Zarządzenie nr 29/2018
Dyrektora Naczelnego Centrum Nauki Kopernik
z dnia 24 maja 2018 r.

w sprawie:

wprowadzenia polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemami informatycznymi w Centrum Nauki Kopernik

Działając w celu zapewnienia bezpieczeństwa danych osobowych, których administratorem jest Centrum Nauki Kopernik oraz realizacji postanowień Rozporządzenia Parlamentu Europejskiego i Rady (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 (ogólne rozporządzenie o ochronie danych), na podstawie § 7 ust. 2 lit. e) statutu Centrum Nauki Kopernik, zarządzam co następuje:

§ 1

Wprowadzam Politykę Bezpieczeństwa Danych Osobowych w nowym brzmieniu, określonym w załączniku nr 1 do niniejszego zarządzenia, oraz zobowiązuję wszystkich pracowników Centrum Nauki Kopernik do zapoznania się z jej postanowieniami.

§ 2

Wprowadzam Instrukcję Zarządzania Systemami Informatycznymi w Centrum Nauki Kopernik w nowym brzmieniu, określonym w załączniku nr 2 do niniejszego zarządzenia, oraz zobowiązuję wszystkich pracowników Centrum Nauki Kopernik do zapoznania się z jej postanowieniami.

§ 3

1. Zarządzenie wchodzi w życie z dniem jego podpisania.
2. Wprowadzone niniejszym zarządzeniem procedury obowiązują od dnia 25 maja 2018 r.
3. Z dniem wejścia w życie niniejszego zarządzenia uchyla się zarządzenie nr 59/2017 Dyrektora Centrum Nauki Kopernik z dnia 3 października 2017 r.

4. Osobą odpowiedzialną za nadzór nad realizacją i aktualizację niniejszego zarządzenia jest Pan Michał Stańczyk – Dział Prawny i Zamówień Publicznych.

Ewa Kłos
DYREKTOR
CENTRUM NAUKI KOPERNIK

.....

(podpis Dyrektora Naczelnego Centrum Nauki Kopernik)

Polityka Bezpieczeństwa Danych Osobowych

CENTRUM NAUKI KOPERNIK

Spis treści

Niniejszy dokument ma na celu zapewnienie bezpieczeństwa informacji w zakresie przetwarzania danych osobowych w Centrum Nauki Kopernik (dalej jako „CNK").

I. Podstawa prawna

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej jako „Ustawa").
2. Rozporządzenie Parlamentu Europejskiego i Rady (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 (ogólne rozporządzenie o ochronie danych, dalej jako „RODO").

II. Definicje

1. **Administrator danych osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. W niniejszej Polityce bezpieczeństwa przez Administratora danych osobowych rozumie się CNK.
2. **Administrator Systemu Informatycznego (ASI)** – osoba zarządzająca systemem informatycznym w CNK.
3. **CNK** – Centrum Nauki Kopernik z siedzibą w Warszawie przy ul. Wybrzeże Kościuszkowskie 20, zarejestrowane przez Prezydenta m.st. Warszawy w Rejestrze Instytucji Kultury pod numerem 2/06.
4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

5. **Identyfikator danych** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania Danych osobowych w systemie informatycznym.
6. **Informacja** – dane, które mogą być wyrażone za pomocą pisma, obrazu lub dźwięku, zawarte w systemie informatycznym.
7. **Integralność informacji** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym.
9. **Inspektor Ochrony danych (IOD)** – osoba wyznaczona przez Administratora danych na podstawie art. 37 RODO oraz ar. 8 Ustawy.
10. **Organ nadzorczy** – Urząd Ochrony Danych Osobowych z siedzibą w Warszawie przy ul. Stawki 2, właściwy dla zapewnienia przestrzegania przepisów dotyczących ochrony danych osobowych.
11. **Polityka bezpieczeństwa** – niniejszy dokument, zawierający zestaw praw, reguł i praktycznych doświadczeń regulujący sposób zarządzania ochroną i dystrybucją Danych osobowych w CNK.
12. **Poufność**– rozumie się przez to właściwość zapewniającą, że Dane osobowe nie są udostępniane nieupoważnionym podmiotom.
13. **Przetwarzanie danych** – 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.
14. **Rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
15. **Uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
16. **Użytkownik** – osoba posiadająca uprawnienie dostępu do systemu informatycznego.
17. **Zabezpieczenie informacji** – zapewnienie poufności, integralności i rozliczalności Danych osobowych.
18. **Zbiór danych** – każdy posiadający strukturę zestaw Danych osobowych, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

III. Postanowienia ogólne

1. Dyrektor Naczelny CNK podejmuje odpowiednie kroki, mające na celu zapewnienie prawidłowej ochrony Danych osobowych, których administratorem jest CNK. Dane osobowe przetwarzane będą:
   1) zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   3) adekwatne w stosunku do celów, dla których są zbierane,
   4) prawidłowe i w razie potrzeby uaktualniane,
   5) przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania,
   6) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają Rozliczalność, Integralność i Poufność danych.
2. Przy przetwarzaniu Danych osobowych w systemach informatycznych w CNK obowiązuje wszystkich Użytkowników „Instrukcja zarządzania systemami informatycznymi CNK".
3. Niniejsza Polityka bezpieczeństwa określa podstawowe zasady bezpieczeństwa przetwarzanych Danych osobowych w CNK oraz ma zastosowanie wobec wszystkich komórek organizacyjnych CNK.
4. Niniejsza Polityka bezpieczeństwa dotyczy wszystkich Danych osobowych, przetwarzanych w CNK, niezależnie od formy ich przetwarzania.
5. Celem niniejszej Polityki bezpieczeństwa jest ochrona Danych osobowych, przetwarzanych w CNK przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem Ustawy lub RODO oraz przed zmianą, uszkodzeniem lub zniszczeniem.
6. Postanowienia niniejszej Polityki bezpieczeństwa realizowane są poprzez zastosowanie środków technicznych i rozwiązań organizacyjnych.
7. Dane osobowe mogą być przetwarzane jedynie na polecenie ADO. Poleceniem przetwarzania Danych osobowych przez Użytkowników jest pisemne upoważnienie do przetwarzania danych, o którym mowa w pkt. IX niniejszej Polityki bezpieczeństwa.
8. Przy przetwarzaniu Danych osobowych każdy Użytkownik zobowiązany jest do przestrzegania zasad minimalizacji danych oraz ograniczonego czasu ich przechowywania, przez co należy rozumieć zbieranie danych w ilości niezbędnej do realizacji celu przetwarzania oraz niezwłoczne usuwanie danych po zrealizowaniu tego celu.

