mający na celu oszacowanie wagi ryzyka rozumianej jako funkcja prawdopodobieństwa wystąpienia skutku i krytyczności jego następstw dla instytutu;

4) **autentyczności** – należy przez to rozumieć właściwość oznaczającą, że zawartość zasobu informatycznego oraz tożsamość osoby lub innego systemu informatycznego, mającego dostęp do tego zasobu jest taka, jak deklarowana;

5) **danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane przez Administratora Danych zarówno w systemach informatycznych, jak i tradycyjnie;

6) **zbiorze danych** – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) **dostępności informacji** – należy przez to rozumieć prawdopodobieństwo, że w ustalonej chwili osoby upoważnione będą miały dostęp do danych osobowych, a system będzie poprawnie realizował usługi zlecone przez użytkownika;

8) **haśle** – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi;

9) **naruszeniu ochrony danych osobowych** – należy przez to rozumieć 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) **integralności danych** – należy przez to rozumieć właściwość zasobu informatycznego oznaczającą, że nie nastąpiła nieautoryzowana zmiana;

11) **koncie administracyjnym** – należy przez to rozumieć konto w systemie informatycznym wykorzystywane przez administratora systemu lub upoważnione osoby w celu zapewnienia prawidłowego funkcjonowania systemu;
12) **mechanizmie kontroli** – należy przez to rozumieć rozwiązanie techniczne, organizacyjne, proceduralne służące ochronie informacji i ograniczające ryzyko; po wdrożeniu właściwego mechanizmu kontrolnego pozostaje jedynie ryzyko szczątkowe;
13) **nośniku informacji** – należy przez to rozumieć wszelkiego rodzaju nośniki danych służące do zapisu i przechowywania danych używane w procesie przetwarzania, w szczególności dyski twarde, płyty CD/DVD, taśmy do streamerów, pamięci przenośne, dyski magnetooptyczne, dokumenty w formie papierowej;
14) **ochronie** – należy przez to rozumieć zespół środków organizacyjno-technicznych prawnych zapewniających bezpieczeństwo informacji;
15) **instytucie** – należy przez to rozumieć Centrum Astronomiczne im. M. Kopernika PAN
16) **osobie możliwej do zidentyfikowania** – należy przez to rozumieć osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne,fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
17) **podatności** – należy przez to rozumieć słabość zasobu informatycznego, która może zostać wykorzystana przez zagrożenie;
18) **poufności** – należy przez to rozumieć właściwość zasobu informatycznego zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
19) **procesie zarządzania bezpieczeństwem systemów informatycznych** – należy przez to rozumieć całość działań organizacyjno-technicznych i prawnych podejmowanych przez instytut,mających na celu właściwą ochronę informacji oraz minimalizację skutków w przypadku naruszenia ochrony danych osobowych ;
20) **przetwarzaniu** – należy przez to rozumieć operację lub zestaw operacji wykonywanych nadanych 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 ;
21) **rozliczalności** – należy przez to rozumieć właściwość zasobu informatycznego oznaczającą, że wykonane na nim działania mogą być jednoznacznie przypisane wykonującej je osobie lub systemowi informatycznemu;
22) **ryzyku** – należy przez to rozumieć prawdopodobieństwo tego, że zagrożenie wykorzysta podatność, powodując skutek;
23) **ryzyku operacyjnym** – należy przez to rozumieć ryzyko wynikające z nieodpowiednich procedur wewnętrznych, błędów ludzkich i zawodności systemów lub z czynników zewnętrznych. Materializacja ryzyka operacyjnego polega na utracie zasobów lub utracie kontroli nad tymi zasobami;
24) **skutku** – należy przez to rozumieć negatywne następstwo naruszenia bezpieczeństwa danych osobowych dla instytutu;
25) **systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
26) **systemie zarządzania bezpieczeństwem danych osobowych** – należy przez to rozumieć całościowy i uporządkowany układ, który tworzą następujące procedury i procesy:
   a) ustanowienie polityki bezpieczeństwa danych osobowych,
   b) określenie zakresu zarządzania bezpieczeństwem danych osobowych,
   c) ocenę zagrożeń bezpieczeństwa danych osobowych i zarządzanie ryzykiem związanym z zagrożeniami,

d) wprowadzenie standardów bezpieczeństwa danych,
e) opracowanie planu ciągłości działania,
f) edukację pracowników w zakresie bezpieczeństwa informacji,
g) weryfikację zgodności procedur bezpieczeństwa z Polityką oraz przepisami prawa;

