ZARZĄDZENIE NR ....89/2018.
STAROSTY CHODZIESKIEGO

z dnia 12 grudnia 2018 r.

w sprawie wprowadzenia Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, w tym ochrony danych osobowych Starostwa Powiatowego w Chodzieży

Na podstawie art. 35 ust. 2 ustawy z dnia ustawy z dnia 5 czerwca 2018r. o samorządzie powiatowym (Dz.U z 2018r. poz. 995 z późn. zm.), w związku z art. 24 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady UE (2016/679) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (Dz. Urz. UE L 119 z dnia 4 maja 2016r., str. 1), zarządza się co następuje:

§ 1. Wprowadza się Dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, w tym ochrony danych osobowych Starostwa Powiatowego w Chodzieży, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2. Zobowiązuje się pracowników Starostwa Powiatowego w Chodzieży do stosowania zasad wynikających z dokumentacji, o której mowa w §1.

§ 3. Traci moc Zarządzenie Nr 43/2012 Starosty Chodzieskiego z dnia 27 września 2012r. w sprawie wprowadzenia „Polityki Bezpieczeństwa" w Starostwie Powiatowym w Chodzieży.

§ 4. Wykonanie Zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Mirosław Juraszek

Beata Kaniewska
Radca prawny
Bd P-195

Załącznik do zarządzenia Nr 89/2018
Starosty Chodzieskiego
z dnia 12 grudnia 2018 r.

DOKUMENTACJA SYSTEMU ZARZĄDZANIA

BEZPIECZEŃSTWEM INFORMACJI

W TYM OCHRONY DANYCH OSOBOWYCH

STAROSTWA POWIATOWEGO

W CHODZIEŻY

UL. WIOSNY LUDÓW 1

64-800 CHODZIEŻ

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w tym Ochrony Danych Osobowych

Starostwa Powiatowego w Chodzieży

zawiera:

Polityka Bezpieczeństwa Informacji
w zakresie bezpieczeństwa informacji i ochrony danych osobowych
podczas przetwarzania dokumentacji
w postaci tradycyjnej oraz elektronicznej
w
Starostwie Powiatowym w Chodzieży
64-800 Chodzież, ul. Wiosny Ludów 1

Szczegóły dokumentu:

Sporządził:	*Beata Lewandowska* Administrator Bezpieczeństwa Informacji Audytor Wewnętrzny PN/ISO 27001
Data przekazania:	

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Warunki użytkowania dokumentacji bezpieczeństwa informacji

Dokumentacja opracowana przez ABI – Audyt, Consulting, Outsourcing Beata Lewandowska podlega ochronie przepisami prawa autorskiego; właścicielem wszystkich praw autorskich jest ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Po dokonaniu płatności, ABI – Audyt, Consulting, Outsourcing Beata Lewandowska udziela Starostwu Powiatowemu w Chodzieży niewyłącznego, stałego, ograniczonego prawa użytkowania dokumentacji, bez ograniczeń terytorialnych, wyłącznie w sposób określony w niniejszym dokumencie. Wszystkie prawa, których nie udzielono w niniejszym dokumencie, są zastrzeżone.

Starostwo Powiatowe w Chodzieży ma prawo wykorzystywać zakupioną dokumentację w dowolnym celu, związanym z działalnością organizacji, w dowolny sposób zgodny z udzielonymi prawami.

Starostwo Powiatowe w Chodzieży ma prawo kopiować dokumentację, w całości lub w części, czasowo lub trwale, w dowolnej formie i dowolnymi środkami.

Starostwo Powiatowe w Chodzieży ma prawo tłumaczyć dokumentację na inne języki, modyfikować ją i dowolnie edytować.

Bezwzględnie zabronione jest usuwanie oznaczeń właściciela praw autorskich oraz użytkowanie dokumentacji komercyjnie dla celów niezwiązanych z działalnością organizacji. W szczególności zabronione jest wynajmowanie lub dystrybucja oryginałów lub kopii dokumentacji poprzez sprzedaż lub w inny sposób przekazywanie jej z intencją sprzedaży, jak również drukowanie, publikowanie, publiczne udostępnianie poprzez systemy naziemne lub bezprzewodowe oraz poprzez udzielanie dostępu do dokumentacji nieautoryzowanym stronom trzecim w dowolny sposób (w tym dostępu przez internet), bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Zabroniony jest transfer praw do korzystania z dokumentacji na rzecz powiązanych lub niepowiązanych osób prawnych lub fizycznych, włącznie z przedsiębiorstwami zależnymi oraz udzielanie takich praw jakimkolwiek stronom trzecim bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

2. Preambuła

Informacja będąca w posiadaniu instytucji ma realną wartość i może przybierać różne formy. Może być wydrukowana lub zapisana odręcznie na papierze, przechowywana elektronicznie, przesyłana pocztą lub za pomocą urządzeń elektronicznych, wyświetlana w formie filmów lub wypowiadana w czasie rozmowy. Niezależnie od tego, jaką formę przybiera lub za pomocą jakich środków jest udostępniana lub przechowywana, powinna być zawsze w odpowiedni sposób chroniona.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów w Starostwie Powiatowym w Chodzieży, opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Niniejszy dokument stanowi rekomendację ABI - Audyt, Consulting, Outsourcing Beata Lewandowska w zakresie bezpieczeństwa informacji i ochrony danych osobowych podczas przetwarzania dokumentacji osobowej w postaci tradycyjnej oraz elektronicznej.

Punktem wyjścia dla opracowania rekomendacji była analiza procesów przetwarzania danych wchodzących w skład dokumentacji osobowej przetwarzanej w postaci tradycyjnej i elektronicznej w Starostwie Powiatowym w Chodzieży. Dokumentację opracowano w oparciu o krajowe i europejskie przepisy ochrony danych osobowych oraz przepisy i regulacje branżowe.

Uwzględniono także wymagania i zalecenia norm ISO związanych z zapewnieniem bezpieczeństwa systemów informatycznych, co pozwala na określenie zaleceń dotyczących bezpiecznego przetwarzania dokumentacji osobowej w zależności od wybranego do jej przechowywania modelu architektury.

Wskazano również zagrożenia występujące podczas przetwarzania dokumentacji w postaci tradycyjnej i elektronicznej, oraz przedstawiono praktyczny plan wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji jako podstawowego zabezpieczenia stosowanego przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Chodzieży.

3. Cel i przeznaczenie dokumentu

Celem niniejszej dokumentacji jest przedstawienie zasad oraz procedur w zakresie budowania i stosowania systemu bezpiecznego przetwarzania danych osobowych w Starostwie Powiatowym w Chodzieży. Dokumentacja ma zastosowanie zarówno, gdy jest już przetwarzana dokumentacja w postaci elektronicznej, jak również gdy podmiot przygotowuje się lub też wdraża system informatyczny. Dokumentacja zawiera informacje w zakresie rozwiązań technicznych umożliwiających przetwarzanie dokumentacji osobowej. Zostały przedstawione wymagania organizacyjne oraz wskazano odpowiedzialność

za przetwarzanie informacji w tym danych osobowych wrażliwych zawartych w dokumentacji osobowej. Celem dokumentacji jest doprecyzowanie zakresu zastosowania przepisów RODO.

Nadrzędnym celem PBI jest:

1) Zapewnienie spełnienia wymagań prawnych.
2) Ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem.
3) Podnoszenie świadomości pracowników.
4) Zmniejszenie ryzyka utraty informacji.
5) Zaangażowanie wszystkich pracowników w ochronę informacji.
6) Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji.
7) Właściwy dobór zabezpieczeń (środków bezpieczeństwa) oparty na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań nadzoru, zobowiązań kontraktowych oraz pozostałych wymagań dotyczących bezpieczeństwa informacji w Starostwie Powiatowym w Chodzieży.

Bezpieczeństwo informacji zapewnione jest poprzez:

Zarządzanie ryzykiem, na które składa się:

1) Klasyfikacja zasobów i ich zawartości.
2) Identyfikacja stopnia zagrożeń i ich następstw.
3) Określenie i wdrożenie działań zabezpieczających zasoby.

Zarządzanie zmianami na które składa się:

a. Analiza wpływu zmian na poziom bezpieczeństwa.
b. Zapewnienie pełnej koordynacji podczas wprowadzania zmian.
c. Zarządzanie ciągłością działania organizacji poprzez wdrożenie instrukcji awaryjnych.

Zakres obowiązywania PBI w Starostwie Powiatowym w Chodzieży

Niniejszy dokument dotyczy wszystkich komórek organizacyjnych oraz wszystkich pracowników, a także innych osób mających dostęp do informacji chronionych w Starostwie Powiatowym w Chodzieży (np. pracowników firm zewnętrznych realizujących prace na rzecz podmiotu).

Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej, video lub innej).

Z dokumentem są zobowiązani zapoznać się wszyscy pracownicy Starostwa Powiatowego w Chodzieży mający dostęp do danych osobowych oraz innych chronionych informacji.

4. Deklaracja

Starostwo Powiatowe w Chodzieży deklaruje, że SZBI, w tym i niniejsza PBI została opracowana na podstawie rozporządzenia KRI, w świetle wytycznych standaryzujących obszary zabezpieczeń według Polskiej Normy PN-ISO/IEC 27001, oraz PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN- SO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

SZBI w Starostwie Powiatowym w Chodzieży to system zapewniający poufność, dostępność i integralność informacji z uwzględnieniem dodatkowo takich atrybutów, jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność, oraz ciągłość działania.

Kierownictwo Starostwa Powiatowego w Chodzieży i podmioty współpracujące, są proporcjonalnie zaangażowani w działaniach wspierania osób funkcyjnych i przestrzegania procedur zmierzających do zapewnienia bezpieczeństwa informacyjnego, na założonym poziomie.

Wdrożony SZBI, którego elementem jest niniejsza PBI, może podlegać ciągłemu doskonaleniu, zgodnie z wymaganiami normy PN-ISO/IEC 27001.

Celem wdrożonego w Starostwie Powiatowym w Chodzieży SZBI jest osiągnięcie właściwego poziomu organizacyjnego i technicznego, który:

1. maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę Starostwa Powiatowego w Chodzieży.
2. zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych (niepublicznych) oraz jawnych (publicznych).
3. zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów informatycznych przetwarzających informację.
4. Zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Starostwa Powiatowego w Chodzieży, jego interesów, posiadanych i powierzonych jemu informacji oraz będzie gwarantem właściwej ochrony informacji oraz ciągłości procesu ich przetwarzania.

5. Podstawowe pojęcia i skróty

1) **Administrator Danych Osobowych (ADO)** w rozumieniu RODO jednostka organizacyjna decydująca o celach i środkach przetwarzania danych osobowych reprezentowana przez Starostwo Powiatowe w Chodzieży.
2) **Inspektor Ochrony Danych (IOD)** – osoba fizyczna odpowiedzialna za zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie

danych osobowych, nadzorowanie opracowania i aktualizowania dokumentacji.

3) **Administrator Systemu Informatycznego (ASI)** - osoba odpowiedzialna za bezpieczeństwo i funkcjonowanie systemów informatycznych oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie.
4) **Akceptowanie ryzyka** - decyzja, aby zaakceptować ryzyko
5) **Aktywa** - wszystko, co ma wartość dla organizacji
6) **Analiza ryzyka** - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka
7) **Autentyczność**- właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane,
8) **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność
9) **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej 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. Za dane osobowe uważa się: nazwisko, imię, nazwisko rodowe, PESEL, NIP, data zatrudnienia, wykształcenie, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, seria i numer dowodu osobistego, książeczki wojskowej, stan cywilny, płeć, adres zamieszkania lub pobytu, informacje o stanie zdrowia, nałogach, przynależności wyznaniowej, związkowej. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
10) **Dane szczególnych kategorii** - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
11) **Dostępność** - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu
12) **Elektroniczne nośniki informacji – (ENI)** - zewnętrzne nośniki danych, w szczególności płyty CD, DVD, PenDrive, pamięci typu FLASH,
13) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
14) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
15) **Incydent związany z bezpieczeństwem informacji** - jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji
16) **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany, właściwość polegająca

na zapewnieniu dokładności i kompletności aktywów.

17) **Niezaprzeczalność** - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
18) **Ocena ryzyka** - proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka
19) **Postępowanie z ryzykiem** - proces wyboru i wdrażania środków modyfikujących ryzyko
20) **Poufność danych** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
21) **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.
22) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
23) **Ryzyko szczątkowe** - ryzyko pozostające po procesie postępowania z ryzykiem
24) **Sieć lokalna (intranet)** - połączenie jednostek komputerowych pracujących w Starostwie Powiatowym w Chodzieży w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,
25) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
26) **Szacowanie ryzyka** - całościowy proces analizy i oceny ryzyka
27) **SZBI** – system zarządzania bezpieczeństwem informacji - jest to część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI zawiera strukturę organizacyjną, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby,
28) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
29) **Użytkownik** - osoba upoważniona przez ADO do przetwarzania danych osobowych zarówno w systemach tradycyjnych „T" jak i w systemie informatycznym – elektronicznym „E" (pracownik, osoba wykonująca pracę na podstawie umowy cywilno-prawnej, osoba odbywająca staż pracy, praktykant),
30) **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
31) **Zarządzanie ryzykiem** - skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem ryzyka
32) **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
33) **Zdarzenie związane z bezpieczeństwem informacji** - jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki

bezpieczeństwa informacji

34) **Zgoda osoby, której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

6. Organizacja bezpieczeństwa informacji

Administrator Danych Osobowych odpowiada za:

1) Przeszkolenie instruktażowe pracowników w zakresie związanym z bezpieczeństwem informacji na stanowiskach pracy.
2) Przestrzeganie zasad bezpieczeństwa informacji przez nich samych jak i przez podległych im pracowników.
3) Identyfikowanie i dokumentowanie zagrożeń istotnych dla bezpieczeństwa informacji.
4) Przeprowadzanie audytów zgodności SZBI.
5) Zatwierdzenie warunków technicznych i organizacyjnych służących bezpieczeństwu informacji, w tym ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących regulacji prawnych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
6) Cele, zakres oraz metody przetwarzania i ochrony informacji, w tym danych osobowych.
7) Właściwą realizację praw osób, których dane przetwarza.
8) Realizację obowiązku informacyjnego.

Kompetencje i odpowiedzialność w obszarze zarządzania bezpieczeństwem informacji:

Obowiązki Administratora Danych:

1) Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów, merytorycznie poprawne i adekwatne w stosunku do celów.
2) Wyznacza osobę, odpowiedzialną za bezpieczeństwo danych osobowych.
3) Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4) Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego zestawu komputerowego.
5) Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6) Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych oraz uprawnionych do dostępu w poszczególnych systemach.

7) Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8) Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem danych, nielegalnym ujawnieniem danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.
9) Zobowiązuje pracowników, sporządzających projekty umów do zawierania w nich projektów umów powierzenia danych zgodnie z wymaganiami ochrony danych osobowych oraz bezpieczeństwa informacji w stopniu właściwym do zakresu umowy oraz ewidencjonowanie ich w stosownym rejestrze umów powierzenia danych.
10) Zgłasza Inspektora Ochrony Danych Osobowych w ewidencji prowadzonej przez PUODO.

Obowiązki Inspektora Ochrony Danych:

1) Informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

2) Monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia pracowników uczestniczących w operacjach przetwarzania oraz powiązane z tym 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;

5) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

6) Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Obowiązki Administratorów Systemów Informatycznych

1) Zarządzają bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa.
2) Doskonalą i rozwijają metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem.
3) Przydzielają identyfikatory (loginy) użytkownikom systemu informatycznego oraz zaznajamiają ich z procedurami ustalania i zmiany haseł dostępu.

4) Nadzorują prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu.
5) Zapewniają bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
6) Prowadzą nadzór nad archiwizacją zbiorów danych oraz zabezpieczają elektroniczne nośniki informacji zawierających dane osobowe.

Obowiązki Kierowników Komórek Organizacyjnych (KKO):

1) Zarządzają zasobem danych osobowych w ramach zadań realizowanych przez swoją komórkę.
2) Występują z wnioskiem do ADO o nadawanie upoważnień do przetwarzania danych osobowych podległym pracownikom.
3) Zgłaszają do ADO zamiar utworzenia procesu przetwarzania danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru.
4) Realizują proces udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą.
5) Wypełniają obowiązki dotyczące obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów.
6) Prowadzą ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w podległej komórce organizacyjnej, z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
7) Prowadzą w podległej komórce organizacyjnej nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny,
8) Dopilnowują, aby monitory stanowisk dostępu do danych osobowych w podległej komórce organizacyjnej były tak ustawione, aby uniemożliwić postronnym osobom wgląd w dane oraz dopilnowanie stosowania zasady „czystego monitora" na tych stanowiskach,
9) Zapoznają pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

Obowiązki użytkownika systemu informacji

1) Użytkownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą Dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji, regulaminami i instrukcjami wewnętrznymi.
2) Ochrona danych przed dostępem osób nieupoważnionych.
3) Ochrona danych przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją.

4) Ochrona nośników magnetycznych i optycznych oraz wydruków komputerowych przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem.
5) Utrzymywanie w tajemnicy powierzonych identyfikatorów, haseł, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia.
6) Archiwizowanie danych zgodnie z instrukcją.
7) Użytkownik obsługujący system informatyczny w obszarze przyznanego mu dostępu do systemu zobowiązany jest do sprawdzania czy nie wprowadzono nieautoryzowanych aplikacji oraz zmian w zainstalowanych aplikacjach.
8) Zabrania się pod rygorem odpowiedzialności służbowej i karnej ujawniania danych, kopiowania baz danych lub ich części poza przewidzianymi kopiami zapasowymi.
9) Zabrania się wykorzystywania sprzętu komputerowego i sieci komputerowej do celów prywatnych.
10) Zabrania się używania prywatnych komunikatorów.
11) Zabrania się ściągania i wysyłania plików (filmów, muzyki itp..).
12) Zabrania się korzystania z nośników nieznanego pochodzenia.
13) Zabrania się instalowania jakiegokolwiek oprogramowania bez wiedzy ASI.
14) Dopuszcza się wykorzystanie zarejestrowanych pamięci pendrive lub innych nośników do przenoszenia informacji wewnątrz siedziby jednostki, a także za zgodą i wcześniejszym sprawdzeniem nośnika przez ASI, poza siedzibę w ściśle określonym celu.
15) Użytkownik, który przewiduje, że w określonych dniach będzie nieobecny, lub w wypadku nagłej nieobecności, inna osoba (np. ASI, KKO itp.) jest zobowiązana do wykonania procedury zmierzającej do ustawienia w poczcie elektronicznej automatycznej odpowiedzi z informacją o nieobecności, a także przekierowaniu poczty do innej osoby. Natychmiast po powrocie z nieobecności należy przywrócić standardowe ustawienia.
16) W celu zachowania bezpieczeństwa wszelkie dane indywidualne i funkcyjne przechowywane są na dyskach lokalnych komputerów użytkowników, zaś kopie na dyskach sieciowych w lokalnej sieci komputerowej.
17) Zaleca się robienie kopii zapasowych ważnych plików i baz danych, jeśli nie są realizowane centralnie. Kopie należy wykonywać na udziałach sieciowych.
18) Użytkownik jest zobowiązany do zachowanie porządku na biurku w trakcie pracy oraz schowanie wszystkich dokumentów po jej zakończeniu.
19) Użytkownik jest zobowiązany do stosowania zasady „czystego pulpitu" polegającej na blokowaniu stacji poprzez wciśnięcie równocześnie klawisza „Windows" + „l".
20) Wszelkie niepotrzebne dokumenty/brudnopisy należy zniszczyć najpierw ręcznie, a następnie w niszczarce jeśli zawierają dane osobowe, pieczątki firmowe, podpisy itp.; zabrania się wyrzucania całych dokumentów do śmietnika.

7. Kontrola dostępu do informacji

Dostęp do informacji podlega ciągłej kontroli, która polega na:

1) Wydzielaniu obszarów przeznaczonych do przechowywania oraz przetwarzania zbiorów danych.
2) Zarządzaniu uprawnieniami poszczególnych użytkowników.
3) Nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji
4) Bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.
5) Wszystkie osoby posiadające dostęp do informacji podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa.

8. Zarządzanie aktywami i ryzykiem

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowego szacowania ryzyka i opracowanie planów postępowania z ryzykiem. Analiza uzyskanych wyników stanowi podstawę do podejmowania działań w zakresie doskonalenia ochrony aktywów.

Identyfikowanie ryzyk polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji.

Na szacowanie ryzyka składają się :

1) Analiza ryzyka (identyfikowanie, estymacja).
2) Ocena ryzyka.

W szacowaniu ryzyka określa się wartość aktywów informacyjnych, identyfikuje się mające zastosowanie zagrożenia oraz istniejące (lub mogące zaistnieć) podatności, identyfikuje się istniejące zabezpieczenia i ich wpływ na zidentyfikowane ryzyko, określa się możliwe następstwa oraz na końcu wskazuje się priorytety uzyskanych ryzyk i ustala ich kolejność zgodnie z kryteriami oceny ryzyka wyznaczonymi podczas ustanawiania kontekstu.

9. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

ADO zapewnia, że wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych, w tym systemów i aplikacji informatycznych własnych i/lub wykonawców, wykorzystywanych wewnętrznie w Starostwie Powiatowym w Chodzieży prowadzone jest w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa informacji.

Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych u ADO obejmuje:

1) uwzględnianie wymogów bezpieczeństwa podczas zakupu lub budowy nowych

systemów informatycznych,
2) dopuszczenie nowego systemu do eksploatacji poprzedzone jest zawsze fazą testów funkcjonalnych i testów bezpieczeństwa,
3) nadzorowanie dostępu do kodów źródłowych oprogramowania,
4) wdrożenie mechanizmów aktualizacji oprogramowania,
5) wdrożenie procedur kontroli zmian oprogramowania,

Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju i utrzymania systemów informatycznych ADO odpowiedzialny jest ASI.

10. Deklaracja ochrony własności intelektualnej

W Starostwie Powiatowym w Chodzieży zostały wdrożone mechanizmy zapobiegające naruszeniom prawa powszechnego związanego z ochroną własności intelektualnej. Stacje robocze zostały zabezpieczone przed możliwością instalowania oprogramowania z naruszeniem licencji.

Prowadzona jest bieżąca ewidencja sprzętu komputerowego i licencji oprogramowania.

Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie.

11. Bezpieczeństwo zasobów ludzkich

Starostwo Powiatowe w Chodzieży zatrudnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki wdrożonym zasadom rekrutacji pracowników.

Prowadzone są szkolenia dla pracowników oraz kontrahentów z zakresu wdrożonych zasad i procedur bezpieczeństwa informacji, które zakończone jest złożeniem oświadczenia o zachowaniu poufności podczas współpracy oraz po jej zakończeniu.

Do przetwarzania informacji dopuszczone są tylko osoby posiadające stosowne upoważnienie.

12. Bezpieczeństwo fizyczne i środowiskowe

Celem bezpieczeństwa fizycznego jest zapewnienie ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w siedzibie organizacji poprzez wprowadzenie technicznych zabezpieczeń.

13. Utrzymanie ciągłości działania

Zastosowanie odpowiednich środków organizacyjnych i technicznych umożliwi utrzymanie ciągłości działania, odtworzenie procesów oraz wznowienie działania systemów w sytuacji kryzysowej.

Na utrzymanie ciągłości działania składają się następujące zasady:

1) zastosowanie działań naprawczych,
2) ustalenie reguł współpracy z innymi podmiotami,
3) opracowanie planu awaryjnego,
4) ciągłe doskonalenie opracowanych procedur, planów oraz środków organizacyjnych i technicznych.

14. Naruszenie bezpieczeństwa informacji

W celu utrzymania wysokiego poziomu bezpieczeństwa informacji w Starostwie Powiatowym w Chodzieży podejmuje się odpowiednie działania wobec sytuacji, które są związane z jego naruszeniem.

Każdy przypadek naruszenia dostępności, poufności i integralności informacji w Starostwie Powiatowym w Chodzieży jest rejestrowany i poddawany odpowiedniej procedurze postępowania. W systemie zarządzania bezpieczeństwem informacji konieczne jest zaangażowanie wszystkich pracowników, w tym niezwłoczna interwencja na różne niepokojące sygnały i zdarzenia.

15. Podstawy prawne i organizacyjne

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (Dz. U. RPUE.L.2016.194.1),
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE.L.2016.119.1),
3. Norma PN-ISO/IEC 27005:2014-01 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji,
4. Norma PN-ISO/IEC 27001:2014-12 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji –Wymagania,
5. Norma PN-ISO/IEC 27002:2014-12 Technika informatyczna -- Techniki bezpieczeństwa - - Praktyczne zasady zabezpieczania informacji,

6. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r.

16. Postanowienia końcowe

W sprawach nieuregulowanych niniejszą PBI odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych Starostwa Powiatowego w Chodzieży.

Polityka Bezpieczeństwa Informacji w Starostwie Powiatowym w Chodzieży wchodzi w życie z dniem podpisania.

17. Dokumenty powiązane

1) Instrukcja Zarządzania Systemem Informatycznym.
2) Instrukcja Postępowania w Sytuacji Naruszeń.
3) Polityka Ochrony Danych Osobowych.
4) Analiza i szacowanie ryzyka w bezpieczeństwie informacji.
5) Wzory dokumentów.
6) Rejestry utrzymywane na podstawie niniejszej dokumentacji.

.....

(podpis Administratora Danych)

Polityka Ochrony Danych Osobowych
podczas przetwarzania dokumentacji
w postaci tradycyjnej oraz elektronicznej
w
Starostwie Powiatowym w Chodzieży
64-800 Chodzież, ul. Wiosny Ludów 1

Szczegóły dokumentu:

Sporządził:	*Beata Lewandowska* Administrator Bezpieczeństwa Informacji Audytor Wewnętrzny PN/ISO 27001
Data przekazania:	

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Warunki użytkowania dokumentacji bezpieczeństwa informacji

Dokumentacja opracowana przez ABI – Audyt, Consulting, Outsourcing Beata Lewandowska podlega ochronie przepisami prawa autorskiego; właścicielem wszystkich praw autorskich jest ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Po dokonaniu płatności, ABI – Audyt, Consulting, Outsourcing Beata Lewandowska udziela Starostwu Powiatowemu w Chodzieży niewyłącznego, stałego, ograniczonego prawa użytkowania dokumentacji, bez ograniczeń terytorialnych, wyłącznie w sposób określony w niniejszym dokumencie. Wszystkie prawa, których nie udzielono w niniejszym dokumencie, są zastrzeżone.

Starostwo Powiatowe w Chodzieży ma prawo wykorzystywać zakupioną dokumentację w dowolnym celu, związanym z działalnością organizacji, w dowolny sposób zgodny z udzielonymi prawami.

Starostwo Powiatowe w Chodzieży ma prawo kopiować dokumentację, w całości lub w części, czasowo lub trwale, w dowolnej formie i dowolnymi środkami.

Starostwo Powiatowe w Chodzieży ma prawo tłumaczyć dokumentację na inne języki, modyfikować ją i dowolnie edytować.

Bezwzględnie zabronione jest usuwanie oznaczeń właściciela praw autorskich oraz użytkowanie dokumentacji komercyjnie dla celów niezwiązanych z działalnością organizacji. W szczególności zabronione jest wynajmowanie lub dystrybucja oryginałów lub kopii dokumentacji poprzez sprzedaż lub w inny sposób przekazywanie jej z intencją sprzedaży, jak również drukowanie, publikowanie, publiczne udostępnianie poprzez systemy naziemne lub bezprzewodowe oraz poprzez udzielanie dostępu do dokumentacji nieautoryzowanym stronom trzecim w dowolny sposób (w tym dostępu przez internet), bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Zabroniony jest transfer praw do korzystania z dokumentacji na rzecz powiązanych lub niepowiązanych osób prawnych lub fizycznych, włącznie z przedsiębiorstwami zależnymi oraz udzielanie takich praw jakimkolwiek stronom trzecim bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

2. Preambuła

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich przetwarzania w Starostwie Powiatowym w Chodzieży.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym.

3. Podstawowe pojęcia i skróty.

Słownik podstawowych pojęć oraz skrótów występujących w niniejszej instrukcji znajduje się w dokumencie Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Chodzieży.

4. Modele architektury bezpiecznego przetwarzania dokumentacji osobowej w postaci elektronicznej

Modele architektury przetwarzania dokumentacji osobowej w postaci elektronicznej przez usługodawców.

1) **Model Klasyczny** - ADO posiada pełną kontrolę nad posiadaną infrastrukturą i oprogramowaniem. Jednak w wielu wypadkach jego samowystarczalność jest ograniczona koniecznością korzystania z usług dostawców łączy internetowych.
2) **Kolokacja** - ADO przekazuje firmie zewnętrznej serwery lub inne urządzenia teleinformatyczne do przeznaczonych do tego celu pomieszczeń (serwerowni). Podmiot zewnętrzny odpowiada również za zapewnienie odpowiedniego łącza.
3) **Hosting** - ADO dzierżawi od podmiotu zewnętrznego serwer lub część jego przestrzeni dyskowej.
4) **Chmura obliczeniowa typu IaaS** - infrastruktura informatyczna jest wynajmowana od podmiotu zewnętrznego. ADO zachowuje kontrolę nad danymi i oprogramowaniem.
5) **Chmura obliczeniowa typu PaaS** –podmiot zewnętrzny dostarcza środowisko, w którym ADO może instalować aplikacje i zarządzać nimi.
6) **Chmura obliczeniowa typu SaaS** – całość infrastruktury wraz z oprogramowaniem pozostają pod kontrolą podmiotu zewnętrznego, który odpowiada za ich bezawaryjne działanie.

