POLITYKA
OCHRONY DANYCH OSOBOWYCH

Wstęp

Niniejsza Polityka Ochrony Danych Osobowych (PODO) określa zasady przetwarzania danych osobowych obowiązujące w Centrum Usług Wspólnych w Halinowie (CUW) i dotyczy wszystkich pracowników przetwarzających dane osobowe w CUW, niezależnie od podstawy zatrudnienia.

PODO zawiera opis zastosowanych środków organizacyjnych i technicznych pozwalających na zoptymalizowanie bezpieczeństwa przetwarzania danych osobowych, zarówno w zbiorach tradycyjnych (papierowych) jak i w infrastrukturze informatycznej.

DEFINICJE

- **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

- **Szczególna kategoria danych osobowych (tzw. dane „wrażliwe")** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;

- **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych 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;

- **Administrator (ADO)** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

- **Administrator Systemów Informatycznych (ASI)** - pracownik Działu IT administrujący systemami informatycznymi służącym do przetwarzania danych, odpowiedzialny za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w tych systemach.

- **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

- **Bezpieczeństwo systemu informatycznego/systemu przetwarzania informacji** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz

informacji przed nieautoryzowaną modyfikacją, utratą, nieuprawnionym dostępem i nieuprawnionym ujawnieniem osobom nieupoważnionym (utrata poufności, integralności i dostępności).

- **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

- **Zgoda** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

- **Bezpieczeństwo danych osobowych** oznacza ochronę danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

- **Osoba upoważniona** – osoba posiadająca upoważnienie wydane przez ADO, na mocy którego wykonuje określone czynności przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.

- **Identyfikator użytkownika (LOGIN) –** ciąg znaków literowych i cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

- **UODO –** Urząd Ochrony Danych Osobowych

- **PUODO –** Prezes Urzędu Ochrony Danych Osobowych

- **RODO –** 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 rozporządzenia o ochronie danych).

- **PODO** – Polityka Ochrony Danych Osobowych

- **Inspektor Ochrony Danych (IOD)** - osoba wyznaczona na podstawie art. 37 RODO przez Administratora do wykonywania zadań z zakresu ochrony danych określonych w art. 39 RODO oraz posiadająca status, zgodnie z art. 38 RODO.

- **CUW** – Centrum Usług Wspólnych w Halinowie

- **Pracownik –** osoba zatrudniona w CUW Halinów, niezależnie od podstawy zatrudnienia.

Rozdział I.
Postanowienia ogólne

1. Przetwarzanie danych osobowych w CUW oparte jest na przestrzeganiu przepisów:
   1) 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 praz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych) – dalej RODO;
   2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   3) przepisów innych ustaw, a także rozporządzeń normujących problematykę przetwarzania danych osobowych;

   oraz wewnętrznych ustaleń Dyrektora CUW.

2. CUW przetwarza dane osobowe:
   1) na podstawie statutu uchwalonego Uchwałą nr XXXVII.349.2021 Rady Miejskiej w Halinowie z dnia 3 listopada 2021 roku;
   2) w celu zapewnienia prawidłowej, zgodnej z prawem polityki personalnej oraz wypełnienia obowiązków prawnych ciążących na administratorze, jako pracodawcy;

3) dla realizacji innych celów i zadań – w szczególności wynikających z przepisów prawa lub prawnie uzasadnionych interesów administratora.

3. Szczególnej ochronie podlegają dane osobowe wymienione w art. 9 ust.1 RODO, tj. tzw. dane „wrażliwe".

4. PODO odnosi się do danych osobowych przetwarzanych w:
   1) tradycyjny sposób w wersji papierowej (np. akta osobowe, upoważnienia, umowy, wnioski, zaświadczenia itp.);
   2) systemach informatycznych i na nośnikach cyfrowych;
   3) systemach dozoru wizyjnego (monitoring).

5. PODO realizowana jest przez wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, w szczególności przez administratora danych osobowych (w osobie Dyrektora) – **ADO,** zgodnie z art. 24 RODO.

6. W CUW wyznaczono inspektora ochrony danych, zgodnie z art. 37 RODO, w osobie Pani Anny Walosińskej. Kontakt poprzez e-mail: iod.cuw.halinow@dpag.pl.