27) **trwałym usunięciu informacji** – należy przez to rozumieć sposób postępowania z nośnikiem informacji mający na celu usunięcie zapisanych na nim informacji, tak aby ich odtworzenie w całości lub w części było niemożliwe;

28) **użytkowniku** – należy przez to rozumieć pracownika instytutu oraz inne osoby, przy pomocy których instytut wykonuje swoje czynności, posiadające uprawnienia do pracy w systemie informatycznym, zgodnie z zakresem obowiązków służbowych i nadanymi uprawnieniami;

29) **właściwej ochronie** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych, organizacyjnych i prawnych stosowanych w celu zapewnienia bezpieczeństwa informacji, przy jednoczesnym uwzględnieniu opłacalności ekonomicznej, wrażliwości informacji i kategorii systemu informatycznego, poziomu akceptacji ryzyka szczątkowego oraz spełnieniu wymogów prawnych; zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

30) **zagrożeniu** – należy przez to rozumieć stan faktyczny, który może spowodować naruszenie bezpieczeństwa informacji.

§ 3
Cele polityki bezpieczeństwa ochrony danych

1. Bezpieczeństwo danych osobowych będących w posiadaniu instytutu rozumiane jest jako zapewnienie zgodności przetwarzania z prawem i zachowanie poufności, integralności, rozliczalności oraz dostępności danych osobowych.
2. Polityka oraz dokumenty powiązane to procedury opisujące całokształt działań zmierzających do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych i przetwarzania danych osobowych w sposób zgodny z prawem.
3. Celem strategicznym polityki jest osiągnięcie akceptowalnego poziomu bezpieczeństwa danych osobowych w instytucie.
4. Celami Szczegółowymi polityki są:
   - określenie podstaw organizacyjnych do wdrożenia systemu zarządzania bezpieczeństwem danych osobowych w instytucie,
   - określenie obowiązków poszczególnych członków instytutu względem przetwarzania danych osobowych i zbiorów danych osobowych,
   - określenie zbiorów danych osobowych w instytucie,
   - określenie sposobów postępowania członków instytutu w zakresie przetwarzania danych osobowych i zachowania bezpieczeństwa przetwarzania,
   - zapewnienie właściwego poziomu bezpieczeństwa danych osobowych zgodnie z najlepszymi praktykami wynikającymi z polskich przepisów i norm,
   - zabezpieczenie zasobów systemów informatycznych, infrastruktury technicznej, sprzętu i osprzętu przed kradzieżą, zniszczeniem, uszkodzeniem, lub nieumyślnym ujawnieniem.
   - zapewnienie gotowości do podejmowania działań w wypadkach naruszenia ochrony danych osobowych i określenie sposobów postępowania w razie naruszenia ochrony danych osobowych
   - ochrona wizerunku instytutu jako podmiotu zachowującego ochronę danych osobowych.
5. Polityka dotyczy wszystkich osób zatrudnionych w instytucie, w rozumieniu Kodeksu pracy,a także osób, przy pomocy których instytut wykonuje swoje czynności, a które przyjęły na siebie zobowiązanie dotyczące jej przestrzegania.
6. Przedstawione w niniejszym dokumencie środki i metody ochrony informacji dotyczą wszelkich jej form zapisu, w tym informacji zapisanych na nośnikach elektronicznych, optycznych, magnetycznych i papierowych.