ADO dokonuje analizy prawnej wykorzystania danego modelu z uwzględnieniem wszystkich indywidualnych okoliczności wdrożenia.

Decydując się na wybór określonego modelu przetwarzania danych ADO określa podział odpowiedzialności pomiędzy siebie a podmiot zewnętrzny, nad wykorzystywanymi zasobami IT zakresie zapewnienia bezpieczeństwa. Im więcej obowiązków zostanie powierzonych, tym mniejszą będzie miał ADO odpowiedzialność, ale jednocześnie mniejszą kontrolę.

5. Zasady przetwarzania danych

Art. 5 ust. 1 RODO wskazuje na sześć zasad przetwarzania danych osobowych:

1) **Zasada zgodności z prawem, rzetelności i przejrzystości przetwarzania** – wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem, rzetelne i przetwarzane w sposób zrozumiały dla osoby, której dane dotyczą. Jest to podstawowa zasada określająca relacje pomiędzy podmiotem danych i ich administratorem. Oznacza ona, że podmiot przetwarzający dane zawsze i na każdym etapie przetwarzania danych jest zobowiązany dbać o interesy osoby, której dane dotyczą. Musi spełniać co najmniej jeden z przewidzianych prawem warunków dopuszczalności przetwarzania danych (np. osoba, której dane dotyczą, wyrazi na to zgodę lub świadczeniem innych usług osobowych, zarządzania udzielaniem usług osobowych). Jednocześnie musi dołożyć staranności w zabezpieczeniu interesów osoby której przetwarzane dane dotyczą (zapewnić bezpieczeństwo danych między innymi poprzez ich pseudonimizację i szyfrowanie) oraz zagwarantować tej osobie kontrolę nad procesem przetwarzania (przekazywanie informacji do których ma prawo umożliwiających podejmowanie decyzji, między innymi: kto jest administratorem danych, w jakim celu i zakresie dane są zbierane i przetwarzane, jakie jest źródło danych, w jaki sposób są udostępniane itd.).
2) **Zasada ograniczoności celu** - dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami. Oznacza to, że administrator jest związany celem ustalonym na początku procesu przetwarzania i nie może go dowolnie zmieniać. Przepisy prawa zezwalają jednak wykorzystywać dane do celów archiwalnych i w interesie publicznym, do celów badań naukowych lub historycznych oraz do celów statystycznych, jednak pod warunkiem, że działania te są zgodne z ustalonymi w tym zakresie wymaganiami.
3) **Zasada minimalizacji danych** – przetwarzane dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Nie wolno zbierać i przetwarzać danych, które nie są niezbędne do osiągnięcia celu przetwarzania i są w stosunku do niego nadmiarowe.

4) **Zasada prawidłowości** – przetwarzane dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Obowiązkiem administratora jest dbałość o to, aby dane były prawidłowe i aktualizowane oraz zapewnienie, że dane które są nieprawidłowe względem celów przetwarzania zostaną niezwłocznie usunięte lub sprostowane.

5) **Zasada ograniczoności przechowywania** – dane osobowe muszą być 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia RODO w celu ochrony praw i wolności osób, których dane dotyczą.

6) **Zasada integralności i poufności** – dotyczy stosowania odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Między innymi chodzi o ochronę przed niedozwolonym przetwarzaniem lub przetwarzaniem niezgodnym z prawem, a także zabezpieczenie danych przed ich utratą, zniszczeniem lub uszkodzeniem.

6. Prawa osób których dane są przetwarzane

1) **Prawo do informacji i dostępu do danych** – Każda osoba fizyczna ma prawo dostępu do zebranych danych jej dotyczących oraz ma możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Dlatego też każda osoba, której dane dotyczą, ma prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania.

   Administrator zwraca szczególną uwagę aby system informatyczny, w którym dane będą przetwarzane zapewniał odnotowanie:

   a) daty pierwszego wprowadzenia danych do systemu;
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   d) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   e) sprzeciwu.

Odnotowanie informacji, o których mowa w pkt. a i b, musi następować automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system musi zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa powyżej.

W zakresie realizacji prawa do informacji i dostępu do danych, jego zakresu oraz sposobu zbierania i przechowywania, osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) cele przetwarzania;
b) kategorie odnośnych danych osobowych;
c) odbiorcy lub kategorie 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 – np. przepis prawa lub czas trwania kampanii marketingowej;
e) prawo do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
h) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, 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;
i) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Prawo do uzyskania kopii, o której mowa powyżej (art. 15 ust. 3 RODO), nie może niekorzystnie wpływać na prawa i wolności innych.

2) **Prawo do poprawienia danych** – prawo to zwane także prawem do sprostowania polega na tym, że osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego uzupełnienia dotyczących jej danych osobowych, które są niekompletne, uaktualnienia danych jeżeli są nieaktualne oraz sprostowania danych jeżeli są one nieprawdziwe, w tym poprzez przedstawienie dodatkowego oświadczenia.

Warunkiem skorzystania z prawa jest wykazanie przez zainteresowanego, że dane są niepełne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem prawa, bądź są już niepotrzebne do realizacji celu, dla którego były gromadzone.

Na podstawie art. 16 RODO osoba, której dane dotyczą może żądać od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Zgodnie z art. 19 RODO administrator jest zobowiązany do informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 lub art. 18 RODO każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

3) **Prawo do żądania usunięcia danych** – zwane także prawem do bycia zapomnianym.

Zgodnie z RODO osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania w przypadku jeżeli jej dane przetwarzane są na potrzeby marketingu bezpośredniego w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego tj. w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

Aby wzmocnić prawo do „bycia zapomnianym" w Internecie, rozszerzono prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o usunięciu wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji. Spełniając ten obowiązek administrator podejmuje racjonalne działania z uwzględnieniem

dostępnych mu technologii i środków, w tym dostępnych środków technicznych, w celu poinformowania administratorów, którzy przetwarzają dane osobowe, o żądaniu osoby, której dane dotyczą.

Przepisy art. 17 ust. 1 i 2 RODO nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c) z uwagi na względy interesu publicznego;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
e) do ustalenia, dochodzenia lub obrony roszczeń.

Administrator informuje o usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

4) **Prawo sprzeciwu** – osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych. By skorzystać z tego uprawnienia musi złożyć pisemne umotywowane żądanie zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. W tej sytuacji administrator jest zobowiązany do zaprzestania przetwarzania, chyba że wykaże istnienie ważnych i prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych nad interesami osoby, której dotyczą. W przypadku danych przetwarzanych w celach marketingowych lub kiedy osoba, której dane dotyczą, chce je przekazać innemu administratorowi, powołanie się na szczególną sytuację nie jest konieczne i w tej sytuacji sprzeciw ma charakter bezwzględny i oznacza, że administrator nie ma prawa podważania sprzeciwu. Osoba, której dane dotyczą nie może skorzystać z prawa sprzeciwu gdy administrator przetwarza dane na podstawie przepisów prawa lub gdy jest to konieczne dla realizacji umowy, której podmiot danych jest stroną.

Zgodnie z art. 21 RODO osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO tj. wtedy gdy: przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, przetwarzanie jest niezbędne do celów wynikających z prawnie

uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, osoba, której dane dotyczą, ma prawo wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

5) **Prawa związane z podejmowaniem zautomatyzowanych decyzji** – Są to przypadki, w których decyzja opiera się wyłącznie na operacjach na danych osobowych, wykonywanych automatycznie przez system informatyczny tj. bez udziału czynnika ludzkiego. Do takiego przetwarzania zalicza się „profilowanie" – które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno

dotyczyć dzieci.

W przypadku kiedy jednak podjęto zautomatyzowane decyzje zgodnie z obowiązującymi przepisami prawa, osoba w sprawie której decyzje podjęto ma szczególne prawo pozwalające jej na kontrolowanie omawianego procesu:

Prawo do uzyskania informacji o przesłankach podjęcia rozstrzygnięcia.

Prawo do żądania ponownego, indywidualnego rozpatrzenia sprawy.

6) **Prawo do przenoszenia danych** – zgodnie z art. 20 RODO – jeżeli przetwarzanie danych: odbywa się na podstawie zgody osoby, której dane dotyczą lub umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany, osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą może zażądać od administratora danych by jego dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Z tego prawa można skorzystać jedynie wtedy kiedy dane mają postać elektroniczną i tylko wtedy, kiedy administrator przetwarza te dane na podstawie zgody podmiotu danych lub na podstawie zawartej z tym podmiotem umowy.

Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku dla prawa do usunięcia danych. Prawo do przenoszenia danych nie powinno w szczególności skutkować usunięciem danych osoby, dane dotyczą, a które osoba ta dostarczyła do wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy.

7. Monitorowanie przestrzegania zgodności przetwarzania danych

Monitorowanie przestrzegania zgodności przetwarzania danych z przepisami o ochronie danych osobowych wiąże się z przeprowadzaniem audytów ochrony danych osobowych. Przepisy RODO jedynie nakreślają ogólny zakres działań, które ADO musi podjąć, aby zapewnić bezpieczeństwo przetwarzania danych. Zgodnie z ogólną zasadą podejścia opartego na ryzyku, podmiot przetwarzający dane osobowe jest zobowiązany wdrożyć odpowiednie zabezpieczenia zarówno w warstwie systemowej, organizacyjnej i technicznej, które zapewnią należytą ochronę danych osobowych.

Ocena skutków ochrony danych osobowych – analiza oparta na ryzyku

Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności gdy:

a) przetwarzanie może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia;
b) naruszeniem poufności danych osobowych chronionych tajemnicą zawodową,
c) nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną;
d) osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
e) przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa;
f) oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;
g) przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Niezbędne elementy oceny skutków określa przepis art. 35 ust. 7 RODO.

Ocena skutków przetwarzania obligatoryjnie zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

8. Zagrożenia i odpowiedzialność wynikająca z przetwarzania dokumentacji osobowej

Zagrożenia występujące podczas przetwarzania dokumentacji osobowej

Naruszenie podstawowych atrybutów bezpieczeństwa przetwarzania informacji tj. naruszenie poufności, integralności i dostępności danych osobowych obejmuje poniższe zagrożenia:

1) Nieuprawniony dostęp przez użytkowników polegający na zaistnieniu sytuacji, w której użytkownicy korzystają z kont do których sami nie mają uprawnień, albo korzystania przez wielu użytkowników z tego samego loginu użytkownika i hasła.
2) „Pragmatyzm zwyczajowy" stanowi naruszenie zasad bezpiecznego uwierzytelniania użytkownika. Przykładem takiego zwyczaju mogą być sytuacje w których jeden pracownik medyczny może zastąpić innego na stanowisku pracy i kontynuuje prace na już zalogowanym koncie poprzednika co skutkuje brakiem potrzeby przelogowania. Pierwsze logowanie użytkownika pozwala na pracę w systemie i jednocześnie bez uprzedniego wylogowania pozwala na pracę przez innych użytkowników na koncie bieżącego użytkownika. Powyższy przykład zachowania powoduje poważne naruszenia poufności i niezaprzeczalności.
3) Nieuprawniony dostęp przez użytkowników (w tym usługodawcy uprawnieni na podstawie umów – personel obsługi technicznej – administratorzy oprogramowania i sprzętu, którzy mogą mieć uzasadniony powód dostępu do systemów i danych) posiadających uprzywilejowany dostęp do systemów i urządzeń polegający na uzyskaniu nieautoryzowanego dostępu do danych. Działanie takie jest naruszeniem bezpiecznych rozwiązań wynikających z umów outsourcingowych. Nieuprawniony dostęp przez usługodawców może być także źródłem poważnych naruszeń poufności informacji w tym danych osobowych.
4) Nieuprawniony dostęp przez osoby z zewnątrz organizacji - zaistnieje w sytuacji, w której nieuprawnione osoby trzecie (hakerzy) posiadają dostęp do danych lub zasobów systemowych, albo poprzez podszywanie się jako autoryzowany użytkownik stanie się upoważnionym użytkownikiem (na przykład przez tak zwany atak wykorzystujący metody socjotechniczne).
5) Przypadek nieuprawnionego dostępu przez użytkowników z zewnątrz może świadczyć o pominięciu kontroli bezpieczeństwa w zakresie:
   a) identyfikacji użytkownika;
   b) uwierzytelniania użytkownika;
   c) identyfikacji użytkownika z uwierzytelnieniem zaufanego sprzętu;
   d) uwierzytelniania pochodzenia;
   e) kontroli dostępu i zarządzania uprawnieniami.
6) Osadzanie złośliwego kodu. Zagrożenie to obejmuje wirusy przesyłane w wiadomościach e-mail i wykorzystanie złośliwego kodu mobilnego. Zwiększenie wykorzystania technologii bezprzewodowych i komórkowych przez pracowników zwiększa potencjał tego zagrożenia. Osadzanie złośliwego kodu stanowi brak skutecznego stosowania kontroli oprogramowania antywirusowego lub kontroli zapobiegania włamaniom.
7) Przekierowanie połączenia. Zagrożenie to obejmuje możliwość, że informacje przesyłane przez sieć informatyczną mogą być dostarczone do niewłaściwego adresata. Przypadkowe przekierowanie połączenia może stanowić uchybienie w działaniu systemu lub niemożność utrzymania integralności informacji przetwarzanych w dokumentacji osobowej.

8) Awaria techniczna systemu lub infrastruktury sieciowej. Zagrożenia te obejmują awarie sprzętu, awarie sieci lub braki w bazach danych. Takie problemy zwykle stanowią o awarii jednego lub większej liczby elementów powodując jego ograniczone działanie lub niedostępność.
9) Awaria środowiska wsparcia, w tym awarie zasilania i zakłócenia wynikające z oddziaływania fizycznego lub katastrof spowodowanych przez człowieka. Te same katastrofy mogą jednak spowodować duże zniszczenia w systemach wsparcia środowisk niezbędnych do utrzymania działalności.
10) Awaria systemu lub oprogramowania sieciowego. Ataki DoS są znacznie ułatwione dzięki słabościom lub błędom systemu operacyjnego lub oprogramowaniu sieciowemu. Awaria systemu lub sieci może być spowodowana awarią oprogramowania do sprawdzania integralności i testowania systemu kontroli lub konserwacji oprogramowania.
11) Błędne operacje. Błędy operatora odpowiadają za niewielki, ale znaczący procent niezamierzonych ujawnień poufnych informacji. Błędy operatora stanowią o braku jednego lub więcej czynników takich jak:
    a) kontrola operacji;
    b) bezpieczeństwo personelu (w tym brak skutecznego szkolenia).