7. PODO obowiązuje we wszystkich pomieszczeniach, które zajmuje CUW.

8. Procedury i zasady określone w PODO mają zastosowanie do wszystkich osób przetwarzających dane osobowe a wykonujących prace związane z działalnością CUW lub na rzecz CUW (niezależnie od formy współpracy, czy rodzaju umowy).

Rozdział II.
Deklaracja Administratora Danych Osobowych

1. ADO deklaruje, iż wdrożył i stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

2. ADO zapewnia przestrzeganie zasad dotyczących bezpieczeństwa przetwarzania:
   a) pseudonimizacji i szyfrowania danych osobowych;
   b) zdolności do ciągłego zapewnienia poufności, integralności i dostępności przetwarzanych danych osobowych;
   c) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, skutkującego naruszeniem ochrony danych osobowych;
   d) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3. ADO uwzględniając zasady wynikające z art. 5 RODO zapewnia, aby dane osobowe były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości);
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzane dalej w sposób niezgodny z tymi celami;
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
   4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);

5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane i zgodnie z okresem przechowywania wymaganym przez odpowiednie przepisy prawa (zasada ograniczenia przechowywania);
6) 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 (zasada integralności i poufności);
7) przetwarzane w sposób, który pozwoli administratorowi wykazać, iż spełnione są zasady wymienione w pkt 1-6 (zasada rozliczalności).

Rozdział III.
Role i odpowiedzialności osób zaangażowanych w ochronę bezpieczeństwa przetwarzania

Obowiązki administratora (ADO)

1. Do obowiązków ADO należą w szczególności:
   1) obowiązek informacyjny wobec osoby, której dane dotyczą (art. 13 i 14 RODO);
   2) realizacja praw osoby fizycznej w tym prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia danych, ograniczenia przetwarzania, prawo do przenoszenia danych, wniesienia sprzeciwu oraz prawo do cofnięcia zgody;
   3) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (art. 24 RODO);
   4) prowadzenie rejestru czynności przetwarzania oraz kategorii czynności przetwarzania (art. 30 RODO);
   5) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   6) zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu (art. 33 RODO);
   7) prowadzenie rejestru naruszeń;
   8) w uzasadnionych przypadkach dokonywanie oceny skutków dla ochrony danych (art. 35 RODO).

Zadania i uprawnienia Inspektora ochrony danych (IOD)

1. Do zakresu obowiązków IOD należy w szczególności:
   1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach związanych z przestrzeganiem prawa o ochronie danych osobowych;
   2) monitorowanie przestrzegania przepisów oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane audyty;
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, zgodnie z art. 35 RODO;
   4) współpraca z organem nadzorczym – PUODO;
   5) pełnienie funkcji podmiotu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem;.

2. W celu powierzonych zadań IOD ma prawo:
   1) wglądu we wszystkie obszary przetwarzania danych osobowych, w tym wglądu do dokumentów;
   2) sprawdzać pracowników CUW w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
   3) żądać od pracowników CUW wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych

osobowych.

Obowiązki Administratora Systemów Informatycznych - ASI

1. Głównym obowiązkiem ASI jest zapewnienie bezpieczeństwa danych osobowych w systemach informatycznych stosowanych w CUW.
2. Do obowiązków ASI w zakresie ochrony danych osobowych należy w szczególności:
   1) wsparcie techniczne użytkowników w zakresie utrzymania i rozwoju infrastruktury systemowej;
   2) instalacja i konfiguracja sprzętu komputerowego;
   3) konfiguracja sieci;
   4) zarządzanie uprawnieniami, dostępami i kontami;
   5) zarządzanie aktualizacjami systemów i aplikacji;
   6) identyfikowanie zagrożeń ciągłości pracy oraz przeciwdziałanie awariom;
   7) współpraca z dostawcami usług serwisowych i wsparcia technicznego;
   8) dokumentowanie konfiguracji systemów oraz jej zmian;
   9) nadzór nad eksploatacją, naprawami, konserwacją i likwidacją urządzeń komputerowych oraz nośników, na których przetwarzane są dane osobowe;
   10) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;
   11) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych.