IV. Odpowiedzialność

1. Administrator danych – czynności w imieniu Administratora danych wykonuje Dyrektor Naczelny CNK.
2. Inspektor Ochrony Danych – jako osoba odpowiedzialna za nadzór nad przestrzeganiem wprowadzonych zasad ochrony Danych osobowych, jest zobowiązany do wykonywania czynności zgodnie z przepisami Ustawy i RODO, w szczególności do jego obowiązków należy:
   1) sprawowanie nadzoru nad stosowaniem dokumentacji wprowadzonej przez CNK w zakresie związanym z przetwarzaniem Danych osobowych,
   2) informowanie Administratora Danych oraz pracowników CNK, którzy przetwarzają Dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszej Polityki Bezpieczeństwa oraz powszechnie obowiązujących przepisów prawa,
   3) współpraca z Organem nadzorczym,
   4) aktualizowanie procedur regulujących proces przetwarzania danych osobowych w CNK,
   5) monitorowanie przestrzegania w CNK niniejszej Polityki Bezpieczeństwa oraz innych powszechnie obowiązujących przepisów prawa,
   6) akceptacja wszelkich umów, w ramach których może dojść do ujawnienia Danych osobowych, których administratorem jest CNK, osobie trzeciej,
   7) współdziałanie z ASI w zakresie stosowanych zabezpieczeń funkcjonującego systemu informatycznego w CNK,
   8) podejmowanie stosownych działań w przypadkach naruszenia zasad ochrony Danych osobowych, mających na celu przywrócenie stanu zgodnego z przepisami prawa
   9) prowadzi rejestr incydentów bezpieczeństwa danych osobowych.
3. Administrator Systemu Informatycznego (ASI) – jest odpowiedzialny za utrzymanie ciągłości działania systemu informatycznego, współpracę z Inspektorem Ochrony Danych oraz wykonywanie procedur regulujących proces przetwarzania Danych osobowych w CNK, w szczególności:
   1) administrowanie systemami informatycznymi, w których przetwarzane są Dane osobowe,
   2) nadawanie Użytkownikom Identyfikatorów i przyznawanie im uprawnień do systemu informatycznego, wynikających z nadanego upoważnienia,
   3) instalowanie, aktualizowanie i konfigurowanie oprogramowania systemowego i użytkowego oraz innych urządzeń, o ile czynności te nie są wykonywane przez upoważnionych przedstawicieli dostawcy, na podstawie zawartej umowy,

4) zapewnienie bezpieczeństwa sieci informatycznej, w szczególności przed dostępem do Danych osobowych przez osoby nieupoważnione,
5) instalowanie i aktualizowanie oprogramowania antywirusowego,
6) reagowanie i rejestrowanie przypadków naruszenia bądź zagrożenia bezpieczeństwa Danych osobowych przetwarzanych w systemie informatycznym,
7) tworzenie, rejestrowanie oraz przechowywanie kopii zapasowych baz danych zawierających Dane osobowe, jak też kopii zapasowych oprogramowania służącego do ich przetwarzania,
8) przygotowywanie urządzeń, dysków i innych elektronicznych nośników Informacji, zawierających Dane osobowe, do likwidacji, przykazania innemu podmiotowi, konserwacji lub naprawy,
9) kompletowanie i przechowywanie dokumentacji dotyczącej systemu, w którym przetwarzane są Dane osobowe,
10) -powiadamianie Administratora danych lub Inspektora Ochrony Danych o miejscu przechowywania oraz metodzie i częstotliwości tworzenia kopii zapasowych,
11) wykonywanie bieżącej konserwacji i przeglądu systemu informatycznego oraz aktualizowanie kont i uprawnień Użytkowników,
12) informowania Inspektora Ochrony Danych o dokonywanych zmianach w systemie informatycznych, które wymagają modyfikacji treści dokumentacji regulującej procesy przetwarzania Danych osobowych
13) prowadzenia rejestru incydentów bezpieczeństwa w zakresie dotyczącym incydentów związanych z bezpieczeństwem systemu informatycznego CNK w kontekście ochrony Danych osobowych.

4. Osoby upoważnione do przetwarzania Danych osobowych zobowiązane są do:
1) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa,
2) postępowanie zgodne z ustaloną przez Administratora Danych Osobowych Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w CNK
3) niezwłocznego informowania Inspektora Ochrony Danych, a także Administratora Systemu Informatycznego, gdy do naruszenia doszło w Systemie informatycznym, o wszelkich incydentach związanych z naruszeniem bezpieczeństwa Danych osobowych,
4) niezwłocznego informowania Inspektora Ochrony Danych o otrzymanych żądaniach osób, których dotyczą Dane osobowe, związanych z realizacją ich praw: żądania dostępu do treści swoich danych, do ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także praw do wniesienia sprzeciwu wobec przetwarzania czy też prawa do przenoszenia danych,

5. Informacje, o których mowa w pkt. 4 ppkt. 3 i 4 powinny być przekazywane przy użyciu poczty elektronicznej.
6. Dopuszczenie się przez Użytkownika nieuprawnionego ujawnienia lub wykorzystania Danych osobowych w sposób sprzeczny z ich przeznaczeniem, czy też ich przetwarzania w sposób niezgodny z przyjętymi w CNK procedurami, jest uważane za ciężkie naruszenie obowiązków pracowniczych zgodnie z postanowieniami Kodeksu pracy. W przypadku osób, z którymi Administrator danych ma zawarte umowy cywilnoprawne, powyższe naruszenie stanowi niewykonanie lub nienależyte wykonanie zobowiązania.
7. Przy projektowaniu wszelkich programów, systemów informatycznych i innych rozwiązań, które będą miały związek z przetwarzaniem Danych osobowych, należy brać pod uwagę i stosować rozwiązania zakładających ochronę prywatności już na etapie tworzenia tych rozwiązań.
8. Domyślne ustawienia wszelkich narzędzi służących do przetwarzania Danych osobowych zakładają ochronę prywatności i zbieranie jak najmniejszej ilości danych.
9. W przypadku, gdy realizacja umowy zawieranej z podmiotami zewnętrznymi wiąże się z dostępem tych podmiotów do Danych osobowych, których administratorem jest CNK, osoba odpowiedzialna za realizację danej umowy zobowiązana jest do umieszczenia takiej informacji w zamówieniu na umowę kierowanym do Działu Prawnego i Zamówień Publicznych.
10. W przypadku otrzymania żądania informacji związanej z Danymi osobowymi od osoby, której te dane dotyczą, pracownik CNK, który takie żądanie otrzymał, zobowiązany jest do niezwłocznego, jednak nie późniejszego niż w terminie miesiąca, udzielenia informacji. W przypadku jakichkolwiek wątpliwości związanych z udzieleniem odpowiedzi, pracownik powinien zasięgnąć opinii Inspektora Ochrony Danych.
11. Osoby upoważnione do przetwarzania Danych osobowych zobowiązane są do:
    1) ścisłego przestrzegania zakresu udzielonego upoważnienia,
    2) zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia,
    3) zgłaszania ASI niewłaściwego funkcjonowania Systemu informatycznego.

V. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są Dane osobowe.

1. Podstawowym obszarem przetwarzania danych osobowych w CNK jest powierzchnia użytkowa lokali:
    1) ul. Wybrzeże Kościuszkowskie 20, 00-390 Warszawa,
    2) ul. Dobra 56/66, 00-920 Warszawa, poziom 2.

2. Powierzchnią przetwarzania danych osobowych jest całkowita powierzchnia wyżej wskazanych lokali z wyłączeniem powierzchni socjalno-bytowych (toalety, magazynki, pomieszczenia gospodarcze) oraz z wyłączeniem powierzchni udostępnionych osobom zwiedzającym. Szczegółowe informacje zawierające plany poszczególnych pomieszczeń posiada Dział Obsługi Gospodarczej i Technicznej CNK.
3. Na obszarze, o którym mowa w pkt. 1 powyżej, a także na obszarze wystaw Centrum Nauki Kopernik oraz terenach przyległych do budynku siedziby CNK, prowadzony jest monitoring wizyjny. Monitoring prowadzony jest w celu zapewnienia bezpieczeństwa osób i mienia. Nagrania z monitoringu zapisywane są na serwerze wewnętrznym CNK, a następnie, w przypadku gdy nie doszło do wydarzenia uzasadniającego dłuższe ich przechowywanie, nadpisywane przez kolejne nagrania po 22 dniach od momentu ich zapisu.

VI. Wykaz Zbiorów Danych osobowych.

1. Zbiór danych kadrowo-płacowych. Dane osobowe przetwarzane są w formie papierowej oraz elektronicznej.
2. Zbiór danych kandydatów do pracy. Dane osobowe przetwarzane są w formie papierowej oraz elektronicznej.
3. Zbiór ZFŚS. Dane osobowe przetwarzane są w formie papierowej oraz elektronicznej.
4. Zbiór umowy cywilno-prawne. Dane osobowe przetwarzane są w formie papierowej oraz elektronicznej.
5. Zbiór danych ewidencja korespondencji prowadzony jest w formie elektronicznej.
6. Zbiór newsletter. Dane osobowe są przetwarzane w formie elektronicznej.
7. Zbiór imprezy. Dane osobowe przetwarzane są w formie papierowej oraz elektronicznej.
8. Zbiór członków Klubów Młodego Odkrywcy (KMO). Dane osobowe przetwarzane są w formie elektronicznej.
9. Baza adresy (kontakty służbowe) Dane osobowe przetwarzane są w formie papierowej oraz elektronicznej.
10. Zbiór Śpiewająca Wiki. Przetwarzanie danych osobowych zostało powierzone firmie Euro RSCG 4D Digital Sp. z o.o. (ul. Marynarska 11, 02-674 Warszawa) oraz Euro RSCG Warsaw Sp. z o.o. (ul. Marynarska 11, 02-674 Warszawa).
11. Zbiór Konkurs FameLab. Przetwarzanie danych osobowych zostało powierzone British Council Polska z siedzibą w Warszawie (al. Jerozolimskie 59, 00-697 Warszawa). Dane przetwarzane są w formie elektronicznej.
12. Zbiór danych klientów. Dane są przetwarzane w formie elektronicznej.
13. Zbiór danych Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007.

W zbiorze przetwarzane są dane osobowe uczestników Projektu „Opracowanie i pilotaż aktywnych metod pracy nauczyciela z uczniem opartych na metodzie badawczej" prowadzonego w ramach Programu Operacyjnego Kapitał Ludzki. Dane osobowe przetwarzane są w formie elektronicznej w Formularzu PEFS 2007. W stosunku do niniejszego zbioru CNK jest zleceniobiorcą przetwarzania danych osobowych, na podstawie umowy zawartej dnia 17 lipca 2013 r . z Ministrem Edukacji Narodowej. Na potrzeby dopełniania obowiązków formalnych związanych z przetwarzaniem tego zbioru CNK wprowadza szczegółową dokumentację regulującą zasady przetwarzania danych osobowych obowiązującą wszystkich pracowników upoważnionych do przetwarzania Danych osobowych w tym zbiorze. Dokumentacja dotycząca Zbioru Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 stanowi załącznik nr 6 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

14. Zbiór danych konkursów. Dane w zbiorze przetwarzane są w formie papierowej i elektronicznej.
15. Zbiór danych Europejskie Biuro Edukacji Kosmicznej ESERO. Dane przetwarzane są w wersji papierowej i elektronicznej.
16. Zbiór Klub Kopernika. Dane przetwarzane są w wersji papierowej i elektronicznej.
17. Ewidencja gości. Zbiór danych przetwarzany jest w wersji papierowej.
18. Zbiór RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki). W stosunku do niniejszego zbioru CNK jest zleceniobiorcą przetwarzania, na podstawie umowy z dnia 8 sierpnia 2017 r. z Województwem Mazowieckim. Administratorem danych osobowych przetwarzanych w zbiorze jest Marszałek Województwa Mazowieckiego Dane przetwarzane są w systemie pn. SL2014 oraz w formie papierowych formularzy.

VII. Opis struktury Zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych.

1. Zbiór Kadrowo-płacowy. Dane osobowe zawarte w zbiorze są przetwarzane w dokumentacji papierowej zgodnie z (1) Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 917), (2) Rozporządzeniem Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz.U. z 1996 r. Nr 62, poz.286). Zbiór zawiera w szczególności imię (imiona) i nazwisko, imiona rodziców; datę urodzenia; miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia oraz inne dane osobowe pracownika, imiona i nazwiska oraz daty urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu

na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, numer PESEL.