Odpowiedzialność

Najważniejszym i jednocześnie najbardziej dotkliwym rodzajem sankcji przewidzianych w RODO są administracyjne kary pieniężne, o których mowa w art. 83 rozporządzenia.

1) Katalog naruszeń, które będą dawały podstawę do nałożenia administracyjnej kary pieniężnej w kwocie do 10 mln euro lub - gdy kara nakładana jest na przedsiębiorstwo - do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego zostały wskazane w art. 83 ust. 4 RODO.
   Należą do nich między innymi:
   a) niestosowanie mechanizmów uwzględniania ochrony danych w fazie projektowania (tzw. privacy by design) oraz domyślnej ochrony danych (tzw. privacy by default), o których mowa w art. 25 RODO,
   b) naruszenie zasad współpracy pomiędzy współadministratorami danych, o których mowa w art. 26 RODO,
   c) naruszenie obowiązków w zakresie powierzania do przetwarzania danych osobowych (w tym obowiązek korzystania przez administratorów danych wyłącznie z usług takich podmiotów przetwarzających, które spełniają wymagania RODO, czy też wymagania odnośnie formy i zakresu umowy, na podstawie której dochodzi do powierzenia przetwarzania danych),
   d) naruszenie obowiązku prowadzenia rejestru czynności przetwarzania danych, o którym mowa w art. 30 RODO,
   e) niestosowanie odpowiednich środków bezpieczeństwa zapewniających wymagany poziom ochrony danych osobowych (zgodnie z przeprowadzaną analizą ryzyka) - art. 32 RODO,
   f) niezgłaszanie faktu naruszenia ochrony danych osobowych do organu kontrolnego

oraz nieprzekazanie informacji o tym fakcie osobom, których te dane dotyczą (art. 33 i 34 RODO),

g) niestosowanie się do obowiązku przeprowadzania oceny skutków dla ochrony danych w sytuacjach gdy jest to wymagane (art. 35 RODO),
h) niewyznaczenie inspektora ochrony danych w przypadkach gdy to wyznaczenie jest obligatoryjne (art. 37 RODO) i wiele innych.

2) Katalog naruszeń, które będą dawały podstawę do nałożenia kary pieniężnej w kwocie do 20 mln euro lub – gdy kara nakładana jest na przedsiębiorstwo – do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego zostały wskazane w art. 83 ust. 5 RODO.

Należą do nich między innymi:

a) niestosowanie się do podstawowych zasad przetwarzania danych, o których mowa w art. 5, 6 , 7 oraz 9 RODO (chodzi między innymi o znane z polskiej ustawy o ochronie danych osobowych, aczkolwiek zmodyfikowane na gruncie RODO zasady legalności i celowości przetwarzania danych, wymagania prawne wobec zgody jako podstawy prawnej przetwarzania danych, czy też warunki przetwarzania danych sensytywnych),
b) naruszenie praw osób, których dane dotyczą, określonych w art. 12-22 RODO (m.in. wymagania wobec obowiązków informacyjnych jakie należy spełniać wobec tych osób, uprawnienia tych osób do dostępu, żądania sprostowania oraz w określonych w RODO)
c) przypadkach żądania usunięcia ich danych, czy też prawo do przenoszenia danych pomiędzy różnymi administratorami danych),
d) naruszenie wymagań prawnych związanych z transferem danych osobowych do tzw. państw trzecich, o których mowa w art. 44-49 RODO.

9. Zalecenia dotyczące bezpiecznego przetwarzania dokumentacji osobowej

Prowadzenie dokumentacji osobowej w Starostwie Powiatowym w Chodzieży wymaga spełnienia poniższych wymagań:

a) zabezpieczenie dokumentacji przed uszkodzeniem lub utratą;
b) integralność treści dokumentacji i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach ustalonych i udokumentowanych procedur;
c) stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;
d) identyfikacja osoby dokonującej wpisu oraz osoby udzielającej świadczeń i dokumentowanie dokonywanych przez te osoby zmian w dokumentacji i metadanych;
e) przyporządkowanie cech informacyjnych dla odpowiednich rodzajów dokumentacji,
f) udostępnienie, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu,

w formacie, w którym jest ona przetwarzana (XML albo PDF);
g) funkcjonalność wydruku dokumentacji.

Dokumentacja prowadzona w postaci elektronicznej jest właściwie zabezpieczona, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

a) jest zapewniona jej dostępność wyłącznie dla osób uprawnionych,
b) jest chroniona przed przypadkowym lub nieuprawnionym zniszczeniem,
c) wprowadzono metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

Zabezpieczenie dokumentacji w postaci elektronicznej wymaga w szczególności:

a) systematycznego dokonywania analizy zagrożeń,
b) opracowania i stosowania procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania,
c) stosowania środków bezpieczeństwa adekwatnych do zagrożeń,
d) bieżącego kontrolowania funkcjonowania wszystkich organizacyjnych i techniczno-informatycznych sposobów zabezpieczania, a także okresowego dokonywania oceny skuteczności tych sposobów,
e) przygotowania i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na nowe informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

10. Zasady ewidencjonowania procesów przetwarzania danych osobowych

1) KKO zgłasza ADO zamiar rozpoczęcia nowego procesu przetwarzania danych osobowych.
2) KKO wraz z ADO określają wymagane parametry procesu, tj. cel, zakres danych, podstawę prawną, okres przetwarzania, odbiorców, przekazywanie do państw trzecich.
3) Dla każdego nowego, planowanego procesu przeprowadzane jest szacowanie ryzyka wraz z oceną skutków, w razie potrzeb. ADO określa minimalne wymagania zabezpieczeń dla ochrony danych w nowym procesie na podstawie tego szacowania. Ponadto na etapie planowania uwzględnia się realizacje wszystkich wymagań mających zastosowanie do nowego procesu, m.in. realizowanie obowiązku informacyjnego.
4) ADO wpisuje nowy proces w Rejestr Czynności Przetwarzania.

11. Zasady udostępniania danych osobowych

1) Dane osobowe w Starostwie Powiatowym w Chodzieży mogą być udostępniane na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie odrębnych przepisów, na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępniania danych oraz na podstawie wniosku osoby uprawnionej, której dane dotyczą.

2) Dane osobowe w Starostwie Powiatowym w Chodzieży udostępnia się na pisemny, umotywowany wniosek, chyba, że inny przepis stanowi inaczej.
3) Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać tylko zgodnie z przeznaczeniem.
4) Wniosek o udostępnienia danych przekazywany jest do KKO, w którym wnioskowane dane są przetwarzane. KKO podejmuje decyzje o udostępnieniu i odnotowuje fakt w rejestrze udostępnionych danych.
5) KKO odpowiedzialny jest za przygotowanie danych osobowych zgodnie z obowiązującą podstawą prawną do udostępnienia w zakresie wskazanym we wniosku.
6) Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom listem poleconym za potwierdzeniem odbioru lub za pośrednictwem skrzynki elektronicznej E-PUAP.

12. Zasady powierzania danych osobowych

1) Powierzenie przetwarzania danych osobowych w Starostwie Powiatowym w Chodzieży odbywa się zgodnie z art. 28 ust. 3 Rozporządzenia. Na podstawie umowy zawartej na piśmie pomiędzy ADO, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
2) Decyzję powierzenia danych osobowych podejmuje KKO, który będzie zlecać podmiotom zewnętrznym czynności związane z przetwarzaniem danych osobowych.
3) KKO odpowiedzialny jest za informowanie ADO o zamiarze powierzenia danych osobowych do przetwarzania.
4) Projekt umowy parafują KKO przygotowujący umowy i/lub Radca Prawny.
5) Zaparafowany projekt umowy jest przedkładany do akceptacji i podpisu ADO.
6) Umowa powierzenia jest wymagana w każdym przypadku, kiedy następuje przekazanie danych osobowych lub ich gromadzenie przez podmiot zewnętrzny.
7) W przypadkach, kiedy pracownik podmiotu zewnętrznego uzyskuje dostęp do danych osobowych, jednak przetwarzanie odbywa się w obszarze ADO wystarczające jest zastosowanie upoważnienia.
8) Zawarta umowa musi zawierać poniższe elementy:
   a) cel przetwarzania, z zastrzeżeniem zakazu wykorzystania danych w innym celu,
   b) zakres, kategorie oraz charakter powierzanych danych,
   c) odpowiedzialność stron, w tym za przestrzeganie postanowień umownych oraz przestrzeganie obowiązujących przepisów prawa – zwłaszcza w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych zabezpieczających dane osobowe,
   d) konieczność upoważniania przez Podmiot, osób przetwarzających w imieniu Podmiotu oraz zobowiązanie ich do zachowania poufności,
   e) zakaz korzystania z innych podmiotów - podwykonawców - bez pisemnej zgody lub aneksu do umowy,
   f) konieczność uczestniczenia Podmiotu w wypełnianiu obowiązków ciążących na ADO, w tym realizacji praw osób, których dane dotyczą oraz przekazywania informacji

o sposobach przetwarzania oraz informacji potrzebnych do szacowania ryzyka i oceny skutków naruszeń,

g) zgłaszanie wszelkich incydentów lub podejrzeń incydentów, z zapewnieniem wszystkich niezbędnych informacji do poprawnej realizacji zgłaszania incydentów zgodnie z przepisami prawa,
h) sposób potwierdzania przestrzegania przepisów prawa i zasad bezpieczeństwa – tj. umożliwienie monitorowania, audytowania Podmiotu,
i) konieczność usunięcia lub zwrócenia powierzonych danych osobowych w przypadku wygaśnięcia umowy lub jej rozwiązania.

9) Każdy Podmiot przetwarzający oraz ewentualnie podwykonawcy zostają wpisani do rejestru umów powierzenia danych.

13. Środki organizacyjne ochrony danych osobowych

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych w Starostwie Powiatowym w Chodzieży, Administrator Danych Osobowych wprowadza określone poniżej środki organizacyjne.

1) Przetwarzanie danych osobowych może odbywać się wyłącznie ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
2) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
3) Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.
4) Zabrania się przetwarzania danych poza wyznaczonym obszarem.
5) Pracownik Starostwa Powiatowego w Chodzieży upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Podpisany dokument wraz z upoważnieniem do przetwarzania danych jest dołączany do akt osobowych.
6) Obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
7) Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora Danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
8) Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
9) Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna, usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
10) Nie należy gromadzić w podręcznej dokumentacji danych osobowych. Wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach.
11) Dokumenty zawierające dane osobowe należy niszczyć w niszczarkach.

12) Każdorazowe zbieranie danych rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
13) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
14) Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza siedzibę placówki lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
15) Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
16) Komputery, które przetwarzają zbiory osobowe, za wyjątkiem komputerów służących jedynie do edycji tekstu, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
17) Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Instrukcji Zarządzania Systemem Informatycznym będącej częścią niniejszej dokumentacji.

14. Środki techniczne ochrony danych osobowych

Potencjalne środki ochrony technicznej danych osobowych w Starostwie Powiatowym w Chodzieży:

1) Ogólna ochrona budynku – gaśnice, systemy p-poż., system alarmowy, monitoring.
2) Zabezpieczenie drzwi –drzwi tradycyjne zamykane na klucz. Dostęp do kluczy posiadają upoważnione osoby.
3) Zabezpieczenia zbiorów tradycyjnych (papierowych) – szafy tradycyjne zamykane na klucz, szafy metalowe lub sejfy (dla danych szczególnie ważnych).
4) Dane przeznaczone do zniszczenia niszczone są w specjalistycznych niszczarkach.
5) Zabezpieczenia zbiorów elektronicznych – w systemy antywirusowe.

15. Podstawy prawne

Podstawy prawne niniejszej PODO znajdują się w dokumencie Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Chodzieży.

16. Postanowienia końcowe

W sprawach nieuregulowanych niniejszą PODO odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych Starostwa Powiatowego w Chodzieży.

Polityka Ochrony Danych Osobowych w Starostwie Powiatowym w Chodzieży wchodzi w życie z dniem podpisania.

17. Dokumenty powiązane

1) Polityka Bezpieczeństwa Informacji
2) Instrukcja Postępowania w Sytuacji Naruszeń
3) Instrukcja Zarządzania Systemem Informatycznym.
4) Analiza i szacowanie ryzyka w bezpieczeństwie informacji.
5) Wzory dokumentów.
6) Rejestry utrzymywane na podstawie niniejszej dokumentacji.

.....

(podpis Administratora Danych)

Instrukcja Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Starostwie Powiatowym w Chodzieży 64-800 Chodzież, ul. Wiosny Ludów 1

Szczegóły dokumentu:

Sporządził:	*Beata Lewandowska* Administrator Bezpieczeństwa Informacji Audytor Wewnętrzny PN/ISO 27001
Data przekazania:	

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Warunki użytkowania dokumentacji bezpieczeństwa informacji

Dokumentacja opracowana przez ABI – Audyt, Consulting, Outsourcing Beata Lewandowska podlega ochronie przepisami prawa autorskiego; właścicielem wszystkich praw autorskich jest ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Po dokonaniu płatności, ABI – Audyt, Consulting, Outsourcing Beata Lewandowska udziela Starostwu Powiatowemu w Chodzieży niewyłącznego, stałego, ograniczonego prawa użytkowania dokumentacji, bez ograniczeń terytorialnych, wyłącznie w sposób określony w niniejszym dokumencie. Wszystkie prawa, których nie udzielono w niniejszym dokumencie, są zastrzeżone.

Starostwo Powiatowe w Chodzieży ma prawo wykorzystywać zakupioną dokumentację w dowolnym celu, związanym z działalnością organizacji, w dowolny sposób zgodny z udzielonymi prawami.

Starostwo Powiatowe w Chodzieży ma prawo kopiować dokumentację, w całości lub w części, czasowo lub trwale, w dowolnej formie i dowolnymi środkami.

Starostwo Powiatowe w Chodzieży ma prawo tłumaczyć dokumentację na inne języki, modyfikować ją i dowolnie edytować.

Bezwzględnie zabronione jest usuwanie oznaczeń właściciela praw autorskich oraz użytkowanie dokumentacji komercyjnie dla celów niezwiązanych z działalnością organizacji. W szczególności zabronione jest wynajmowanie lub dystrybucja oryginałów lub kopii dokumentacji poprzez sprzedaż lub w inny sposób przekazywanie jej z intencją sprzedaży, jak również drukowanie, publikowanie, publiczne udostępnianie poprzez systemy naziemne lub bezprzewodowe oraz poprzez udzielanie dostępu do dokumentacji nieautoryzowanym stronom trzecim w dowolny sposób (w tym dostępu przez internet), bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Zabroniony jest transfer praw do korzystania z dokumentacji na rzecz powiązanych lub niepowiązanych osób prawnych lub fizycznych, włącznie z przedsiębiorstwami zależnymi oraz udzielanie takich praw jakimkolwiek stronom trzecim bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

2. Istota naruszenia bezpieczeństwa informacji

Zagrożenia losowe zewnętrzne w szczególności klęski żywiołowe, przerwy w zasilaniu - ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.