§ 4
Zadania ADO

ADO zapewnia:

a) gromadzenie danych osobowych w sposób zgodny z prawem tj. na podstawie zgody osoby, której
dane dotyczą lub na podstawie wyraźnego przepisu prawa nie wymagającego zgody tej osoby,
b) gromadzenie i przetwarzanie danych w sposób rzetelny i przejrzysty dla osoby, której dane
dotyczą,
c)gromadzenie i przetwarzanie danych w sposób adekwatny, stosowny oraz ograniczony w stosunku do celów dla których są przetwarzane,
d) gromadzenie i przetwarzanie danych w sposób prawidłowy i zgodny z rzeczywistym
e) przetwarzane przez określony czas przez wskazanie okresu przez jaki będą przetwarzane lub
podstaw do jego ustalenia,
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym
ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową
utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"),
g) wykonanie obowiązku informacyjnego w stosunku do osób, których dane dotyczą zgodnie z
określonymi w Rozporządzeniu trybami gromadzenia danych osobowych,
h) ochronę danych w wypadkach ich powierzenia podmiotom przetwarzającym poprzez dochowanie obowiązku zawarcia umowy odpowiadającej wymogom przepisu art. 28 ust. 3 Rozporządzenia.

§ 5
Kompetencje ADO

ADO:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie oraz technik i środków zabezpieczenia danych osobowych;
2) nadaje uprawnienia poszczególnym użytkownikom systemu do przetwarzania danych osobowych przez akceptację wniosku o nadanie uprawnień lub odmawia nadania uprawnień do przetwarzania danych osobowych;
3) wyznacza, rekomenduje i egzekwuje wykonanie zadań związanych z ochroną danych osobowych w całym instytucie;
4) powołuje Inspektora Ochrony Danych;
5) zapewnia użytkownikom odpowiednie stanowiska i warunki pracy pozwalające na spełnianie wymagań niniejszej Polityki i powiązanych z nią dokumentów;
6) w wypadku niepowołania IOD wykonuje zadania z zakresu ochrony danych osobowych i realizacji Polityki osobiście działając przez osoby uprawnione do reprezentowania ADO;
7) podejmuje odpowiednie działania w przypadku naruszenia ochrony danych lub wykrycia zagrożenia lub podatności.

§ 6
Zbiory danych - uprawnienie do przetwarzania

1. ADO identyfikuje i ujawnia zbiory danych osobowych w osobnym zestawieniu obejmującym:

1) podstawę prawną przetwarzania danych w ramach danego zbioru,
2) narzędzia przetwarzania i formę nośników danych osobowych,
3) cel przetwarzania danych w zbiorze i rodzaj danych,
4) przewidywany czas przetwarzania danych,
5) odbiorców danych osobowych w ramach poszczególnych zbiorów.

2. Przetwarzanie danych osobowych w zakresie poszczególnych zbiorów odbywa się jedynie na podstawie nadania uprawnień do przetwarzania danych osobowych we wskazanym zakresie przez ADO.
3. Wniosek o nadanie uprawnień do przetwarzania danych osobowych składany jest przez użytkownika na formularzu stanowiącym załącznik do niniejszej polityki.
4. Użytkownik informuje ADO o ustaniu lub zmianie zakresu uprawnień do przetwarzania danych osobowych poprzez złożenie pisemnego wniosku na formularzu stanowiącym załącznik do niniejszej polityki.
5. Z momentem zakończenia zatrudnienia użytkownika ustaje jego uprawnienie do przetwarzania danych osobowych znajdujących się w posiadaniu ADO.
6. ADO może zmieniać zakres uprawnień do przetwarzania danych osobowych użytkownikom oraz cofać uprawnienia do przetwarzania danych.
7. ADO prowadzi wykaz osób uprawnionych do przetwarzania danych osobowych zawierający dane identyfikujące użytkownika zakres uprawnień oraz daty nadania, zmiany i cofnięcia uprawnień do przetwarzania danych osobowych.

§ 7
Zbiory powierzone

1. Instytut przetwarza dane osobowe w zakresie powierzonych zbiorów danych osobowych jedynie na podstawie umowy odpowiadającej wymogom określonym w art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679.
2. Zbiory danych, które instytut przetwarza jako podmiot przetwarzający podlegają ochronie na takich samych zasadach jak własne zbiory danych ADO.
3. Instytut ujawnia powierzone jej zbiory danych osobowych w odrębnym wykazie obejmującym:
- podstawę prawną przetwarzania danych w ramach danego zbioru,
- narzędzia przetwarzania i formę nośników danych osobowych,
- cel przetwarzania danych w zbiorze i rodzaj danych,
- przewidywany czas przetwarzania danych,
- odbiorców danych osobowych w ramach poszczególnych zbiorów.