2. Zbiór danych kandydatów do pracy jest przetwarzany aplikacyjnych zgodnie z Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 917). Dane osobowe przetwarzane w zbiorze: imię nazwisko, adres, numer telefonu, adres e-mail, data urodzenia, dane dotyczące dotychczasowego zatrudnienia i edukacji, posiadane dodatkowe uprawnienia i kwalifikacje.
3. Dane ze zbioru ZFŚS są przetwarzane w dokumentacji papierowej zgodnie z Ustawą z dnia 4 marca 1994 r. o Zakładowym Funduszu Świadczeń Socjalnych (Dz.U. z 2017 r. poz. 2191) i zawierają następujące kategorie danych osobowych: imię, nazwisko, adres zamieszkania (pobytu), miejsce pracy. W dokumentacji papierowej kategorie danych osobowych przetwarzane w ramach ZFŚS to: dane pracownika – imię, nazwisko; dane rodziny – imię i nazwisko współmałżonka, imię i nazwisko dzieci, dochód na członka rodziny.
4. Zbiór Dane osób świadczących usługi na podstawie umów cywilno-prawnych. Dane przetwarzane w zbiorze: imię, nazwisko, adres, nr dowodu osobistego, nr PESEL, NIP, kwalifikacje.
5. Zbiór rejestr korespondencji zawiera kategorie danych: imię, nazwisko, adres, data nadania/odebrania korespondencji, znak CNK, identyfikator (l.p.) ewentualne dodatkowe informacje.
6. Zbiór newsletters - Dane osobowe przetwarzane w zbiorze to: imiona i nazwiska, adres e-mail, wiek.
7. Zbiór Imprezy. Dane osobowe przetwarzane w zbiorze: imię, nazwisko, adres, miejsce pracy, adres e-mail, telefon, wiek, zawód wykonywany/specjalność, umiejętności/kwalifikacje zawodowe, wykształcenie/zawód wyuczony, doświadczenie zawodowe, zainteresowania naukowe, preferencje żywieniowe (rezerwacja noclegu, zapewnienie cateringu).
8. Zbiór danych członków Klubów Młodego Odkrywcy (KMO) – Dane osobowe przetwarzane w zbiorze: imię, nazwisko, adres e-mail, nazwa szkoły/indtytucji.
9. Baza adresy (kontakty służbowe) dane kontaktowe dziennikarzy i ekspertów. Dane osobowe przetwarzane w zbiorze: imię, nazwisko, adres, nr telefonu, adres e-mail, stopień naukowy, miejsce zatrudnienia.
10. Zbiór Śpiewająca Wiki: Dane osobowe w tym zbiorze zawierają imię, nazwisko, adres poczty elektronicznej, „nick", awatar. Dane są przetwarzane w systemie informatycznym procesora.
11. Zbiór Konkurs FameLab: Dane osobowe w tym zbiorze zawierają imię, nazwisko, adres zamieszkania lub pobytu, miejsce pracy, wykształcenie, nr telefonu, adres

poczty elektronicznej, wiek, płeć, stopień naukowy, dziedzinę nauki, miejsce nauki, staż, video-prezentację, informacje dodatkowe o prezentacji oraz doświadczeniach w komunikacji naukowej.

12. Zbiór dane Klientów. Dane osobowe przetwarzane w tym zbiorze: imię, nazwisko, adres e-mail, adres zamieszkania, numer telefonu, dane dotyczące transakcji zakupu biletów.
13. Zbiór Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007. Opis struktury zbioru zawiera załącznik nr 6 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
14. Zbiór danych konkursów. Dane osobowe przetwarzane w zbiorze: imię i nazwisko, adres mailowy, adres zamieszkania, numer telefonu, dane związane z uczestnictwem w danym konkursie.
15. Europejskie Biuro Edukacji Kosmicznej ESERO. Dane osobowe przetwarzane w zbiorze: imię i nazwisko, adres e-mail, nazwa instytucji, adres, przedmiot/specjalność.
16. Zbiór Klub Kopernika. Dane osobowe przetwarzane w zbiorze: imię, nazwisko, data urodzenia, adres zamieszkania, adres e-mail, telefon kontaktowy, dane związane z korzystaniem z uprawnień członka Klubu Kopernika.
17. Ewidencja gości. Dane przetwarzane w zbiorze: imię nazwisko, data wejścia/wyjścia, nazwa podmiotu z którego osoba została skierowana/delegowana.
18. Zbiór RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki). Dane przetwarzane w zbiorze: dane uczniów, dyrektorów szkół i nauczycieli, szczegółowy zakres danych przetwarzanych w ramach zbioru zawiera załącznik nr 3 do niniejszej procedury.

Administrator Systemu Informatycznego prowadzi pełną dokumentację techniczną aplikacji składających się na systemy informatyczne funkcjonujące w CNK oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

VIII. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia Poufności, Integralności i Rozliczalności przetwarzanych Danych osobowych.

1. Wyznaczenie Inspektora Ochrony Danych.
2. Wyznaczenie Administratora Systemów Informatycznych.
3. Wprowadzenie procedur regulujących procesy przetwarzania danych.
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania Danych osobowych zgodnie ze wzorem ewidencji stanowiącym załącznik nr 1 do niniejszej Polityki bezpieczeństwa.
5. Prowadzenie rejestru naruszeń bezpieczeństwa danych.

6. Do przetwarzania Danych osobowych są dopuszczone tylko osoby upoważnione zgodnie ze wzorem upoważnienia stanowiącym załącznik nr 2 do niniejszej Polityki bezpieczeństwa.
7. Przeprowadzanie okresowych przeglądów sieci informatycznej w tym przeprowadzanie cyklicznych testów odtwarzania serwera z kopii zapasowej.
8. Dostęp do systemu informatycznego następuje z użyciem Identyfikatora i Hasła.
9. Zastosowanie mechanizmów rozliczalności działań poszczególnych Użytkowników.
10. Zastosowanie oprogramowania antywirusowego w tym systematyczne instalowanie wymaganych przez producentów oprogramowania aktualizacji związanych z bezpieczeństwem.
11. Zastosowanie zapory ogniowej (firewall) ze zdefiniowanymi listami dostępów.
12. Szczegółowe zabezpieczenia fizyczne są opisane w dokumentacji prowadzonej przez Specjalistę ds. bezpieczeństwa. Dokumentacja może być udostępniona tylko osobom upoważnionym przez Dyrektora Naczelnego CNK.
13. Obowiązkowe szkolenia pracowników CNK w zakresie ochrony Danych osobowych, odbywające się w miarę uzasadnionych potrzeb oraz szkolenia dla wszystkich nowozatrudnionych pracowników.
14. W celu zapewnienia Rozliczalności dostępu do danych:
    1) z dniem rozwiązania stosunku pracy z Użytkownikiem:
        a) ASI zamyka konto Użytkownika w systemie informatycznym oraz zabezpiecza dostęp do danych hasłem; dane z konta Użytkownika, z którym rozwiązano stosunek pracy, są archiwizowane lub usuwane – zgodnie z decyzją kierownika komórki organizacyjnej, w której zatrudniony był Użytkownik,
        b) IOD, lub w jego zastępstwie Kierownik Działu Prawnego i Zamówień Publicznych (PZP), wpisuje w ewidencji osób upoważnionych do przetwarzania Danych osobowych, datę wygaśnięcia upoważnienia do przetwarzania Danych osobowych,
    2) w karcie obiegowej Użytkownika, z którym rozwiązano stosunek pracy:
        a) ASI potwierdza zamknięcie konta pracownika w systemie informatycznym,
        b) IOD lub Kierownik PZP potwierdza wpisanie do ewidencji osób upoważnionych daty wygaśnięcia upoważnienia.