Zagrożenia losowe wewnętrzne w szczególności niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

Zagrożenia zamierzone, świadome i celowe najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
b) nieuprawniony dostęp do systemu z jego wnętrza,
c) nieuprawniony przekaz danych,
d) pogorszenie jakości sprzętu i oprogramowania,
e) bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.,
b) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu,
c) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
d) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
e) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
f) stwierdzenie próby lub modyfikacji danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
g) wystąpienie niedopuszczalnej manipulacji danymi osobowymi w systemie,
h) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,

i) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
j) ujawnienie, istnienie nieautoryzowanych kont dostępu do danych,
k) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub skopiowanie danych osobowych,
l) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych w Starostwie Powiatowym w Chodzieży uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), zdjęciach, płytach w formie niezabezpieczonej itp.

3. Podstawowe pojęcia i skróty

Słownik podstawowych pojęć oraz skrótów występujących w niniejszej instrukcji znajduje się w dokumencie Polityki Bezpieczeństwa Informacji.

4. Postępowanie w przypadku naruszenia bezpieczeństwa informacji

Każdy pracownik Starostwa Powiatowego w Chodzieży biorący udział w przetwarzaniu danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) jest odpowiedzialny za bezpieczeństwo tych danych.

Każda osoba zatrudniona w Starostwie Powiatowym w Chodzieży, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, **zobowiązana jest do natychmiastowego poinformowania Administratora Danych.**

Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych w Starostwie Powiatowym w Chodzieży powinna być przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.

W przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż Administrator Danych, jest ona obowiązana poinformować o tym fakcie Administratora Danych.

Każdy pracownik Starostwa Powiatowego w Chodzieży, który stwierdzi fakt naruszenia bezpieczeństwa ma obowiązek:

a) podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość
b) zaniechać wszelkich działań mogących uniemożliwić analizę wystąpienia naruszenia i udokumentowanie zdarzenia.
c) zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie,
d) wstrzymać pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
e) podjąć stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
f) powinien wstępnie udokumentować zaistniałe naruszenie

Administrator Danych niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:

a) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa Powiatowego w Chodzieży,
b) zapisać wszelkie informacje związane z danym zdarzeniem,
c) nawiązać kontakt ze specjalistami jeżeli zachodzi taka potrzeba,
d) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
e) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
f) poinformować o naruszeniu bezpieczeństwa danych osobowych Organ Nadzorczy oraz osoby, których dane są przetwarzane, a bezpieczeństwo zostało naruszone, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Administrator Systemu Informatycznego Starostwa Powiatowego w Chodzieży powinien podjąć następujące działania zmierzające do wyjaśnienia zgłoszonego zdarzenia w systemie informatycznym:

a) wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,

b) przeprowadzić wywiady z pracownikami Starostwa Powiatowego w Chodzieży w celu ustalenia zaistniałych faktów,
c) przeprowadzić analizę poprawności funkcjonowania systemu informatycznego w Starostwie Powiatowym w Chodzieży, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem,
d) przeprowadzić analizę zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników,
e) przeprowadzić analizę danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych,
f) zabezpieczyć dane przetwarzane w systemie informatycznym dotkniętym incydentem, w szczególności dane konfiguracyjne tego systemu,
g) zabezpieczyć system informatyczny przed dalszym rozprzestrzenianiem się zagrożenia,
h) zebrać materiały pozwalające na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.
i) zasięgnąć potrzebnych opinii i zaproponować działania naprawcze (w tym także ustosunkować się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) oraz wznowienia terminu przetwarzania.

System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.

Okres kwarantanny, o którym mowa w ust. 1, jest uzależniony od charakteru incydentu i specyfiki systemu informatycznego jest on każdorazowo określany przez Administratora Systemu.

5. Sankcje karne

Wobec osoby, która w przypadku naruszenia bezpieczeństwa informacji nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z innymi regulacjami prawnymi.

6. Podstawy prawne

Podstawy prawne niniejszej IPSN znajdują się w dokumencie Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Chodzieży.

7. Postanowienia końcowe

W sprawach nieuregulowanych niniejszą IPSN odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych Starostwa Powiatowego w Chodzieży.

Instrukcja Postępowania w Sytuacji Naruszeń w Starostwie Powiatowym w Chodzieży wchodzi w życie z dniem podpisania.

8. Dokumenty powiązane

1) Polityka Bezpieczeństwa Informacji.
2) Polityka Ochrony Danych Osobowych.
3) Instrukcja Zarządzania Systemem Informatycznym.
4) Analiza i szacowanie ryzyka w bezpieczeństwie informacji.
5) Wzory dokumentów.
6) Rejestry utrzymywane na podstawie niniejszej dokumentacji.

.....

(podpis Administratora Danych)

Instrukcja Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Starostwie Powiatowym w Chodzieży 64-800 Chodzież, ul. Wiosny Ludów 1

Szczegóły dokumentu:

Sporządził:	*Beata Lewandowska* Administrator Bezpieczeństwa Informacji Audytor Wewnętrzny PN/ISO 27001
Data przekazania:	

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Warunki użytkowania dokumentacji bezpieczeństwa informacji

Dokumentacja opracowana przez ABI – Audyt, Consulting, Outsourcing Beata Lewandowska podlega ochronie przepisami prawa autorskiego; właścicielem wszystkich praw autorskich jest ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Po dokonaniu płatności, ABI – Audyt, Consulting, Outsourcing Beata Lewandowska udziela Starostwu Powiatowemu w Chodzieży niewyłącznego, stałego, ograniczonego prawa użytkowania dokumentacji, bez ograniczeń terytorialnych, wyłącznie w sposób określony w niniejszym dokumencie. Wszystkie prawa, których nie udzielono w niniejszym dokumencie, są zastrzeżone.

Starostwo Powiatowe w Chodzieży ma prawo wykorzystywać zakupioną dokumentację w dowolnym celu, związanym z działalnością organizacji, w dowolny sposób zgodny z udzielonymi prawami.

Starostwo Powiatowe w Chodzieży ma prawo kopiować dokumentację, w całości lub w części, czasowo lub trwale, w dowolnej formie i dowolnymi środkami.

Starostwo Powiatowe w Chodzieży ma prawo tłumaczyć dokumentację na inne języki, modyfikować ją i dowolnie edytować.

Bezwzględnie zabronione jest usuwanie oznaczeń właściciela praw autorskich oraz użytkowanie dokumentacji komercyjnie dla celów niezwiązanych z działalnością organizacji. W szczególności zabronione jest wynajmowanie lub dystrybucja oryginałów lub kopii dokumentacji poprzez sprzedaż lub w inny sposób przekazywanie jej z intencją sprzedaży, jak również drukowanie, publikowanie, publiczne udostępnianie poprzez systemy naziemne lub bezprzewodowe oraz poprzez udzielanie dostępu do dokumentacji nieautoryzowanym stronom trzecim w dowolny sposób (w tym dostępu przez internet), bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Zabroniony jest transfer praw do korzystania z dokumentacji na rzecz powiązanych lub niepowiązanych osób prawnych lub fizycznych, włącznie z przedsiębiorstwami zależnymi oraz udzielanie takich praw jakimkolwiek stronom trzecim bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

2. Charakterystyka systemu

Sieć informatyczną, w której przetwarzane są dane osobowe stanowią wszystkie pracujące w Starostwie Powiatowym w Chodzieży obecne i przyszłe, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.

Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.

System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie.

3. Podstawowe pojęcia i skróty.

Słownik podstawowych pojęć oraz skrótów występujących w niniejszej instrukcji znajduje się w dokumencie Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Chodzieży.

4. Ogólne zasady pracy w systemie.

ADO odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.

Przetwarzanie danych w systemie informatycznym Starostwa Powiatowego w Chodzieży może być realizowane wyłącznie poprzez dopuszczone przez ADO do eksploatacji licencjonowane oprogramowanie.

Administrator Systemu Informatycznego Starostwa Powiatowego w Chodzieży prowadzi ewidencję oprogramowania.

Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

a) mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika z pominięciem narzędzi do edycji tekstu,
b) mechanizmy ochrony poufności, dostępności i integralności informacji z uwzględnieniem potrzeby ochrony kryptograficznej,
c) mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
d) urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
e) mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
f) mechanizmy zarządzania zmianami.

Użytkownikom zabrania się:

a) korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez zgody przełożonego,
b) udostępniania stanowisk roboczych osobom nieuprawnionym,
c) samowolnego instalowania i używania programów komputerowych,
d) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
e) umożliwiania dostępu do zasobów sieci Internetowej osobom nieuprawnionym,
f) używania komputera bez zainstalowanego oprogramowania antywirusowego.

5. Procedury nadawania uprawnień

Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych w Starostwie Powiatowym w Chodzieży wymagane jest upoważnienie.

Upoważnienie nadaje ADO na podstawie wniosku o nadanie uprawnień do systemów sporządzonego przez KKO przy współpracy z ASI.

Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:

a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
b) zawieszenia w pełnieniu obowiązków służbowych.

Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

6. Metody i środki uwierzytelnienia

System informatyczny Starostwa Powiatowego w Chodzieży przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną małą i wielką literę, jedną cyfrę lub jeden znak specjalny.

Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały, itp.) i nie może być sekwencją kolejnych znaków klawiatury.

W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu Administratorowi Systemu Informatycznego do natychmiastowej zmiany hasła.

Hasło nie może być zapisywane i przechowywane.

Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

Stacja lokalna ma skonfigurowany profil administratora oraz użytkownika. Konto użytkownika posiada ograniczone prawa w zakresie instalowania i usuwania oprogramowania.

7. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

Każdy użytkownik systemu Starostwa Powiatowego w Chodzieży korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.

Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.

Zakończenie pracy w systemie następuje poprzez prawidłowe, wymagane przez daną aplikację oraz system operacyjny, wykonanie czynności kończących. Niedopuszczalne jest zakończenie pracy poprzez wyłączenie napięcia zasilającego bez pełnej procedury zamknięcia.

Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.

Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.

8. Procedury korzystania ze sprzętu przenośnego

Pracownicy Starostwa Powiatowego w Chodzieży, którym powierzono sprzęt mobilny są upoważnieni do wynoszenia go poza obszar przetwarzania, jeśli jest to uzasadnione wykonywanymi obowiązkami. W innych przypadkach lub kiedy wynoszenie ma charakter sporadyczny należy poinformować o tym fakcie przełożonego.

Urządzenia mobilne są wyposażone w mechanizmy szyfrujące, jeśli występuje na nich przetwarzanie danych osobowych. Szyfrowanie dysków jest realizowane przez funkcje

systemu operacyjnego, dedykowane rozwiązania producenta sprzętu lub zewnętrzne programy.

W zależności od wykorzystywanego rozwiązania, użytkownik urządzenia przenośnego może być zobowiązany do wykonania dwustopniowego logowania. W przypadku logowania dwustopniowego, oba hasła muszą spełniać wymagania opisane w niniejszej Instrukcji. Zmiana hasła do odszyfrowania nie jest konieczna co 30 dni – jednak dopuszczalne jest wykorzystywanie jednego hasła do obu logowań.

Pracownik jest zobowiązany do zapewnienia odpowiedniej ochrony fizycznej sprzętu mobilnego, w szczególności poprzez niepozostawianie go bez nadzoru oraz bezpieczny transport i eksploatację z uwagą na czynniki środowiskowe, tj. zalanie lub przegrzanie.

Należy unikać podłączania się do sieci publicznej za pośrednictwem ogólnodostępnych hotspotów wi-fi. Wykonując pracę poza miejscem przetwarzania, użytkownik powinien ograniczać ryzyko wglądu w wyświetlane informacje osób nieupoważnionych. Dostęp zdalny do sieci wewnętrznej lub poszczególnych systemów informatycznych nie jest realizowany dla pracowników. Wyjątki dotyczą serwisu zdalnego oprogramowania dostępnego dla ASI.

Dostęp do sprzętu mobilnego powinna mieć jedynie uprawniona osoba. Obowiązuje zakaz dopuszczania osób nieupoważnionych do sprzętu komputerowego.

9. Zasady bezpiecznej wymiany informacji

Przed wysłaniem wiadomości zawierającej dane osobowe, należy się upewnić, że podmiot odbierający jest do nich uprawiony. Uprawnienie może wynikać z upoważnienia, przydzielenia do danego zadania, zawartej umowy lub porozumienia lub na podstawie przepisów prawa.

Wysyłając wiadomości elektroniczne należy sprawdzić poprawność wprowadzonego adresu mailowego oraz załączonych plików. Weryfikacja wysyłanych treści oraz adresatów dotyczy również innych kanałów komunikacji. W szczególności, w przypadku faksu, należy zweryfikować obecność osoby odbierającej przy urządzeniu.

Szyfrowanie załączanych plików dokonuje się poprzez ich spakowanie w archiwum oraz ustalenie hasła, np. w programie 7-zip. Hasło do archiwum powinno być przesyłane inną drogą niż zaszyfrowane archiwum.

Wiadomości przychodzące należy zweryfikować poprzez:

a) weryfikację adresu mailowego nadawcy,
b) analizę treści pod kątem prób wyłudzeń informacji,
c) poprawność załączonych w treści linków – przed kliknięciem, poprzez zawieszenie kursora nad linkiem i weryfikacje wyświetlonego adresu,
d) obecność szyfrowanych załączników – w szczególności faktur,

e) obecność plików wykonywalnych w załącznikach.

10. Procedury tworzenia i sposobu przechowywania kopii zapasowych

Dane osobowe w Starostwie Powiatowym w Chodzieży zabezpiecza się poprzez wykonywanie kopii awaryjnych.

Za proces tworzenia kopii programów odpowiedzialny jest użytkownik systemu. Kopie przechowywane są w zamkniętej szafie w wydzielonym i zabezpieczonym pomieszczeniu.

Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.

Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii awaryjnych.

Nośniki, na których są przechowywane kopie danych osobowych powinny być wyraźnie oznaczone.

Komputery przenośne oraz inne mobilne nośniki danych osobowych w Starostwie Powiatowym w Chodzieży powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.

Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.

Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych.

Użytkownik systemu Starostwa Powiatowego w Chodzieży przechowuje dokumenty w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

11. Sposób zabezpieczenia systemu przed działalnością złośliwego oprogramowania

ADO zapewnia ochronę antywirusową. System antywirusowy w Starostwie Powiatowym w Chodzieży jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.

System antywirusowy ma aktywną funkcję automatycznej aktualizacji wzorców wirusów.

Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

12. Przesyłanie danych poza obszar przetwarzania

Urządzenia i nośniki w Starostwie Powiatowym w Chodzieży zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.

W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptograficzną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (tel., faks, bezpośrednia rozmowa).

Zabrania się przekazywania danych przez aplikacje internetowe nie wykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https").

13. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji

Urządzenia, dyski lub inne elektroniczne nośniki informacji Starostwa Powiatowego w Chodzieży, zawierające dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem wyznaczonego użytkownika przez ADO.

Instalacji, konserwacji oraz napraw sprzętu komputerowego w Starostwie Powiatowym w Chodzieży dokonują pracownicy firm wskazanych przez ADO.

Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych w Starostwie Powiatowym w Chodzieży mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Burmistrza lub posiadające umowy na powierzenie przetwarzania danych w zakresie konserwacji i napraw.

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

14. Zasady podpisania Zobowiązania pomiędzy ADO, a Użytkownikiem sprzętu IT

W związku z wprowadzeniem Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, każdy pracownik Starostwa Powiatowego w Chodzieży jest zobowiązany do podpisania Zobowiązania, które określa odpowiedzialność pracownika za użytkowany sprzęt IT i zainstalowane na nim oprogramowanie.

Zobowiązanie składa się z trzech części: A, B i C. Część A stanowi wstęp do zobowiązania, w części B znajduje się Metryka Urządzenia, za który pracownik jest odpowiedzialny, natomiast część C jest oświadczeniem pracownika o nie wykorzystywaniu zainstalowanego oprogramowania do nielegalnych celów oraz o nie korzystaniu ze szkodliwych i niebezpiecznych programów.

Lista programów jest aktualizowana po zakupach nowego oprogramowania.

Zobowiązanie zostaje sporządzone w trzech egzemplarzach po jednym dla stron (ADO, ASI, Użytkownik).

Zobowiązanie przechowywane jest w aktach osobowych użytkownika.

15. Podstawy prawne

Podstawy prawne niniejszej IZSI znajdują się w dokumencie Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Chodzieży.

16. Postanowienia końcowe

1) W sprawach nieuregulowanych niniejszą IZSI odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych Starostwa Powiatowego w Chodzieży.
2) Instrukcja Zarządzania Systemem Informatycznym w Starostwie Powiatowym w Chodzieży wchodzi w życie z dniem podpisania.

17. Dokumenty powiązane

1) Polityka Bezpieczeństwa Informacji.
2) Instrukcja Postępowania w Sytuacji Naruszeń.
3) Polityka Ochrony Danych Osobowych.
4) Analiza i szacowanie ryzyka w bezpieczeństwie informacji.
5) Wzory dokumentów.
6) Rejestry utrzymywane na podstawie niniejszej dokumentacji.

.....

(podpis Administratora Danych)

Analiza i szacowanie ryzyka w bezpieczeństwie informacji w Starostwie Powiatowym w Chodzieży 64-800 Chodzież, ul. Wiosny Ludów 1

Szczegóły dokumentu:

Sporządził:	*Beata Lewandowska* Administrator Bezpieczeństwa Informacji Audytor Wewnętrzny PN/ISO 27001
Data przekazania:	

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Warunki użytkowania dokumentacji bezpieczeństwa informacji

Dokumentacja opracowana przez ABI – Audyt, Consulting, Outsourcing Beata Lewandowska podlega ochronie przepisami prawa autorskiego; właścicielem wszystkich praw autorskich jest ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Po dokonaniu płatności, ABI – Audyt, Consulting, Outsourcing Beata Lewandowska udziela Starostwu Powiatowemu w Chodzieży niewyłącznego, stałego, ograniczonego prawa użytkowania dokumentacji, bez ograniczeń terytorialnych, wyłącznie w sposób określony w niniejszym dokumencie. Wszystkie prawa, których nie udzielono w niniejszym dokumencie, są zastrzeżone.

Starostwo Powiatowe w Chodzieży ma prawo wykorzystywać zakupioną dokumentację w dowolnym celu, związanym z działalnością organizacji, w dowolny sposób zgodny z udzielonymi prawami.

Starostwo Powiatowe w Chodzieży ma prawo kopiować dokumentację, w całości lub w części, czasowo lub trwale, w dowolnej formie i dowolnymi środkami.

Starostwo Powiatowe w Chodzieży ma prawo tłumaczyć dokumentację na inne języki, modyfikować ją i dowolnie edytować.

Bezwzględnie zabronione jest usuwanie oznaczeń właściciela praw autorskich oraz użytkowanie dokumentacji komercyjnie dla celów niezwiązanych z działalnością organizacji. W szczególności zabronione jest wynajmowanie lub dystrybucja oryginałów lub kopii dokumentacji poprzez sprzedaż lub w inny sposób przekazywanie jej z intencją sprzedaży, jak również drukowanie, publikowanie, publiczne udostępnianie poprzez systemy naziemne lub bezprzewodowe oraz poprzez udzielanie dostępu do dokumentacji nieautoryzowanym stronom trzecim w dowolny sposób (w tym dostępu przez internet), bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Zabroniony jest transfer praw do korzystania z dokumentacji na rzecz powiązanych lub niepowiązanych osób prawnych lub fizycznych, włącznie z przedsiębiorstwami zależnymi oraz udzielanie takich praw jakimkolwiek stronom trzecim bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

2. Podstawy prawne opracowanej dokumentacji

RODO - ROZDZIAŁ IV

Administrator i podmiot przetwarzający

Sekcja 1

Obowiązki ogólne

Artykuł 24

Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator danych wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora danych ciążących na nim obowiązków.

Artykuł 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Każda organizacja przetwarzająca dane narażona jest na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem:

- zniszczenia,
- utracenia,
- zmodyfikowania,
- nieuprawnionego ujawnienia,
- nieuprawnionego dostępu

} RYZYKO

Ocenę ryzyka w zakresie bezpieczeństwa przetwarzania danych osobowych przeprowadzamy biorąc pod uwagę potencjalnie negatywne skutki (straty,) zarówno dla administratora jak i dla osób, których dane dotyczą.

UWAGA! Gdyby istniało wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, wówczas należy dodatkowo przeprowadzić ocenę skutków dla ochrony danych osobowych.

3. Definicje

Ryzyko – możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów. Ryzyko jest mierzone wpływem (skutkami) i „prawdopodobieństwem wystąpienia". W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.

Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005)

Identyfikacja ryzyka - jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.

Kryteria akceptacji ryzyka – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową, np. przy przedziałach ryzyka 0-2, 3-5 oraz 6-8, akceptowalną wartością jest ryzyko tylko w zakresie 0-2.

Kryteria oceny ryzyka - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.

Podatność - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

Zabezpieczenie - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

Zagrożenie - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

Proces przetwarzania danych osobowych – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

Operacja przetwarzania danych osobowych - każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

Anonimizacja– oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.

Grupa Robocza Art. 29 - Grupa Robocza Art. 29 to powołany na mocy Dyrektywy 95/46 zespół roboczy do spraw ochrony osób fizycznych mający charakter doradczy i działający w sposób całkowicie niezależny. Jej misją jest służenie radą Komisji Europejskiej, i przyczynianie się do jednolitego stosowania przepisów krajowych przyjętych na mocy dyrektywy. Grupę tworzą przedstawiciele krajowych organów nadzorczych, przedstawiciele organów ustanowionych dla instytucji i organów unijnych (po jednym dla każdej z instytucji i organu) oraz przedstawiciele Komisji Europejskiej. Działania Grupy sprowadzają się głównie do wydawania niemających mocy wiążącej zaleceń, rekomendacji oraz opinii w sprawach unijnych aktów normatywnych z zakresu ochrony prywatności.

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 rozporządzenie o ochronie danych), które będzie stosowane od 25 maja 2018 r.; jego celami są skuteczna ochrona podstawowych praw i wolności osób

fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i zapewnienie swobodnego przepływu danych osobowych w UE w taki sposób, by ochrona praw jednostki nie stała temu na przeszkodzie.

4. Ogólne wymogi bezpieczeństwa

Przetwarzanie danych osobowych w Starostwie Powiatowym w Chodzieży odbywa się w postaci:

a) elektronicznej (np.: pliki na dysku komputera, w pamięci operacyjnej komputera),
b) papierowej (wydruki).

Aby zapewnić bezpieczeństwo przetwarzania danych osobowych należy stosować:

a) środki ochrony fizycznej stanowiska komputerowego oraz wydruków przed nieuprawnionym dostępem,
b) środki ochrony technicznej stanowiska komputerowego (np.: hasła dostępu do stacji roboczej, program antywirusowy).

5. Ewentualne koszty związane z utratą aktywów

1) Koszty związane z odtworzeniem aktywów,
2) Koszty utraty zaufania do administratora danych osobowych,
3) Koszty związane z utratą:
   a) poufności,
   b) integralności,
   c) dostępności danych ,
4) Możliwość nałożenia kary przez organ nadzorczy,
5) Koszty związane z możliwością nakazania przez organ nadzorczy całkowitego zaprzestania lub czasowego zaprzestania przetwarzania danych osobowych, np. w sytuacji niezastosowania przez administratora odpowiednich środków bezpieczeństwa.

6. Zagrożenia dla systemu informatycznego

Podstawowe zagrożenia dla systemu informatycznego w Starostwie Powiatowym w Chodzieży, przeznaczonego do przetwarzania danych osobowych:

1) Utrata poufności (pozyskanie danych przez osoby nieupoważnione):
   a) nieuprawniony dostęp do pomieszczenia gdzie znajdują się dane osobowe(wydruki),
   b) nieuprawniony dostęp do stacji roboczej (komputera) gdzie znajdują się dane osobowe (np. poprzez ujawnienie hasła dostępu),
   c) nieuprawnione skopiowanie danych osobowych na inny nośnik,

d) zgubienie nośnika zawierającego dane osobowe,
e) niedostateczne zniszczenie wydruku zawierającego dane osobowe,
f) klęska żywiołowa powodująca utratę poufności danych.

2) Utrata integralności (zmiany w systemie informatycznym przeprowadzone przez osoby nieupoważnione):
   a) nielegalny dostęp do dokumentów zawierających dane osobowe (w formie papierowej i elektronicznej),
   b) błędy ludzkie,
   c) działania wirusów (brak programów antywirusowych i firewalli),
   d) awarie oprogramowania komputerów.

3) Utrata rozliczalności (brak możliwości przypisania danemu podmiotowi konkretnych działań):
   a) brak mechanizmu uniemożliwiającego usunięcie logów o pracy danej osoby na komputerze,
   b) brak kontroli nad kopiowaniem dokumentów z komputera na nośniki zewnętrzne.

7. Źródło zagrożenia, sposób zabezpieczenia

1) Siły wyższe – naturalne -niezależne od jednostki ludzkiej:
   a) pożar np.: będący skutkiem uderzenia pioruna,
   b) starzenie się sprzętu,
   c) powódź,
   d) katastrofa budowlana,
   e) wilgoć, kurz,

Skutki zagrożeń wynikających z sił natury można starać się ograniczyć poprzez odpowiednie zabezpieczenie budynku, w którym znajdują się dane osobowe.

2) Działalność człowieka:
   a) błędy użytkowników,
   b) zgubienie nośnika informacji,
   c) niewłaściwe usunięcie danych z nośnika informacji,
   d) terroryzm,
   e) utrata prądu,
   f) szpiegostwo,
   g) kradzież,
   h) wandalizm,
   i) podsłuch,
   j) ataki socjotechniczne.

Zagrożenia wynikające z działalności człowieka mogą zostać ograniczone poprzez rygorystyczne przestrzeganie zasad ochrony danych osobowych obowiązujących oraz systematyczne szkolenia użytkowników.

8. Analiza zagrożeń i ryzyka

1) Analiza zagrożeń i ryzyka w Starostwie Powiatowym w Chodzieży polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.
2) Zagrożenia i ryzyka w zakresie ochrony danych osobowych Starostwa Powiatowego w Chodzieży:
   a) niedostateczne kwalifikacje Inspektora (w tym brak podnoszenia kwalifikacji),
   b) brak procedur ochrony danych osobowych,
   c) niezgodne z wymogami prawnymi, nieaktualne, nieadekwatne do zagrożeń procedury ochrony danych osobowych,
   d) brak aktualnego wykazu zbiorów będących w zasobach jednostki,
   e) brak lub wady upoważnień do przetwarzania danych osobowych,
   f) udzielanie upoważnienia do przetwarzania danych osobowych osobom postępującym nieetycznie,
   g) brak lub wady szkoleń z zakresu ochrony danych osobowych,
   h) wady nadzoru nad przetwarzaniem i ochroną danych osobowych,
   i) brak lub wady identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych,
   j) brak reakcji lub nieprawidłowa reakcja na zagrożenie bezpieczeństwa danych osobowych lub systemów i sieci teleinformatycznych.

9. Pojęcie i cele ryzyka

1) Ryzyko jest mierzone wpływem (skutkami) i „prawdopodobieństwem wystąpienia". Rozporządzenie w Artykule 32 definiuje cele w zakresie bezpieczeństwa przetwarzania i są to:
   a) pseudonimizacja i szyfrowanie danych osobowych,
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2) W związku z powyższym ryzyko w przetwarzaniu danych jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność (np. niezabezpieczony hasłem sprzęt komputerowy), powodując w ten sposób szkodę dla jednostki organizacyjnej (np. kradzież lub upublicznienie informacji).

10. Identyfikacja ryzyka

Zgodnie z zapisem 75 punktu preambuły Rozporządzenia, wyszczególnione zostały zagrożenia związane z przetwarzaniem danych z wyszczególnieniem prowadzących do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

a) jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
b) jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
c) jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,
d) jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
e) lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
f) jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

11. Pomiar i analiza ryzyka

Prawdopodobieństwo w terminologii zarządzania ryzykiem to możliwość wystąpienia jakiegoś zdarzenia (np. jako prawdopodobieństwo lub częstość w określonym przedziale czasu).

Zdefiniowanie poziomu ryzyka realizujemy wykorzystując macierz ryzyka, która daje możliwość zobrazowania poziomu zagrożeń.

PRAWDOPODOBIEŃSTWO

NISKI	1-20
ŚREDNI	21-60
WYSOKI	61-80

KRYTYCZNY 81-100

POZIOM RYZYKA *SPOSÓB DZIAŁANIA*

N - niski Poziom ryzyka akceptowany

Działania podejmowane są w zależności od wymaganych nakładów.

Ś - średni Poziom ryzyka nieakceptowany

Działanie może zostać przesunięte w czasie, lecz wymagany jest okresowy nadzór i monitorowanie.

W – wysoki Poziom ryzyka nieakceptowany

Działanie może zostać przesunięte w czasie, lecz wymagany jest stały nadzór i monitorowanie.