§ 8
Środki bezpieczeństwa

1. ADO stosuje następujące środki organizacyjne i techniczne dla ochrony poufności, integralności i rozliczalności danych osobowych:
a) stosowanie polityki bezpieczeństwa,
b) stosowanie instrukcji przetwarzania danych osobowych,
c) prowadzenie rejestru zbiorów danych osobowych,
d) prowadzenie wykazu osób upoważnionych do przetwarzania danych,
e) szkolenie pracowników i innych użytkowników w zakresie obowiązujących przepisów o ochronie danych osobowych i zasad zachowania bezpieczeństwa danych osobowych,
f) nadawanie, zmiana i cofanie uprawnień do przetwarzania danych w sposób sformalizowany,
g) bieżąca kontrola stanu bezpieczeństwa zbiorów dokumentowych oraz nośników elektronicznych zawierających dane osobowe,

h) przeprowadzanie audytu w zakresie aktualności dokumentacji, oceny potrzeb przeprowadzania oceny skutków i prowadzenia rejestru czynności przetwarzania, a także faktycznego przestrzegania obowiązujących zasad ochrony danych przez użytkowników,
i) bieżące aktualizowanie oprogramowania służącego do przetwarzania danych osobowych,
j) dostęp do miejsc, w których przetrzymywane są dane osobowe zabezpieczony jest kluczem, dostęp do klucza jest ograniczony do niezbędnego kręgu osób wchodzących w skład kierownictwa instytutu i podlega ewidencjonowaniu,
k) teren na którym znajduje się budynek instytutu poddany jest stałemu dozorowi służb ochrony, teren jest ogrodzony i zamykany poza godzinami pracy instytutu,
l) sieć instytutu chroniona jest firewallem, a dostęp poszczególnych użytkowników limitowany jest poprzez delegowanie uprawnień ,
m)
n)

2. Każdy użytkownik jest odpowiedzialny za bezpieczne korzystanie ze swojej stacji roboczej w zakresie przetwarzania danych osobowych.
3. Instalacji nowego oprogramowania lub wprowadzenia nowego sprzętu IT do użytku w instytucie dokonuje osoba upoważniona przez ADO.
4. Wycofanie sprzętu z użytku odbywa się poprzez fizyczne uszkodzenie nośnika danych uniemożliwiającego odczytanie danych znajdujących się na nośniku.
5. Dane osobowe w formie papierowej niszczone są za pomocą niszczarki po upływie okresu ich przechowywania nie później niż w terminie 14 dni od upływu tego terminu.

§ 9
Szkolenia

1. Użytkownicy systemu w zakresie odpowiednim do swoich zadań i obowiązków są zobowiązani znać treść niniejszej Polityki Bezpieczeństwa Danych osobowych oraz dokumentów regulujących szczegółowo zasady zachowania bezpieczeństwa danych osobowych.
2. Każdy użytkownik systemu powinien zostać poinformowany o zakresie odpowiedzialności i obowiązków wynikających z niniejszej Polityki wraz z konsekwencjami prawnymi, a w przypadku pracowników, dyscyplinarnymi wynikającymi z naruszenia Polityki oraz dokumentów z nią powiązanych.
3. Każdy użytkownik systemu powinien podpisać stosowne zobowiązanie do przestrzegania regulacji wewnętrznych i zewnętrznych dotyczących tego obszaru.
4. Okresowym szkoleniom – stosownie do potrzeb wynikających ze zmian w systemie zabezpieczenia danych osobowych (zastosowania nowych sposobów, środków i form ochrony informacji) oraz w związku ze zmianą przepisów o ochronie informacji – podlegają wszyscy użytkownicy.
5. Szkolenia przeprowadza się w razie potrzeby, po zarządzeniu szkolenia przez ADO.
6. Niniejszą Politykę i dokumenty powiązane można przedstawiać podmiotom zewnętrznym na podstawie przepisów prawa lub pisemnej zgody udzielonej przez ADO.