IX. Nadawanie, zmiana i odbieranie upoważnień do przetwarzania Danych osobowych.

1. Kierownik komórki organizacyjnej CNK po zatrudnieniu nowego pracownika występuje z wnioskiem do IOD o nadanie mu upoważnienia do przetwarzania Danych

osobowych, zgodnie z regulacjami zawartymi w treści *Procedury nadawania upoważnień do przetwarzania danych osobowych w Centrum Nauki Kopernik.*

2. Wniosek zawiera imię i nazwisko, stanowisko i nazwę komórki organizacyjnej, zakres upoważnienia, uzasadnienie oparte na zakresie obowiązków pracownika.
3. IOD, a w przypadku jego nieobecności Kierownik PZP, aprobuje wniosek lub go odrzuca, w zależności od relacji zakresu obowiązków pracownika do wnioskowanego zakresu upoważnienia:
    a) w przypadku akceptacji wniosku wystawia upoważnienie do przetwarzania Danych osobowych uwzględniając wnioskowany zakres (upoważnienie powinno być nadane w formie pisemnej),
    b) w przypadku odmowy zwraca wniosek do wnioskodawcy z uzasadnieniem odmowy nadania upoważnienia.
4. Niezależnie od postanowień pkt. 1 – 3 powyżej, w przypadku, gdy upoważnienie ma być wydane na rzecz któregoś z Dyrektorów wymienionych w § 10 ust. 1 Statutu Centrum Nauki Kopernik lub osoby pełniącej funkcje kierownika komórki organizacyjnej, zakres upoważnienia może zostać uzgodniony pomiędzy IOD a osobą, na rzecz której ma być wystawione upoważnienie, przy użyciu poczty elektronicznej, bez konieczności sporządzania pisemnego wniosku.
5. Zapisy pkt. 1-3 powyżej stosuje się odpowiednio w przypadku, gdy dostęp do Danych osobowych, których administratorem jest CNK, miałaby uzyskać osoba zatrudniona na podstawie umowy cywilno-prawnej.
6. IOD prowadzi ewidencję osób upoważnionych do przetwarzania Danych osobowych, która zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania upoważnienia, zakres upoważnienia do przetwarzania danych osobowych, identyfikator osoby posiadającej uprawniania do systemu informatycznego (jeśli znajduje zastosowanie).
7. W przypadku zbioru RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki) upoważnienia nadawane są na wniosek Kierownika Projektu skierowany do IOD. Wzór upoważnienia do zbioru, o którym mowa w zdaniu poprzednim, stanowi załącznik nr 4 do niniejszej procedury. Wzór odwołania upoważnienia stanowi załącznik nr 5 do niniejszej procedury.
8. W stosunku do osób upoważnionych do przetwarzania danych zawartych w zbiorze RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki), IOD prowadzi ewidencję odrębną do ewidencji, o której mowa w pkt. 6 powyżej.

X. Załączniki

Załącznik nr 1 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Zakres upoważnienia:

A - Zbiór kadrowo płacowy

B - Zbiór kandydatów do pracy

C - Zbiór ZFŚS

D - Zbiór umowy cywilno-prawne

E- Rejestr korespondencji

F- Zbiór newsletters

G- Zbiór imprezy (Organizacja różnego rodzaju imprez kulturalnych)

H- Zbiór członków klubów młodego odkrywcy (KMO)

I- Baza adresy (adresy kontaktowe do osób zainteresowanych wydarzeniami, goście specjalni), Baza dziennikarzy (kontakty służbowe)

J- Zbiór Śpiewająca Wiki

K- Zbiór Konkurs FameLab

L- Zbiór danych klientów

M- Zbiór – Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007

N- Zbiór danych konkursów (wszystkie inne konkursy niż wymienione powyżej)

O- Europejskie Biuro Edukacji Kosmicznej ESERO

P- Klub Kopernika

Q- Ewidencja gości

Lp.	Data nadania	imię i nazwisko	Identyfikator	komórka organizacyjna	upoważnienie	zakres	Data ustania
					nadanie		
					modyfikacja		
					ustanie		

Ewa Kloc
DYREKTOR ADMINISTRACYJNY
CENTRUM NAUKI KOPERNIK

Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 29 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) udzielam Pani/Panu*

.....

(imię i nazwisko pracownika)

.....

(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych, których Administratorem danych jest Centrum Nauki Kopernik w Warszawie oraz do przetwarzania danych powierzonych Centrum Nauki Kopernik przez podmioty trzecie.

Jest Pani/Pan* upoważniony/upoważniona* do przetwarzania danych osobowych zgodnie z poniższym zakresem:

Zakres upoważnienia (oznaczyć „X" we właściwych polach). Zakres danych osobowych w poszczególnych zbiorach jest dodatkowo ograniczany ze względu na zakres obowiązków pracownika.	
	(A) Zbiór kadrowo płacowy
	(B) Zbiór kandydatów do pracy.
	(C) Zbiór ZFŚS.
	(D) Zbiór umowy cywilno-prawne.
	(E) Rejestr korespondencji.
	(F) Zbiór newsletters
	(G) Zbiory osób chcących uczestniczyć w imprezach CNK.
	(H) Zbiór członków klubów młodego odkrywcy (KMO)
	(I) Baza adresy, Baza dziennikarzy (kontakty służbowe)
	(J) Zbiór Śpiewająca Wiki
	(K) Zbiór Konkurs FameLab
	(L) Zbiór danych klientów
	(M) Zbiór – Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007
	(N) Zbiór danych konkursów (wszystkie inne konkursy niż wymienione powyżej)

	(O) Europejskie Biuro Edukacji Kosmicznej ESERO
	(P) Klub Kopernika
	(Q) Ewidencja gości

Osoba upoważniona może korzystać z danych osobowych zawartych we wskazanych wyżej zbiorach tylko w granicach swoich obowiązków pracowniczych oraz przy zachowaniu obowiązujących w tym zakresie w Centrum Nauki Kopernik procedur. Upoważnienie traci ważność z chwilą ustania stosunku pracy. Upoważnienie może być stosowane dla osób świadczących pracę na rzecz Centrum Nauki Kopernik na podstawie stosunku cywilno-prawnego. W takim przypadku zakres upoważnienia do przetwarzania danych osobowych w poszczególnych zbiorach dodatkowo jest ograniczony treścią zawartej umowy i traci ważność w chwili wygaśnięcia stosunku prawnego.