Rozdział IV.
Powierzanie i udostępnianie danych osobowych oraz prawa osób, których dane osobowe są przetwarzane

1. CUW, jako administrator danych powierza przetwarzane w swoich zasobach dane osobowe:

   1) osobom, które przetwarzają dane osobowe na polecenie administratora tj. posiadającym upoważnienie do przetwarzania danych osobowych; wszystkie osoby, którym zostaje udzielone upoważnienie do przetwarzania danych osobowych są zobowiązane do podpisania oświadczenia o zachowaniu poufności danych osobowych.
   2) podmiotom przetwarzającym, tj. osobom lub podmiotom na podstawie umowy powierzenia przetwarzania danych osobowych, która w szczególności określa:
      a) przedmiot i czas trwania przetwarzania;
      b) charakter i cel przetwarzania;
      c) rodzaj danych osobowych;
      d) kategorie osób, których dane dotyczą;
      e) obowiązki i prawa administratora.

2. ADO lub wyznaczona przez niego osoba prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz ewidencję podmiotów, z którymi zawarto umowy powierzenia, które stanowią odpowiednio załącznik nr 1 i 2 do niniejszej Polityki.

3. CUW, jako administrator danych udostępnia przetwarzane w swoich zasobach dane osobowe:
   1) osobom, których dane dotyczą,
   2) organom i podmiotom uprawnionym do kontroli działalności administratora;
   3) osobom oraz podmiotom uprawnionym na podstawie przepisów prawa.

4. Każda osoba, której dane osobowe dotyczą, na podstawie art. 15 RODO ma prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane w CUW, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   1) cele przetwarzania;

2) kategorie odnośnych danych osobowych;
3) odbiorcy lub kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcy w państwach trzecich lub organizacjach międzynarodowych;
4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5) prawo do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) prawo wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8) zautomatyzowane podejmowanie decyzji, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4, RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

5. Udostępnianie danych/informowanie o danych odbywa się na podstawie pisemnego wniosku osoby, której dane dotyczą. W momencie otrzymanie wniosku jw. obowiązują następujące zasady:
   1) odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania;
   2) wniosek o udostępnienie danych przekazywany jest do właściciela zasobów danych osobowych, który podejmuje decyzję o udostępnieniu i informuje o tym IOD;
   3) IOD akceptuje decyzję o udostępnieniu i przekazuje ją do właściciela zasobów danych osobowych;
   4) właściciel zasobów danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku;
   5) IOD prowadzi rejestr wniosków o udostępnienie danych, który stanowi załącznik nr 3 do niniejszej Polityki.

6. Odmowa udostępnienia danych osobowych następuje wówczas, gdy:
   1) spowodowałoby to naruszenia praw i wolności osób, których dane dotyczą oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy;
   2) o dane wnioskuje osoba lub podmiot nieuprawniony.

Rozdział V.
Zgoda na przetwarzanie danych osobowych

1. Zgoda na przetwarzanie danych osobowych nie jest wymagana w przypadkach określonych w art. 6 ust. 1 litery b)-f) RODO.

2. Zgoda na przetwarzanie danych osobowych tzw. „wrażliwych” nie jest wymagana w przypadkach określonych w art. 9 ust.1 litery b)-j) RODO.

3. Przetwarzanie danych osobowych w celach innych, niż ww. może odbywać się tylko wobec osób (lub ich opiekunów prawnych), które wcześniej wyraziły zgodę na piśmie na przetwarzanie danych osobowych, np. w celach marketingowych, w celu wzięcia udziału w konkursie itp.

4. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele.

5. Kandydaci do pracy jak i pracownicy zobowiązani są podpisać pisemną zgodę na przetwarzanie w zakresie danych wykraczających poza dane określone w Kodeksie Pracy, jeżeli takie dane podali dobrowolnie.

6. Osoba, której dane dotyczą może w każdej chwili wycofać wyrażoną zgodę bez podania przyczyny. Cofnięcie zgody nie ma wpływu na przetwarzanie, którego dokonano na podstawie zgody przed jej cofnięciem.

Rozdział VI.
Budynki, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe

1. CUW zajmuje wyznaczone pomieszczenia w budynku Urzędu Gminy Halinów.

2. Budynek jest ogrodzony i zabezpieczony przed nieuprawnionym wejściem elektronicznym systemem alarmowym.

3. Wejścia do budynków posiadają fizyczne zabezpieczenia w formie zamków oraz monitoringu wizyjnego.

4. Dane osobowe w wersji papierowej przechowywane są w szafach i szufladach zamykanych na klucze, do których dostęp mają tylko upoważnione osoby.