§ 10
Analiza i ocena skutków dla naruszenia wolności i praw

1. ADO dokonuje analizy i oceny ryzyka naruszenia wolności i praw podmiotów danych osobowych w przypadku:
a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10,

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

2. W przypadku konieczności dokonania analizy i oceny ryzyka ADO lub osoba przez niego upoważniona dokonuje następujących czynności:

a) opis planowanych czynności i celów przetwarzania,

b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów przetwarzania,

c) ocenę poziomu ryzyka,

d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie Rozporządzenia,

e) w wypadku braku możliwości zminimalizowania ryzyka do poziomu akceptowalnego dokonuje zgłoszenia do organu nadzorczego celem wykonania obowiązku konsultacji zgodnie z art. 36 Rozporządzenia.

§ 11
Naruszenie ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w ust. 1, musi zawierać co najmniej:

a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
5. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze . Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.
6. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
7. Zgłoszenie, o którym mowa w ust. 6 nie jest wymagane w wypadkach przewidzianych w przepisie art. 34 ust. 3 Rozporządzenia.
8. Każdy użytkownik systemu zobowiązany jest zgłosić ADO naruszenie ochrony danych osobowych lub podatność systemu ochrony danych osobowych lub stan zagrożenia naruszenia ochrony danych osobowych niezwłocznie podając:

a) dane zgłaszającego oraz datę i godzinę zgłoszenia

b) opis incydentu lub stanu zagrożenia lub podatności wraz z datą i godziną wystąpienia zdarzenia,

c) wskazanie innych okoliczności wystąpienia incydentu,

d) znane przyczyny wystąpienia zdarzenia,

e) podjęte dotychczas działania.

§ 12
Polityka tworzenia kopii zapasowych

1. ADO tworzy regularne kopie zapasowe danych przetwarzanych w systemach informatycznych znajdujących się na serwerach instytutu.
2. Użytkownicy we własnym zakresie dokonują archiwizacji własnych zasobów informatycznych.
3. Kopie zapasowe tworzone są metodą różnicową oraz pełną.
4. ADO prowadzi wykaz kopii zapasowych do poszczególnych systemów.
5.

§ 13
Obowiązek informacyjny

1. W wypadku zwrócenia się do ADO przez osobę, której dane dotyczą z wnioskiem o potwierdzenie przetwarzania danych osobowych ADO podaje tej osobie:
   a) cele przetwarzania,
   b) kategorie odnośnych danych osobowych,
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) informacje o prawie wniesienia skargi do organu nadzorczego;
   g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.
2. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu na jej wniosek złożony w formie dokumentowej po zweryfikowaniu tożsamości osoby występującej z wnioskiem.

§ 14
Przegląd Polityki i obowiązującej dokumentacji

1. Polityka i dokumenty powiązane podlegają przeglądom zarządczym i weryfikacji zgodnie z zasadami obowiązującymi w instytucie.
2. Przeglądy powinny być dokonywane co najmniej raz do roku lub w trakcie roku w przypadku wystąpienia znaczących zmian, powinny obejmować:
   1) weryfikację zasad i ewentualne dostosowanie Polityki do zmieniającego się profilu ryzyka w instytucie;
   2) adekwatność zapisów do zmian środowiska organizacyjnego;
   3) adekwatność zapisów do zmian w budowie systemu informatycznego;
   4) dostosowanie do zmian w obowiązującym prawie i norm nadzorczych.
3. Wszelkie zmiany w niniejszej Polityce wymagają akceptacji wg obowiązujących w instytucie procedur.