.....

(data i podpis)

* niepotrzebne skreślić

Załącznik nr 3 – zakres danych przetwarzanych w zbiorze RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki).
Załącznik nr 4 – wzór upoważnienia do zbioru RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki).
Załącznik nr 5 – wzór odwołania upoważnienia do zbioru RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki).
Załącznik nr 6 – Dokumentacja regulująca szczegółowe zasady przetwarzania danych osobowych w Zbiorze Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007.

Na niniejszą dokumentację składają się:

1. POLITYKA BEZPIECZEŃŚTWA DLA ZBIORU PODSYSTEM MONITOROWANIAEUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007 U BENEFICJENTA PO KL.
2. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM DLA SYSTEMU PODSYSTEM MONITOROWANIA EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007 U BENEFICJENTA PO KL.
3. WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH W ZBIORZE PODSYSTEM MONITOROWANIA EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007.
4. WZÓR ODWOŁANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH W ZBIORZE PODSYSTEM MONITOROWANIA EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO 2007.
5. FORMULARZ PEFS 2007 – POKL.

Załącznik 3 do umowy: Zakres danych osobowych powierzonych do przetwarzania

Nazwa i adres Beneficjenta (miejsce i data)

Nazwa i nr projektu

Zakres danych osobowych przetwarzanych w Zbiorze RPO WM 2014-2020

1.	Imię
2.	Nazwisko
3.	Miejsce pracy-Instytucja
4.	PESEL
5.	Telefon kontaktowy
6.	Adres e-mail
7.	Adres strony www
8.	Login
9.	Kraj
10.	Forma prawna
11.	Forma własności
12.	NIP
13.	REGON
14.	Nazwa rejestru i nr wpisu
15.	PKD
16.	Adres:
17.	Ulica
18.	Nr budynku
19.	Nr lokalu
20.	Kod pocztowy
21.	Miejscowość
22.	Nr telefonu
23.	Nr faksu
24.	Typ inwestycji
25.	Obszar wg stopnia urbanizacji
26.	Rodzaj przyznanego wsparcia
27.	Rodzaj uczestnika

Zakres danych osobowych przetwarzanych w Zbiorze CST

1	Imię
2	Nazwisko
3	Miejsce pracy-Instytucja
4	PESEL

5	Telefon kontaktowy
6	Adres e-mail
7.	Adres strony www
8.	Login
9.	Kraj
10.	Forma prawna
11.	Forma własności
12.	NIP
13.	REGON
14.	Nazwa rejestru i nr wpisu
15.	PKD
16.	Adres:
17.	Ulica
18	Nr budynku
19.	Nr lokalu
20.	Kod pocztowy
21.	Miejscowość
22.	Nr telefonu
23.	Nr faksu
24.	Typ inwestycji
25.	Obszar wg stopnia urbanizacji
26.	Data rozpoczęcia udziału w projekcie
27.	Data zakończenia udziału w projekcie
28.	Czy wsparciem zostali objęci pracownicy instytucji
29.	Rodzaj przyznanego wsparcia
30.	Rodzaj uczestnika
31.	Wiek w chwili przystępowania do projektu
32.	Wykształcenie
32.	Wykonywany zawód
33.	Zatrudniony (miejsce zatrudnienia)
34.	Zakończenie udziału osoby w projekcie zgodnie z zaplanowaną dla niej ścieżką uczestnictwa
35.	Data założenia działalności gospodarczej
36.	Kwota przyznanych środków na założenie działalności gospodarczej
37.	PKD założonej działalności gospodarczej
38.	Forma zaangażowania
39.	Okres zaangażowania w projekcie
40.	Wymiar czasu pracy
41.	Stanowisko
42.	Płeć
43.	Status osoby na rynku pracy w chwili przystąpienia do projektu

44.	Sytuacja osoby w momencie zakończenia udziału w projekcie
45.	Osoba należąca do mniejszości narodowej lub etnicznej, migrant, osoba obcego pochodzenia
46.	Osoba bezdomna lub dotknięta wykluczeniem z dostępu do mieszkań
47.	Osoba z niepełnosprawnościami
48.	Osoba przebywająca w gospodarstwie domowym bez osób pracujących
49.	W tym: gospodarstwie domowym z dziećmi pozostającymi na utrzymaniu
50.	Osoba żyjąca w gospodarstwie składającym się z jednej osoby dorosłej i dzieci pozostających na utrzymaniu
51.	Osoba w innej niekorzystnej sytuacji społecznej (innej niż wymienione powyżej)

Upoważnienie nr _____

do przetwarzania danych osobowych

Z dniem _____ r., na podstawie art. 37 w związku z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze zm.), upoważniam _____ do przetwarzania danych osobowych w zbiorze RPO WM 2014-2020 (projekt Szkoła Bliżej Nauki). Upoważnienie wygasa z chwilą ustania Pana/Pani* zatrudnienia w Centrum Nauki Kopernik lub z chwilą jego odwołania.

_____

Czytelny podpis osoby upoważnionej do wydawania i odwoływania upoważnień.

Upoważnienie otrzymałem

_____

(miejscowość, data, podpis)

Oświadczam, że zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), a także z obowiązującymi w Centrum Nauki Kopernik Polityką bezpieczeństwa ochrony danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie zatrudnienia w Centrum Nauki Kopernik, jak też po jego ustaniu.

_____

Czytelny podpis osoby składającej oświadczenie

*niepotrzebne skreślić

Załącznik nr 5: Odwołanie upoważnienia do przetwarzania danych osobowych na poziomie Beneficjenta i podmiotów przez niego umocowanych

Odwołanie upoważnienia nr _____ do przetwarzania danych osobowych

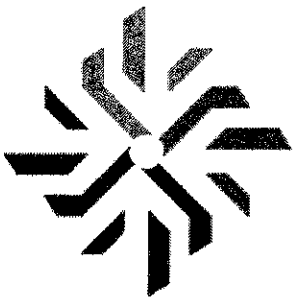
Z dniem ..... r., na podstawie art. 37 w związku z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), odwołuję upoważnienie Pana /Pani* ..... do przetwarzania danych osobowych nr ..... wydane w dniu .....