5. Urządzenia zawierające systemy informatyczne są zabezpieczone hasłem dostępu i w przypadku urządzeń przenośnych, po skończonej pracy zamykane na klucze w szafach.

6. W budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu i/lub przetwarzania danych osobowych.

7. Osoby nie upoważnione do przetwarzania danych osobowych, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, w których przetwarzane są dane osobowe, wyłącznie w obecności upoważnionego pracownika.

8. Osoby sprzątające pomieszczenia, w których przechowuje się dane osobowe, zostały pouczone o zasadach ochrony tych danych i podpisały stosowne oświadczenia poufności.

9. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe wiąże się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem tam osób niepowołanych.

10. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia lub danych jest niedopuszczalne, i będzie traktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

Rozdział VII.
Rejestry czynności przetwarzania danych osobowych

1. CUW, jako administrator danych osobowych prowadzi rejestr czynności przetwarzania, zgodnie z art. 30 RODO. Rejestr czynności przetwarzania danych osobowych jest aktualizowany na bieżąco, po każdej zmianie. Rejestr stanowi załącznik nr 4 do niniejszej Polityki.

2. CUW jest podmiotem przetwarzającym w rozumieniu art. 28 RODO na mocy porozumienia z jednostkami oświatowymi, dla obsługi których został powołany. CUW prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, który stanowi załącznik nr 5 do niniejszej Polityki.

3. Nadzór nad aktualizacją rejestrów, o których mowa powyżej prowadzi ADO lub osoba przez niego wyznaczona.

Rozdział VIII.
Zasady dotyczące bezpieczeństwa danych osobowych

1. Zasady dotyczące bezpieczeństwa przetwarzania danych osobowych:
   1) dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca pisemne upoważnienie. Pracownicy mają dostęp wyłącznie do takich informacji i danych, jakie się wiążą z wykonywaną przez nich pracą, której zakres został określony w umowie o pracę lub umowie cywilnoprawnej oraz w zakresie zadań/obowiązków (zasada wiedzy koniecznej);
   2) dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Każdy użytkownik powinien posiadać indywidualny identyfikator oraz hasło dostępu. Hasło powinno składać się z co najmniej 8 znaków (duże, małe litery, cyfry i znaki specjalne) np.: P@ssw0rd. Zabrania się udostępniania identyfikatora i hasła;
   3) pracownik może przetwarzać dane osobowe tylko w zakresie wskazanym w nadanym przez pracodawcę upoważnieniu do przetwarzania danych osobowych;
   4) decyzję o dopuszczeniu nowych programów lub systemów informatycznych służących przetwarzaniu danych osobowych podejmuje ADO;
   5) pracownik powinien korzystać z systemów informatycznych w sposób uniemożliwiający podejrzenie danych osobowych przez osobę nieupoważnioną (odpowiednie ustawienie monitora, stosowanie wygaszacza ekranu z hasłem itp.);
   6) instalowanie programów i aplikacji na komputerach/telefonach służbowych tylko za zgodą ADO;
   7) wynoszenie danych osobowych poza obszar CUW (zarówno w wersji papierowej, jak i elektronicznej) jest z zasady zabronione. Wyjątek stanowią tylko te przypadki, na które wyraził zgodę ADO;
   8) pracownicy podczas przetwarzania danych osobowych korzystają tylko z tych urządzeń, które udostępnił im pracodawca;
   9) podczas przetwarzania danych osobowych zabrania się korzystania z urządzeń prywatnych;
   10) przesyłanie drogą elektroniczną danych osobowych odbywa się tylko w formie zaszyfrowanej;
   11) niszczenie danych osobowych w formie papierowej powinno odbywać się z użyciem dostępnej niszczarki;
   12) w przypadku drukowania danych osobowych należy stosować tzw. „bezpieczny wydruk".

2. Zasady bezpieczeństwa podczas przekazywania danych osobowych:
   1) stosowanie technik kryptograficznych podczas przesyłania danych publicznymi sieciami telekomunikacyjnymi z zachowaniem zasady, iż hasło podajemy inną drogą, niż przesłane pliki;
   2) zapewnienie ochrony przesyłanych danych osobowych przed przechwyceniem, skopiowaniem, modyfikacją, zniszczeniem poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych oraz należytej staranności;
   3) weryfikacja osoby, której przekazuje się dane osobowe zarówno w formie pisemnej, elektronicznej jak i ustnej;
   4) zachowanie szczególnej ostrożności w trakcie rozmów telefonicznych, aby uniknąć podsłuchania danych osobowych przez osoby nieupoważnione;
   5) przekazywanie danych w formie papierowej w zamykanych kopertach/teczkach, z unikaniem pośredników;
   6) nie pozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach, poczcie głosowej.