§ 15
Audyt i kontrola systemów informatycznych oraz zbiorów papierowych

1. Przez audyt lub kontrolę systemów informatycznych należy rozumieć czynności mające na celu uzyskanie racjonalnego zapewnienia, że mechanizmy kontroli eksploatacji systemów informatycznych i bezpieczeństwa informacji funkcjonują zgodnie z założeniami, są adekwatne do poziomu ryzyka, wymogów prawnych i obowiązujących norm. Sprawdzeniu podlega, czy mechanizmy kontroli wewnętrznej w systemie informatycznym i związanych z nim zasobach właściwie chronią informacje, utrzymują integralność, poufność i rzetelność danych.
2. Do przeprowadzania audytu lub kontroli systemów informatycznych upoważnione są w szczególności:
    1) audytor wewnętrzny;
    2) podmioty zewnętrzne z mocy prawa lub na podstawie umowy cywilno-prawnej.
3. Audyt lub kontrola zbiorów papierowych obejmuje zweryfikowanie istniejących zbiorów danych osobowych w formie papierowej, prawidłowości ich kwalifikacji, zgodności z zasadami bezpieczeństwa i zgodności z prawem w zakresie przetwarzania danych osobowych.

§ 16

Niniejsza Polityka wchodzi w życie z dniem podpisania i podlega ogłoszeniu wobec wszystkich użytkowników systemu w instytucie.

Załączniki:
1. Wzór umowy powierzenia danych osobowych
2. Wzór rejestru naruszań ochrony danych osobowych.
3. Wzór upoważnienia do przetwarzania danych osobowych i oświadczenie o zachowaniu tajemnicy

Załącznik nr 1

Umowa powierzenia przetwarzania danych osobowych

Nr .....

zawarta w Warszawie w dniu ..... pomiędzy:

Centrum Astronomicznym im. Mikołaja Kopernika PAN z siedzibą w Warszawie, ul. Bartycka 18, wpisanym do rejestru instytutów naukowych PAN pod nr RIN-III-20/98, NIP 525-000-89-56, zwanym w treści umowy „**Zleceniodawcą**", reprezentowanym przez:

..... – Dyrektora,

a

.....

zwaną w treści umowy **„Zleceniobiorcą"**, reprezentowaną przez:

.....– .....

§ 1

Oświadczenia stron

1. Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych w zakresie i celu objętym niniejszą umową.

2. Zleceniodawca oświadcza, że jest administratorem danych osobowych w rozumieniu art. 4 pkt 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016 r.(Dz.Urz. UE L 2016, nr 119/1, **dalej RODO**), które przetwarza zgodnie z obowiązującymi przepisami prawa. Zleceniodawca oświadcza ponadto, że zawiera niniejszą umowę w celu bezpośrednio związanym z jego działalnością zawodową.

3. Zleceniobiorca oświadcza, iż dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z przepisami prawa unijnego oraz polskimi przepisami w zakresie ochrony danych osobowych.

§ 2

Zakres i cel przetwarzania danych osobowych

1. Zleceniobiorca może przetwarzać dane osobowe przekazane przez Zleceniodawcę wyłącznie w zakresie i w celu określonych w niniejszej umowie.

2. Dane osobowe będą przetwarzane przez Zleceniobiorcę tylko i wyłącznie w celu realizacji umowy.....z dnia ..... r. (dalej: Umowa Główna).

3. Zakres przetwarzania obejmuje następujące dane osobowe:

– .....,

– .....,

– .....

4. Poprzez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

5. Zleceniobiorca jest uprawniony do przetwarzania danych osobowych poprzez wykonywanie wszelkich czynności uzasadnionych wykonywaniem Umowy Głównej oraz poleceń i instrukcji Zleceniodawcy pozostających w związku z Umową Główną, w szczególności Zleceniobiorca jest uprawniony do:

- utrwalania,

- zwielokrotniania,

- przechowywania i udostępniania danych osobowych,

w zakresie i na zasadach wynikających z niniejszej umowy i Umowy Głównej oraz poleceń i instrukcji Zleceniodawcy.

6. Zleceniobiorca będzie przetwarzał dane osobowe w następującej lokalizacji: ul. ..... Zleceniobiorca niezwłocznie poinformuje Zleceniodawcę o wszelkich zmianach lokalizacji, w których przetwarzane są dane osobowe.

7. Zleceniobiorca zapewni, że przetwarzanie danych osobowych przez Zleceniobiorcę i podmioty trzecie, którym przekaże dane osobowe, będzie się odbywało wyłącznie na terytorium Polski.