.....
czytelny podpis osoby, upoważnionej do wydawania i odwoływania upoważnień

.....
miejscowość, data

*niepotrzebne skreślić

Instrukcja Zarządzania Systemami Informatycznymi



CENTRUM NAUKI KOPERNIK

Spis treści

Niniejszy dokument ma na celu zapewnienie bezpieczeństwa danych osobowych w zakresie ich przetwarzania w systemie informatycznym Centrum Nauki Kopernik.

1. Podstawa prawna

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej jako „Ustawa").
2. Rozporządzenie Parlamentu Europejskiego i Rady (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 (ogólne rozporządzenie o ochronie danych, dalej jako „RODO").

2. Definicje

1. CNK – Centrum Nauki Kopernik z siedzibą w Warszawie przy ul. Wybrzeże Kościuszkowskie 20, zarejestrowane przez Prezydenta m.st. Warszawy w Rejestrze Instytucji Kultury pod numerem 2/06.
2. Administrator danych osobowych (ADO) – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. W niniejszej Polityce bezpieczeństwa przez Administratora danych osobowych rozumie się CNK.
3. Inspektor Ochrony danych (IOD) – osoba wyznaczona przez Administratora danych na podstawie art. 37 RODO.
4. Administrator Systemu Informatycznego (ASI) – osoba zarządzająca Systemem informatycznym.
5. Użytkownik – osoba posiadająca uprawnienie dostępu do Systemu informatycznego.
6. Kierownik komórki organizacyjnej CNK – osoba będąca przełożonym Użytkownika, w imieniu którego występuje do ASI w sprawie nadania, modyfikacji lub odebrania uprawnień do Systemu informatycznego.
7. Informacja – dane, które mogą być wyrażone za pomocą pisma, obrazu lub dźwięku, zawarte w Systemie informatycznym.
8. Identyfikator– rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania Danych osobowych w Systemie informatycznym.
9. Hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w Systemie informatycznym.

10. Uwierzytelnienie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika.
11. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
12. Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
13. Przetwarzanie danych – 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.
14. System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania Informacji i narzędzi programowych zastosowanych w celu przetwarzania Danych osobowych, funkcjonujący w CNK.

3. Procedura nadawania uprawnień do przetwarzania Danych osobowych i rejestrowania tych uprawnień w Systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Osobą odpowiedzialną za nadawanie, modyfikację oraz odbieranie uprawnień do Systemu informatycznego jest ASI.
2. Kierownik komórki organizacyjnej CNK występuje z wnioskiem (określającym zakres i czas uprawnienia) do IOD o nadanie uprawnień do Systemu informatycznego zatrudnionemu pracownikowi (forma pisemna lub elektroniczna). Zakres i czas uprawnienia do przetwarzania danych jest uzależniony od zakresu obowiązków pracownika.
3. Wniosek zawiera: imię, nazwisko, wnioskowany zakres uprawnień, uzasadnienie ze względu na zakres obowiązków.
4. IOD, a w przypadku jego nieobecności Kierownik Działu Prawnego i Zamówień Publicznych (PZP), aprobuje wniosek lub go odrzuca, w zależności od relacji zakresu obowiązków służbowych oraz zakresu upoważnienia do przetwarzania danych osobowych do zakresu wnioskowanych uprawnień:
    - w przypadku akceptacji wniosku, kieruje go do ASI w celu nadania uprawnienia pracownikowi,

- w przypadku odmowy, wniosek wraca do wnioskodawcy z uzasadnieniem odmowy nadania uprawnień.

5. W przypadku, gdy osoba, której dotyczy wniosek, będzie przetwarzać Dane osobowe, warunkiem uzyskania uprawnień do Systemu informatycznego jest posiadanie przez tę osobę upoważnienia do przetwarzania Danych osobowych.
6. W przypadku konieczności modyfikacji uprawnień, Kierownik komórki organizacyjnej CNK występuje do IOD z wnioskiem o modyfikację uprawnienia.
7. Wniosek o modyfikację uprawnienia zawiera: imię, nazwisko, wnioskowany zakres uprawnień, uzasadnienie ze względu na zakres obowiązków.
8. IOD, a w przypadku jego nieobecności Kierownik PZP, aprobuje wniosek o modyfikację uprawnień lub go odrzuca, w zależności od relacji zakresu obowiązków służbowych oraz zakresu upoważnienia do przetwarzania Danych osobowych do zakresu wnioskowanego uprawnienia:
   - w przypadku akceptacji wniosku kieruje go do ASI w celu modyfikacji uprawnień pracownika,
   - w przypadku odmowy, wniosek wraca do wnioskodawcy z uzasadnieniem odmowy nadania uprawnienia.
9. W przypadku ustania stosunku pracy (rozwiązania umowy o pracę lub rozwiązania umowy, na podstawie której osoba posiadała uprawnienia do Systemu informatycznego), Kierownik komórki organizacyjnej CNK występuje do ASI z wnioskiem o odebranie dostępu do Systemu informatycznego.
10. ASI, nadając, modyfikując lub odbierając uprawnienie do Systemu informatycznego, czynność tę rejestruje w prowadzonym rejestrze. Rejestr zawiera imię i nazwisko pracownika, Identyfikator, zakres dostępu, okres w jakim uprawnienie jest ważne.
11. ASI prowadzi dokumentację związaną z nadawaniem, modyfikacją oraz odbieraniem uprawnień do Systemu informatycznego, na którą składają się wnioski o nadanie, modyfikację i odebranie uprawnienia, pokwitowania odbioru Identyfikatora i Hasła.

4. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Każdy Użytkownik posiada swój niepowtarzalny Identyfikator i Hasło.