K – krytyczny Poziom ryzyka nieakceptowany

Wymagana jest niezwłoczna reakcja i działanie

RYZYKO SZCZĄTKOWE:

Ryzyko szczątkowe – ryzyko, które pozostaje po wprowadzeniu zabezpieczeń, często zwane również ryzykiem pozostałym lub ryzykiem akceptowalnym.

Po analizie zagrożeń i podatności wszystkich czynników występujących czy też mogących wystąpić opisanych dotychczas, niewątpliwie istnieje jeszcze pewne ryzyko dla bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Chodzieży. W celu bardziej przejrzystego zidentyfikowania pozostałego ryzyka niżej przedstawiono proces analizy ryzyka w oparciu o podaną macierz. W rzędach macierzy wyszczególnione są zasoby podlegające ochronie.

Analiza dotyczy ryzyk jakie zagrażają:

- INTEGRALNOŚCI,
- POUFNOŚCI ,
- DOSTĘPNOŚCI.

INTEGRALNOŚĆ - właściwość zapewniająca, że informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany – pożar, katastrofa budowlana, błąd ludzki przy przetwarzaniu danych osobowych, zniszczenie płyty zawierającej jedyną kopię danych osobowych.

POUFNOŚĆ - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom – nieuprawniony dostęp klientów do danych osobowych, zagubienie wydruku.

DOSTĘPNOŚĆ - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.

Skutek - rezultat niepożądanego incydentu, następstwa zaistnienia zagrożeń, szkody mierzone wysokością strat, jakie poniosłaby jednostka organizacyjna w wyniku ujawnienia, utraty lub modyfikacji informacji lub zasobu systemu.

Podatność - słabość zasobów, która może być wykorzystana przez zagrożenie – charakteryzuje łatwość, z jaką dane zagrożenie może wyrządzić szkodę.

Ryzyko - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobów, aby spowodować ich straty lub zniszczenie.

RYZYKO (iloczyn) : PODATNOŚĆ X SKUTEK = RYZYKO

PRZYJĘTE WARTOŚCI ZWIĄZANE Z OCENĄ ZAGROŻENIA:

- 1 - 3 - nie ma realnej szansy wystąpienia zidentyfikowanego zagrożenia; zagrożenie nigdy nie wystąpiło,
- 4 - 7 - zagrożenie jest mało realne, jednak zagrożenie może się pojawić,
- 8 - 9- zagrożenie jest realne i może pojawić się w nieoczekiwanym momencie, pomimo iż nie wystąpiło w okresie ostatnich 24 miesięcy,
- 10 - zagrożenie jest realne lub bardzo realne; zagrożenie wystąpiło w okresie ostatnich 24 miesięcy.

12. Szacowanie ryzyka integralności

W analizie ustalono cztery poziomy zagrożeń dotyczących zachowania integralności oraz zakres wartości liczbowych (1-10) dla tych poziomów:

Poziomy zagrożeń	Zakres wartości liczbowych skutków utraty integralności odpowiadający danemu poziomowi zagrożeń
Niskie - **N**	1-3
Średnie - **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

MACIERZ OSZACOWANIA „RYZYKA INTEGRALNOŚCI"

ZASOBY (miejsce)	SZACOWANIE	ZAGROŻENIA							
		Nielegalny dostęp	Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Wirusy	Personel	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	8	6	8	6	5	4	5	4
	PODATNOŚĆ	3	5	3	3	5	6	5	3
	RYZYKO	**24**	**30**	**24**	**24**	**25**	**24**	**25**	**12**
Zgromadzone dane – zbiory	SKUTKI	4	5	6	6	6	5	6	5
	PODATNOŚĆ	6	5	4	4	5	6	5	4
	RYZYKO	**24**	**25**	**24**	**24**	**30**	**30**	**30**	**20**
Oprogramowanie	SKUTKI	6	5	7	5	6	7	6	4
	PODATNOŚĆ	5	6	4	6	7	7	6	5
	RYZYKO	**30**	**30**	**28**	**30**	**42**	**49**	**36**	**20**
Sprzęt komputerowy	SKUTKI	6	6	5	6	6	7	6	4
	PODATNOŚĆ	6	5	4	5	6	7	5	4
	RYZYKO	**36**	**30**	**20**	**30**	**36**	**49**	**30**	**16**

OSZACOWANIE RYZYKA INTEGRALNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów, w ujęciu integralności informacji. Zgodnie z przyjętą metodyką szacowania ryzyka poziom wielkości ryzyka dla obliczonych wartości liczbowych wynosi:

NISKI 1-20

ŚREDNI 21-60

WYSOKI 61-80

KRYTYCZNY 81-100

Analizując otrzymane wyniki należy stwierdzić, że nie zanotowano poziomu ryzyka wysokiego i krytycznego w Starostwie Powiatowym w Chodzieży.

13. Szacowanie ryzyka poufności

W analizie szacowania ryzyka przyjęto cztery poziomy zagrożeń zachowania „poufności" i 10 - cio stopniową skalę skutków utraty „poufności":

Poziomy zagrożeń	Zakres wartości liczbowych skutków utraty poufności odpowiadający danemu poziomowi zagrożeń
Niskie - **N**	1-3
Średnie- **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

MACIERZ OSZACOWANIA „RYZYKA POUFNOŚCI"

ZASOBY (miejsce)	SZACOWANIE	ZAGROŻENIA									
		Nielegalny dostęp	Błędy, pomyłki	Pokonanie i omijanie zabezpieczeń	Nielegalne kopiowanie	Nieuprawnione naprawy	Rotacja personelu	Awarie	Klęski żywiołowe	Podsłuch i pogląd	Niedyskrecja
Nośniki informacji	SKUTKI	9	6	6	8	6	5	4	4	5	9
	PODATNOŚĆ	3	5	6	7	7	7	4	4	5	6
	RYZYKO	**27**	**30**	**36**	**56**	**42**	**35**	**16**	**16**	**25**	**54**
Zgromadzone dane	SKUTKI	8	8	8	7	8	6	6	3	7	8
	PODATNOŚĆ	6	5	7	6	5	4	5	3	3	5
	RYZYKO	**48**	**40**	**56**	**42**	**40**	**24**	**30**	**9**	**21**	**40**
Oprogramowanie	SKUTKI	8	8	9	9	7	5	5	4	6	6
	PODATNOŚĆ	3	6	6	5	3	4	4	4	4	4
	RYZYKO	**24**	**56**	**54**	**45**	**21**	**20**	**20**	**16**	**24**	**24**

Sprzęt komputerowy	SKUTKI	8	7	8	2	8	4	6	4	6	6
	PODATNOŚĆ	7	7	7	3	7	5	7	3	6	4
	RYZYKO	**56**	**49**	**56**	**6**	**56**	**20**	**42**	**12**	**36**	**24**

OSZACOWANIE RYZYKA POUFNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów w ujęciu integralności, poufności i dostępności informacji. Zgodnie z przyjętą metodyką szacowania ryzyka poziom wielkości ryzyka dla obliczonych wartości liczbowych wynosi:

NISKI 1-20

ŚREDNI 21-60

WYSOKI 61-80

KRYTYCZNY 81-100

Analizując otrzymane wyniki należy stwierdzić, że w Starostwie Powiatowym w Chodzieży nie zanotowano poziomu ryzyka wysokiego i krytycznego.

14. Szacowanie ryzyka dostępności

W analizie „ryzyka dostępności" przyjęto cztery poziomy zagrożeń zachowania „dostępności" i 10-cio stopniową skalę skutków utraty „dostępności":

Poziomy zagrożeń	**Zakres wartości liczbowych skutków utraty dostępności odpowiadający danemu poziomowi zagrożeń**
Niskie - **N**	1-3
Średnie- **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

MACIERZ OSZACOWANIA „RYZYKA DOSTĘPNOŚCI"

ZASOBY (miejsce)	SZACOWANIE	ZAGROŻENIA						
		Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Infekcja wirusowa	Rotacja personelu	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	2	2	3	3	3	3	4
	PODATNOŚĆ	2	1	2	3	3	3	4
	RYZYKO	**4**	**2**	**6**	**9**	**9**	**9**	**16**
Zgromadzone dane	SKUTKI	6	6	6	6	6	6	6
	PODATNOŚĆ	7	3	3	5	2	2	2
	RYZYKO	**42**	**18**	**18**	**30**	**12**	**12**	**12**
Oprogramowanie	SKUTKI	3	4	2	2	3	3	2
	PODATNOŚĆ	2	3	2	3	2	3	4
	RYZYKO	**6**	**12**	**4**	**6**	**6**	**9**	**8**
Sprzęt komputerowy	SKUTKI	3	4	2	2	3	5	3
	PODATNOŚĆ	4	2	3	3	3	5	2
	RYZYKO	**12**	**8**	**6**	**6**	**9**	**25**	**6**

OSZACOWANIE RYZYKA DOSTĘPNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów i dostępności informacji. Zgodnie z przyjętą metodyką szacowania ryzyka poziom wielkości ryzyka dla obliczonych wartości liczbowych wynosi:

NISKI 1-20

ŚREDNI 21-60

WYSOKI 61-80

KRYTYCZNY 81-100

Analizując otrzymane wyniki szacowania ryzyka Starostwa Powiatowego w Chodzieży w zakresie integralności, poufności, dostępności należy stwierdzić, że zanotowano średni poziom zagrożeń, natomiast nie zanotowano poziomu ryzyka wysokiego i krytycznego.

15. Dokumenty powiązane

1) Polityka Bezpieczeństwa Informacji.
2) Polityka Ochrony Danych Osobowych.
3) Instrukcja Postępowania w Sytuacji Naruszeń.
4) Instrukcja Zarządzania Systemem Informatycznym.
5) Wzory dokumentów.
6) Rejestry utrzymywane na podstawie niniejszej dokumentacji.

.....

(podpis Administratora Danych)

Rejestry

utrzymywane na podstawie niniejszej dokumentacji

w

Starostwie Powiatowym w Chodzieży

64-800 Chodzież, ul. Wiosny Ludów 1

Szczegóły dokumentu:

Sporządził:	*Beata Lewandowska* Administrator Bezpieczeństwa Informacji Audytor Wewnętrzny PN/ISO 27001
Data przekazania:	

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Warunki użytkowania dokumentacji bezpieczeństwa informacji

Dokumentacja opracowana przez ABI – Audyt, Consulting, Outsourcing Beata Lewandowska podlega ochronie przepisami prawa autorskiego; właścicielem wszystkich praw autorskich jest ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Po dokonaniu płatności, ABI – Audyt, Consulting, Outsourcing Beata Lewandowska udziela Starostwu Powiatowemu w Chodzieży niewyłącznego, stałego, ograniczonego prawa użytkowania dokumentacji, bez ograniczeń terytorialnych, wyłącznie w sposób określony w niniejszym dokumencie. Wszystkie prawa, których nie udzielono w niniejszym dokumencie, są zastrzeżone.

Starostwo Powiatowe w Chodzieży ma prawo wykorzystywać zakupioną dokumentację w dowolnym celu, związanym z działalnością organizacji, w dowolny sposób zgodny z udzielonymi prawami.

Starostwo Powiatowe w Chodzieży ma prawo kopiować dokumentację, w całości lub w części, czasowo lub trwale, w dowolnej formie i dowolnymi środkami.

Starostwo Powiatowe w Chodzieży ma prawo tłumaczyć dokumentację na inne języki, modyfikować ją i dowolnie edytować.

Bezwzględnie zabronione jest usuwanie oznaczeń właściciela praw autorskich oraz użytkowanie dokumentacji komercyjnie dla celów niezwiązanych z działalnością organizacji. W szczególności zabronione jest wynajmowanie lub dystrybucja oryginałów lub kopii dokumentacji poprzez sprzedaż lub w inny sposób przekazywanie jej z intencją sprzedaży, jak również drukowanie, publikowanie, publiczne udostępnianie poprzez systemy naziemne lub bezprzewodowe oraz poprzez udzielanie dostępu do dokumentacji nieautoryzowanym stronom trzecim w dowolny sposób (w tym dostępu przez internet), bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Zabroniony jest transfer praw do korzystania z dokumentacji na rzecz powiązanych lub niepowiązanych osób prawnych lub fizycznych, włącznie z przedsiębiorstwami zależnymi oraz udzielanie takich praw jakimkolwiek stronom trzecim bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

2. Rejestr sprzętu informatycznego, oprogramowania oraz licencji

L.p.	Nazwa sprzętu informatycznego (numer zestawu)	Wykorzystywane oprogramowanie	Numer licencji	Dane użytkownika	Uwagi

3. Rejestr naruszeń bezpieczeństwa informacji

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

4. Rejestr udostępnień danych osobowych innym podmiotom

Lp.	Imię i Nazwisko/Nazwa zbioru (możliwie najlepszy opis osoby, której dane zostały udostępnione lub całego zbioru)	Data	Nazwa podmiotu, któremu udostępniono dane (np. upoważniony organ, instytucja lub inny, który wykazał uprawnienia do udostępniania mu danych)	Cel udostępniania (podstawa prawna/numer umowy)	Zakres danych (jakie dane zostały udostępnione)	Rodzaj zbioru/zasobu i jego lokalizacja (np. papierowy wydruk, dane w formie elektronicznej

5. Rejestr podmiotów z którymi zawarto umowę powierzenia danych

Lp.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Zakres powierzonych danych (jakie dane zostały powierzone)	Określenie zbioru/zasobu

6. Rejestr wniosków w sprawie realizacji praw osób, których dane są przetwarzane

L.p.	Data	Dane wnioskodawcy (imię, nazwisko, adres)	Jakiego prawa dotyczy wniosek	Data realizacji roszczeń	Sposób realizacji roszczeń.