8. Zleceniobiorca może powierzyć przetwarzanie danych osobowych podmiotom trzecim o czym niezwłocznie powiadomi Zleceniodawcę. Listę podmiotów, którym Zleceniobiorca powierzył przetwarzanie danych osobowych stanowi załącznik nr 1 do Umowy

9. Zleceniodawca może wycofać zgodę na dalsze powierzenie przetwarzania danych osobowych podmiotom trzecim, jeżeli z okoliczności wynika, że przetwarzanie przez nich danych osobowych odbywa się niezgodnie z prawem, umową lub zagraża bezpieczeństwu danych osobowych. W przypadku wycofania zgody, Zleceniobiorca jest zobowiązany niezwłocznie doprowadzić do zaprzestania przetwarzania danych przez podmiot trzeci.

§ 3

Zasady przetwarzania danych osobowych

1. Przy przetwarzaniu danych osobowych Zleceniobiorca jest zobowiązany do przestrzegania obowiązujących przepisów prawa, w tym przepisów o ochronie danych osobowych mających zastosowanie oraz postanowień umowy. W szczególności Zleceniobiorca jest zobowiązany do:

a) przetwarzania powierzonych przez Zleceniodawcę danych osobowych wyłącznie w zakresie i celu określonych w § 2 umowy, na udokumentowane polecenie Zleceniodawcy, chyba że obowiązek przetwarzania w inny sposób nakładają na Zleceniobiorcę przepisy prawa,

b) poinformowania Zleceniodawcy, przed rozpoczęciem przetwarzania, o obowiązku prawnym skutkującym koniecznością przetwarzania danych osobowych inaczej niż na udokumentowane polecenie Zleceniodawcy, chyba że przepisy prawa zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny,

c) zabezpieczenia danych osobowych poprzez zastosowanie odpowiednich, wymaganych przez obowiązujące przepisy prawa mające zastosowanie, środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa przetwarzanych danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w tym zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

d) wdrożenia wymaganych obowiązującymi przepisami prawa mającymi zastosowanie środków zapewniających poufność, integralność, dostępność danych osobowych i odporność systemów wykorzystanych do ich przetwarzania, w szczególności poprzez pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów, w których przetwarzane są dane osobowe, zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie wystąpienia incydentu fizycznego lub technicznego,

e) dopuszczenia do przetwarzania danych osobowych, w tym obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, wyłącznie osób posiadających imienne upoważnienie od Zleceniobiorcy,

f) zgłaszania Zleceniodawcy przypadków naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu jednego dnia od zaistnienia przypadku,

g) zapewnienia kontroli nad prawidłowością przetwarzania danych osobowych.

§ 4

Odpowiedzialność za szkody

1. Zleceniobiorca odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez Zleceniobiorcę powierzonych danych osobowych.

2. Zleceniobiorca nie jest odpowiedzialny za udostępnienie powierzonych danych osobowych osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem tych danych osobowych w przypadku, gdy przyczyną powyższego jest działanie bądź zaniechanie Zleceniodawcy.

§ 5

Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują przepisy RODO oraz powiązanych z nią przepisów polskich aktów normatywnych i kodeksu cywilnego.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....	.....
(Zleceniodawca)	(Zleceniobiorca)

REJESTR NARUSZEŃ DANYCH OSOBOWYCH
w Centrum Astronomicznym im. M. Kopernika PAN

Załącznik nr 2

L.p.	Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

Załącznik nr 3

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
ORAZ
OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Działając na podstawie obowiązujących unijnych i polskich przepisów prawa powszechnie obowiązujących jako Administrator Danych Osobowych upoważniam/cofam upoważnienie Panią/Pana .....zatrudnioną/ego w oparciu o (umowę o pracę, inne) na stanowisku ..... do przetwarzania danych osobowych (można wyszczególnić zakres) w formie elektronicznej i papierowej w ramach wykonywanych obowiązków służbowych.

Jednocześnie pouczam, że nieprzestrzeganie zasad bezpieczeństwa danych osobowych obowiązujących w Centrum Astronomicznym im. M. Kopernika PAN określonych w Polityce Bezpieczeństwa Danych Osobowych może być potraktowane jako naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu pracy i prowadzić do konsekwencji służbowych.