2. Użytkownik posiadający dostęp do Systemu informatycznego jest zobowiązany do zachowania w tajemnicy posiadanego Hasła.
3. Na podstawie zaakceptowanego wniosku, ASI przekazuje Użytkownikowi, w zaklejonej kopercie z nadrukowanymi danymi Użytkownika, jego Identyfikator i Hasło.
4. Użytkownik poprzez pierwsze logowanie potwierdza fakt otrzymania Identyfikatora oraz Hasła.
5. Użytkownik (który otrzymał Identyfikator i Hasło) – po zalogowaniu powinien niezwłocznie zmienić Hasło.
6. Hasło powinno się składać z przynajmniej 8 znaków uwzględniając duże i małe litery oraz cyfry lub znaki specjalne.
7. Hasło powinno być zmienione nie rzadziej, niż co 30 dni.
8. Identyfikator, nie może być przydzielony innej osobie.
9. W przypadku, gdy Użytkownik zgubi lub zapomni Hasło zwraca się do ASI o nadanie nowego. Użytkownik poprzez ponowne logowanie potwierdza fakt otrzymania nowego Hasła. Fakt ten powinien zostać odnotowany Systemie informatycznym.
10. W przypadku ustania stosunku pracy (rozwiązania umowy o pracę lub rozwiązania umowy, na podstawie której Użytkownik posiadał uprawnienia do Systemu informatycznego) ASI, na podstawie otrzymanej tzw. obiegówki zamyka wszystkie dostępy do Systemu informatycznego.
11. Każdy Użytkownik zobowiązany jest do zachowania w poufności Danych osobowych i Informacji, w których posiadanie wszedł w związku z przyznaniem dostępu do Systemu informatycznego.

5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla Użytkowników Systemu informatycznego.

1. W celu rozpoczęcia pracy Użytkownik wprowadza Identyfikator i Hasło do okna dialogowego komputera.
2. Użytkownik, w przypadku braku możliwości zalogowania się, niezwłocznie informuje o tym fakcie ASI.
3. W przypadku zawieszenia pracy, każdy Użytkownik jest zobowiązany do zablokowania stacji roboczej.

4. W przypadku zakończenia pracy, Użytkownik jest zobowiązany do wylogowania się z konta Użytkownika (do którego jest uprawniony).

6. Procedury tworzenia kopii zapasowych Zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Procedura stanowi odrębny dokument, który jest opracowany i aktualizowany przez ASI.
2. ASI dołącza procedurę do niniejszej dokumentacji. Procedura może być udostępniona tylko osobom upoważnionym przez Dyrektora Naczelnego CNK lub ASI.

7. Sposób, miejsce i okres przechowywania.

1. Elektronicznych nośników Informacji zawierających Dane osobowe:
   - nośniki służące do przenoszenia Danych osobowych pomiędzy stacjami roboczymi oraz pomiędzy systemami informatycznymi powinny być kasowane w sposób uniemożliwiający odtworzenie danych, niezwłocznie po ich przeniesieniu,
   - nośniki służące do przechowywania Danych osobowych powinny być zabezpieczone przed dostępem osób nieupoważnionych,
   - w przypadku, gdy w posiadanie nośnika wejdzie osoba nieupoważniona, niezwłocznie należy o tym poinformować IOD lub ASI.
2. Kopii zapasowych:
   - kopie zapasowe powinny umożliwić odtworzenie danych z okresu do 2 dni,
   - kopie zapasowe powinny być przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym (szafa pancerna, pomieszczenia o określonym dostępie),
   - dla kopii zapasowych składowanych na nośnikach typu: taśma, płyta CD/DVD: nośnik zawierający kopię zapasową powinien być przechowywany nie krócej niż 1 miesiąc,
   - o każdym dostępie do nośników zawierających kopie zapasowe powinien być poinformowany ASI.

8. Sposób zabezpieczenia Systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do Systemu informatycznego.

Zabezpieczenie:

1. Zastosowane jest oprogramowanie antywirusowe oraz adekwatne do potrzeb biznesowych zabezpieczenie styku z siecią publiczną.
2. Osobą odpowiedzialną za zabezpieczenie Systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do Systemu informatycznego jest ASI.
3. Każdy Użytkownik systemu ma obowiązek niezwłocznie poinformować ASI o każdej zauważonej nieprawidłowości w Systemie informatycznym.
4. ASI opracowuje i aktualizuję dokumentację opisującą procedurę zabezpieczenia Systemu informatycznego. Dokumentacja jest dołączana do niniejszej dokumentacji i może być udostępniona tylko osobom upoważnionym przez Dyrektora Naczelnego CNK lub ASI.
5. Instalacja prywatnego oprogramowania na komputerze służbowym wymaga uprzedniej zgody ASI i okazania licencji na użytkowanie oprogramowania. Oprogramowanie, o którym mowa w zdaniu poprzednim, nie może być wykorzystywane do celów służbowych. Użytkownik oprogramowania jest odpowiedzialny za posiadanie licencji do oprogramowania.

9. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników Informacji służących do przetwarzania Danych osobowych.

1. Celem wykonywania przeglądów i konserwacji Systemów informatycznego oraz nośników Informacji jest zapewnienie bezpieczeństwa procesom przetwarzania Danych osobowych.
2. Przeglądy powinny być wykonywane okresowo, przynajmniej raz na 6 miesięcy.
3. Zakres przeglądów jest uzależniony od rodzaju urządzeń będących elementami Systemu informatycznego.
4. Osobą uprawnioną do dokonywania przeglądów i konserwacji jest ASI.

5. W przypadku powierzenia osobie trzeciej czynności przeglądów i konserwacji Systemu informatycznego, Dane osobowe powinny być usunięte, lub też wszelkie czynności powinny być wykonywane pod nadzorem ASI.
6. W przypadku przekazania do naprawy nośników informatycznych, wszelkie Dane osobowe powinny być z nich usunięte.
7. Każde powierzenie wykonywania czynności przeglądów i konserwacji Systemu informatycznego oraz nośników Informacji powinno odbywać się na podstawie pisemnej umowy zaopiniowanej przez IOD.

10. Zasady użytkowania komputerów przenośnych.

1. Korzystanie z komputerów przenośnych odbywa się za zgodą ASI.
2. Udostępnienie komputera przenośnego następuje na wiosek Kierownika komórki organizacyjnej składany w formie elektronicznej.
3. Wniosek powinien zawierać uzasadnienie.
4. ASI podejmuje decyzję o wydaniu przenośnego komputera Użytkownikowi.
5. ASI prowadzi dokumentację dotyczącą wydanych komputerów przenośnych.
6. Użytkownik komputera przenośnego jest zobowiązany do zachowania szczególnej staranności podczas transportu, przechowywania i użytkowania komputera przenośnego poza obszarem CNK.
7. Komputer przenośny powinien mieć zainstalowane oprogramowanie antywirusowe, które powinno być przynajmniej raz w tygodniu aktualizowane.

Ewa Kloc
DYREKTOR ADMINISTRACYJNY
CENTRUM NAUKI KOPERNIK