3. Szczegółowe zasady dotyczące przetwarzania danych w systemach informatycznych opisano w Instrukcji Zarządzania Systemami Informatycznymi, która stanowi załącznik nr 6 do niniejszej Polityki.
4. W CUW zastosowano następujące środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, w szczególności:
   1) wyznaczono Inspektora Ochrony Danych;
   2) wdrożono niniejszą Politykę Ochrony Danych Osobowych;
   3) wdrożono Instrukcję Zarządzania Systemami Informatycznymi;
   4) wdrożono Procedurę postępowania w sytuacji naruszenia ochrony danych osobowych (załącznik nr 7);
   5) przeprowadzono szkolenia pracowników w zakresie bezpieczeństwa przetwarzania danych osobowych;
   6) przeprowadzono ocenę ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i skutku zagrożenia, w związku z przetwarzaniem danych osobowych (załącznik nr 8);
   7) wprowadzono ewidencję osób, którym nadano upoważnienie do przetwarzania danych osobowych;
   8) wprowadzono ewidencję podmiotów, z którymi zawarto umowy powierzenia;
   9) wprowadzono rejestr wniosków o udostępnienie danych;
   10) wprowadzono kontrolę dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
   11) zablokowano dostęp do komputerów elektronicznych urządzeń przenośnych, typu pendrive.

Rozdział IX.
Naruszenia bezpieczeństwa ochrony danych osobowych

Postępowanie w przypadku naruszenia bezpieczeństwa ochrony danych osobowych zostało opisane w Procedurze postępowania w sytuacji naruszenia ochrony danych osobowych.

Rozdział X.
Odpowiedzialność służbowa i karna

1. Pracownik, który przetwarza dane osobowe:
   a) do których przetwarzania nie jest upoważniony,
   b) których przetwarzanie jest zabronione,
   c) niezgodnie z celem, dla którego zostały zebrane,
   d) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
   e) nie zgłasza naruszenia bezpieczeństwa ochrony danych osobowych;
   f) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw;

   podlega odpowiedzialności karnej wynikającej z art. 107 z dnia 10 maja 2018 roku Ustawy o ochronie danych osobowych, a także art. 266-267 Kodeksu Karnego.
2. Naruszenie zasad ochrony danych osobowych może również zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną określoną w odrębnych przepisach.
3. Inne osoby mające dostęp do danych osobowych ponoszą odpowiedzialność na podstawie odrębnych umów gwarantujących im dostęp, lub na podstawie przepisów gwarantujących im dostęp.

Rozdział XI.
Postanowienia końcowe

1. CUW na bieżąco dokłada wszelkich starań, aby gromadzone i przetwarzane dane osobowe podlegały ochronie zgodnie z wymogami obowiązującego w tym zakresie prawa.

2. PODO jest przeglądana pod kątem jej aktualizacji przynajmniej raz w roku lub w razie wystąpienia istotnych zmian dotyczących przetwarzania danych osobowych, np. organizacyjnych lub wymagań prawnych.

3. W celu oceny zgodności prowadzonej działalności z wymaganiami RODO, przeprowadza się co najmniej 1 raz w roku audyty sprawdzające.

4. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z niniejszą Polityką przed dopuszczeniem do przetwarzania danych osobowych.

Załączniki:

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
2. Ewidencja podmiotów, z którymi zawarto umowy powierzenia.
3. Rejestr wniosków o udostępnienie danych.
4. Rejestr czynności przetwarzania.
5. Rejestr kategorii czynności przetwarzania.
6. Instrukcja Zarządzania Systemami Informatycznymi.
7. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.
8. Analiza ryzyka.

Źródło

1. 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 praz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenia o ochronie danych).
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
3. uodo.gov.pl
4. Ustawa z dnia 6 czerwca 1997r. Kodeks karny.

Dyrektor CUW:

Signature Not Verified
Dokument podpisany przez Dominika Martoń-Jaroszewska
Data: 2022.06.08 14:07:59 CEST

.....

Wersja	1
Obowiązuje od	01.06.2022