Data i podpis wydającego upoważnienie

.....

Data i podpis upoważnionego pracownika

.....

OŚWIADCZENIE O ZACHOWANIU TAJEMNICY I POUFNOŚCI

W CENTRUM ASTRONOMICZNYM IM. M. KOPERNIKA PAN

W związku z dopuszczeniem do przetwarzania danych osobowych oświadczam, że:

- zapoznałem/am się i zobowiązuję się do przestrzegania obowiązków wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z dnia 27 kwietnia 2016 r. oraz powszechnie obowiązujących przepisów prawa polskiego w zakresie ochrony danych osobowych i regulacji wewnętrznych Administratora obowiązujących w obszarze przetwarzania danych i bezpieczeństwa informacji,
- zapewnię bezpieczeństwo przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją i zniszczeniem, nielegalnym ujawnieniem, pozyskaniem lub utratą,
- zachowam w tajemnicy dane osobowe oraz sposoby ich zabezpieczeń do których uzyskam dostęp w trakcie współpracy z Administratorem i po jej zakończeniu,
- znane mi są zasady odpowiedzialności prawnej za niezgodne z przepisami unijnymi oraz polskimi przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u Administratora, kodeksu pracy, kodeksu cywilnego oraz przepisów unijnych i polskich w zakresie danych osobowych.

Data i podpis

.....

Załącznik nr 2 do Zarządzenia nr 12/2018

ul. Bartycka 18, 00-716 Warszawa
tel: (22) 841 00 41, (22) 3296 100
fax: (22) 841 00 46
email: camk@camk.edu.pl
http://www.camk.edu.pl

CENTRUM ASTRONOMICZNE IM. MIKOŁAJA KOPERNIKA PAN

Instrukcja
postępowania w sytuacji naruszenia systemu ochrony danych osobowych w Centrum Astronomicznym im. M. Kopernika PAN

Rozdział 1.
Postanowienia ogólne

§ 1

1. Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych.
2. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu,w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie, jest wyznaczony przez administratora danych osobowych – IOD.

Rozdział 2.
Tryb i zasady postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego

§ 2

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym IOD.
2. IOD po otrzymaniu powiadomienia we współpracy z pracownikiem DAS:
   1) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł),
   2) zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,
   3) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
   4) niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
   5) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
   6) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu (włamaniu do systemu), opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

3. Raport wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) administrator bezpieczeństwa informacji przekazuje administratorowi danych osobowych jednostki.
4. IOD w porozumieniu z administratorem danych osobowych podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu w przyszłości.

Rozdział 3.
Tryb postępowania w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych

§ 3

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, obowiązana jest niezwłocznie powiadomić o tym inspektora danych osobowych lub inną upoważnioną przez niego osobę.
2. IOD po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń) we współpracy z pracownikiem DAS:
   1) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   2) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),
   3) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
   4) sprawdza zawartości zbioru danych osobowych,
   5) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.
3. W przypadku stwierdzenia naruszenia zabezpieczeń danych:
   1) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia(odłączenie wadliwych urządzeń, blokuje dostęp do sieci telekomunikacyjnej, do programów oraz zbiorów danych itp.),
   2) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   3) niezwłocznie przywraca prawidłowy stan działania systemu,
   4) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na
   skutek ich naruszenia,
   5) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie), administrator bezpieczeństwa informacji przekazuje administratorowi danych osobowych jednostki.
5. IOD, w porozumieniu z administratorem danych osobowych, podejmuje niezbędne działania w celu wyeliminowania naruszeń bezpieczeństwa danych w przyszłości, a w szczególności:
   1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu,uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej,niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
   2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągniecie konsekwencji prawem przewidzianych.

Rozdział 4.
Postanowienia końcowe

§ 4

1. Każda osoba wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zobowiązana jest do zapoznania się z niniejszą instrukcją. Wykonanie powyższego zobowiązania pracownik potwierdza własnoręcznym podpisem.
2. Wszelkie zmiany niniejszej instrukcji skutkują wobec osób, których dotyczą, z dniem ich doręczenia na piśmie.