7. Rejestr czynności przetwarzania

LP.	1 **Nazwa czynności przetwarzania**	2 **Jednostka organizacyjna (departament, dział itp.)**	3 **Cel przetwarzania**	4 **Kategorie osób**	5 **Kategorie danych**	6 **Podstawa prawna**	7 **Źródło danych**	8 **Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	9 **Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*	10 **Nazwa podmiotu przetwarzającego i dane kontakowe** *(jeśli dotyczy)*	11 **Kategorie odbiorców** *(innych niż podmiot przetwarzający)*	12 **Nazwa systemu lub oprogramowania**	13 **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1** *(jeżeli jest to możliwe)*	14 **DPIA (jeśli tak, lokalizacja raportu)**	15 **Transfer do kraju trzeciego lub org. międzynarodowej**	16
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
			Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**			**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt a**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**		**Art.. 30 ust. 1 pkt g**		**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**
Przykład wypełnienia tabeli																
1.	**Rekrutacja pracowników**	Dyrektor Szkoły	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniac	• Zgoda osób, których dane dotyczą • Przepis prawa Ustawa z dnia 26	Kandydaci do pracy	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	System Kadry. Dokumentacja papierowa	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy

					h zawodowych.	czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22^1 ust. 1							systemu informatycznego, dostęp tylko dla osób upoważnionych.			
2.	**Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy**	Samodzielne stanowisko ds. kadr	Prowadzenie ewidencji pracowników w zgodnie z Kodeksem pracy	Pracownicy pomocniczy (recepcjoniści, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem pracy	• Umowa o pracę • Przepis prawa Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22^1 w związku z art. 94 pkt 9a i 9b	Pracownik	50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	System Kadry. Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy

8. Rejestr kategorii przetwarzania

	1	2	3	4	5	6	7	8	9	10	11
LP.	**Kategorie przetwarzań**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)**	**Administrator**				**Czas trwania przetwarzania**	**Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane**	**Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi**	**Podprzetwarzający (podwykonawca) - jeśli dotyczy**	
			Nazwa i dane kontaktowe administratora	**Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)**	**Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)**	**Inspektor ochrony danych administratora (jeśli powołano)**				**Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)**	**Kategorie podpowierzonych przetwarzań**
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		
Przykład wypełnienia tabeli											
1	**Udostępnienie i utrzymywanie zdalnej platformy programistycznej do prowadzenia sklepu internetowego w środowisku**	**• Kontrola dostępu do infrastruktury, aplikacji i baz danych. • Dostęp do danych otrzymują wyłącznie osoby wskazane przez**	**Spółka BCA - sklep www** ul. Kwiatkowa 5 kontakt@bcaspolka.pl tel.: 123 456 789	Nie dotyczy	Nie dotyczy	**Andrzej Nowak** jan@bcaspolka.pl tel.: 123 456 788	**29 marca 2019 r.**	**Szwajcaria** (przetwarzający w celu realizacji tej usługi korzysta z usług podwykonawcy w Szwajcarii)	Nie dotyczy	**BeispielRechenzentrum A.B.C GmbH** ul. Beispiel Straße 123/3 3006 Berno, Szwajcaria info@beispielrechencetrum.ch	**Przechowywanie, udostępnianie, utrwalanie i usuwanie danych w ramach udostępnianiej mocy obliczeniowej procesorów, przestrzeni**
2			**Sklep Internetowy XYZ** ul. DanychOosobowych 1, tel.: 123 545 567, kontakt@sklepxyz.pl	Nie dotyczy	**Andrzej Przykładowy** andrzej@sklepintxyz.pl tel.: 999 444 321	**Jan Bezpieczny** jan@sklepintxyz.pl tel.: 123 456 788	**29 marca 2019 r.**				

3	**sprzętowo-programowym wynajętym przez przetwarzającego**	**przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze).** **• Szyfrowana transmisja danych.** (szczegółowe procedury znajdują się w polityce bezpieczeństwa - link/numer dokumentu)	**PrzykładowySklep.pl** ul. Przykładowa 4/5 tel. 765 432 234 kontakt@przykladowysklep.pl	Nie dotyczy	Nie dotyczy	**Imię Nazwisko** imie@przykladowysklep.pl tel.: 333 444 555	**22 maja 2021 r.**				**pamięci operacyjnej i dyskowej.**
4			**Spółka ABC** ul. IOD 5 kontakt@spolkaabc.pl tel.: 133 456 888	Nie dotyczy	Nie dotyczy	**Imię Nazwisko** iod@spolkaabc.pl tel.: 123 456 788	**23 maja 2020 r.**				

9. Zarządzanie rejestrami utrzymywanymi na podstawie niniejszego dokumentu

L.p.	Nazwa rejestru	Miejsce przechowywania	Osoba odpowiedzialna za przechowywanie	Zabezpieczenia rejestru	Okres przechowywania
1.	Rejestr sprzętu informatycznego, oprogramowania oraz licencji				
2.	Rejestr naruszeń bezpieczeństwa informacji				
3.	Rejestr udostępnień danych osobowych innym podmiotom				
4.	Rejestr podmiotów z którymi zawarto umowę powierzenia danych				
5.	Rejestr wniosków w sprawie realizacji praw osób, których dane są przetwarzane				
6.	Rejestr czynności przetwarzania				
7.	Rejestr kategorii przetwarzania				

10. Dokumenty powiązane.

1) Polityka Bezpieczeństwa Informacji.
2) Polityka Ochrony Danych Osobowych.
3) Instrukcja Postępowania w Sytuacji Naruszeń.
4) Instrukcja Zarządzania Systemem Informatycznym.
5) Analiza i szacowanie ryzyka w bezpieczeństwie informacji.
6) Wzory dokumentów.

.....

(podpis Administratora Danych)

Wzory dokumentów
systemu zarządzania bezpieczeństwem informacji
w
Starostwie Powiatowym w Chodzieży
64-800 Chodzież, ul. Wiosny Ludów 1

Szczegóły dokumentu:

Sporządził:	*Beata Lewandowska* Administrator Bezpieczeństwa Informacji Audytor Wewnętrzny PN/ISO 27001
Data przekazania:	

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Warunki użytkowania dokumentacji bezpieczeństwa informacji

Dokumentacja opracowana przez ABI – Audyt, Consulting, Outsourcing Beata Lewandowska podlega ochronie przepisami prawa autorskiego; właścicielem wszystkich praw autorskich jest ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Po dokonaniu płatności, ABI – Audyt, Consulting, Outsourcing Beata Lewandowska udziela Starostwu Powiatowemu w Chodzieży niewyłącznego, stałego, ograniczonego prawa użytkowania dokumentacji, bez ograniczeń terytorialnych, wyłącznie w sposób określony w niniejszym dokumencie. Wszystkie prawa, których nie udzielono w niniejszym dokumencie, są zastrzeżone.

Starostwo Powiatowe w Chodzieży ma prawo wykorzystywać zakupioną dokumentację w dowolnym celu, związanym z działalnością organizacji, w dowolny sposób zgodny z udzielonymi prawami.

Starostwo Powiatowe w Chodzieży ma prawo kopiować dokumentację, w całości lub w części, czasowo lub trwale, w dowolnej formie i dowolnymi środkami.

Starostwo Powiatowe w Chodzieży ma prawo tłumaczyć dokumentację na inne języki, modyfikować ją i dowolnie edytować.

Bezwzględnie zabronione jest usuwanie oznaczeń właściciela praw autorskich oraz użytkowanie dokumentacji komercyjnie dla celów niezwiązanych z działalnością organizacji. W szczególności zabronione jest wynajmowanie lub dystrybucja oryginałów lub kopii dokumentacji poprzez sprzedaż lub w inny sposób przekazywanie jej z intencją sprzedaży, jak również drukowanie, publikowanie, publiczne udostępnianie poprzez systemy naziemne lub bezprzewodowe oraz poprzez udzielanie dostępu do dokumentacji nieautoryzowanym stronom trzecim w dowolny sposób (w tym dostępu przez internet), bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

Zabroniony jest transfer praw do korzystania z dokumentacji na rzecz powiązanych lub niepowiązanych osób prawnych lub fizycznych, włącznie z przedsiębiorstwami zależnymi oraz udzielanie takich praw jakimkolwiek stronom trzecim bez uzyskanej uprzednio pisemnej zgody ABI – Audyt, Consulting, Outsourcing Beata Lewandowska.

2. Wniosek o nadanie uprawnień do przetwarzania danych osobowych

Wniosek

o założenie profilu/nadanie uprawnień/modyfikację uprawnień*

Dane użytkownika:

Nazwisko i imię	
Stanowisko służbowe	

Wnioskuję o:

założenie profilu i nadanie uprawnień/modyfikację uprawnień/zablokowanie profilu*

do systemu informatycznego: .....

Tak	Nazwa uprawnienia	Opis uprawnienia	Uwagi
	Z	Pełne prawa do zarządzania bazą	
	W	Pełne prawa do edycji danych	
	N	Prawo do zakładania nowych kont	
	M	Prawo do dodawania i modyfikacji danych	
	P	Prawo do przeglądania danych	
	D	Prawo do drukowania danych	
	A	Prawo do wykonywania kopii archiwalnych	

Wniosek o nadanie/modyfikację uprawnień złożył:

_____

Nazwisko i imię (przełożony pracownika)

_____

Podpis, data

Nazwisko i imię pracownika	
Identyfikator w systemie (login)	

Wniosek o nadanie/modyfikację uprawnień wykonał:

_____

Nazwisko i imię (administrator systemu)

_____

Podpis, data

3. Zobowiązanie Użytkownika

Część A **ZOBOWIĄZANIE**

Niniejsze zobowiązanie (zwane dalej „Zobowiązaniem") zostało zawarte w dniu ..... w ..... pomiędzy:

..... reprezentowanym przez ..... Panią/Pana .....zwanego dalej „Pracodawcą"

oraz Panią/Panem ..... zwaną/ym dalej „Użytkownikiem".

Wstęp:

1. Użytkownik zatrudniony jest przez Pracodawcę na podstawie .....
2. Pracodawca wyposażył stanowisko pracy Użytkownika w oprogramowanie na używanie, którego nabył licencję.
3. Użytkownik korzysta z komputera/notebooka/tabletu, telefonu i oprogramowania w związku z wykonywaniem obowiązków pracowniczych.
4. Zobowiązanie składa się z części A – ogólnej, części B - metryki urządzenia, w której znajduje się opis sprzętu i zainstalowanego dozwolonego oprogramowania i części C - oświadczeniu użytkownika o nie wykorzystywaniu zainstalowanego oprogramowania do nielegalnych celów oraz o nie korzystaniu ze szkodliwych i niebezpiecznych programów.
5. Pracodawca i Użytkownik uzgadniają, że do podstawowych obowiązków Użytkownika należy korzystanie z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również nie korzystanie z jakiegokolwiek Oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
6. Użytkownik oświadcza, iż jest świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny, oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.
7. Pracodawca i Użytkownik uzgadniają, że naruszenie przez Użytkownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę stosunku pracy, lub rozwiązanie przez Pracodawcę stosunku pracy bez wypowiedzenia, z winy użytkownika.
8. Niniejsze Zobowiązanie zostało sporządzone w trzech egzemplarzach, po jednym dla każdej ze stron oraz dla Administratora Systemu Informatycznego. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Zobowiązania za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności. Rozwiązanie Zobowiązania następuje również na skutek rozwiązania stosunku pracy.

....

podpis Pracodawcy podpis Użytkownika

Część B **Metryka Urządzenia**

Nazwa użytkownika w systemie:

Numer ewidencyjny zestawu:

Wyposażenie sprzętowe			
Nazwa urządzenia		**Nr seryjny**	**Okres gwarancji**
Jednostka Centralna			
MONITOR			
UPS			
Pamięć przenośna			
Inne (tablet, telefon)			

Oprogramowanie	
Nazwa	**Licencja**

Przyjmuję do użytkowania wyżej wymieniony sprzęt i oprogramowanie.

....

Podpis ASI **data i podpis użytkownika**

Część C

Użytkownik nie może korzystać z nielegalnie nabytych plików i oprogramowania, plików mp3 oraz szkodliwych, niebezpiecznych programów (np. typu p2p, torrent, czy też nabytych z nielegalnego źródła plików) w miejscu pracy oraz poza nim, gdzie wykorzystywałby ich do zabronionych celów.

Użytkownik oświadcza, iż nie będzie instalował żadnego oprogramowania, bez wcześniejszej konsultacji z Administratorem Systemu Informatycznego.

Użytkownik odpowiada za uszkodzenia wynikłe podczas złego/nieprawidłowego eksploatowania sprzętu.

Wszelkie urządzenia magazynujące dane (pendrive, karty pamięci, przenośne dyski twarde) zakupione do celów służbowych, mają być używane do celów służbowych.

Oświadczam, iż zapoznałem(am) się z porozumieniem i będę się stosować do wyżej wymienionych zaleceń oraz jestem świadomy(ma) odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny, oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.

Podpis użytkownika

4. Upoważnienie do przetwarzania danych osobowych

....., dn. ..... 20..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679/UE z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) - dalej RODO) nadaję upoważnienie Pani/ Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie

.....
(zakres obowiązków)

.....

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych dostępnych w zasobach (zbiorach danych, procesach) .....

.....

bez prawa dostępu do informacji o .....

.....

z wykorzystaniem systemu informatycznego.....

.....

do którego ustalono Identyfikator (login) .....

.....

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy o ochronie danych osobowych, a także z Dokumentacją Bezpieczeństwa Informacji Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w

..... .

Okres ważności
od:
do:

.....
podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia*, ...
Odwołano, dnia .....

.....
podpis osoby uprawnionej do odwołania upoważnienia

* Data rozwiązania stosunku pracy/umowy cywilno-prawnej

5. Oświadczenie o poufności.

....., dn. .....

Oświadczenie pracownika o zachowaniu poufności i przestrzeganiu zasad przetwarzania danych osobowych oraz informacji stanowiących tajemnicę firmową

.....

Ja, niżej podpisany/a ..... jako pracownik ..... oświadczam, że jestem świadomy/a ciążącego na mnie, na podstawie art. 100 Kodeksu Pracy obowiązku przestrzegania w tajemnicy informacji, których ujawnienie mogłoby narażać pracodawcę na szkodę.

W związku z tym oświadczam, że w czasie trwania zatrudnienia w ..... (zwanej w dalszej części oświadczenia Pracodawcą), zobowiązuję się do zachowania w ścisłej tajemnicy wszelkich informacji personalnych, finansowych i organizacyjnych stanowiących tajemnicę, których ujawnienie mogłoby narazić Pracodawcę na szkodę. W szczególności zobowiązuję się do przestrzegania tajemnicy przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji.

Zostałem przy tym poinformowany/a, że tajemnicę stanowią wszelkie informacje, które nie zostały udostępnione do wiadomości publicznej.

Jakiekolwiek przekazywanie, ujawnianie, wykorzystywanie, nabywanie od osób nieuprawnionych, zbywanie lub oferowanie do zbycia tajemnicy jest zabronione, chyba że następuje za uprzednim pisemnym zezwoleniem Pracodawcy. Za naruszenie tajemnicy uważa się również przekazanie informacji ją stanowiących pracownikowi nieuprawnionemu.

Jednocześnie zobowiązuję się do zachowania szczególnej staranności przy dostępie i korzystaniu z danych, objętych tajemnicą, a mianowicie:

- korzystać z nich będę jedynie w zakresie potrzebnym do wykonania konkretnego zadania,
- nie będę utrwalać w/w danych na jakichkolwiek nośnikach informacji, bez zgody przełożonego,
- będę chronić wszelkie dane, jak również nośniki, objęte tajemnicą informacji przed osobami nieupoważnionymi,
- wszelkie, zauważone przeze mnie braki w ochronie poufnych danych będę natychmiast zgłaszać odpowiedzialnej za zabezpieczenie danych osobie lub bezpośredniemu przełożonemu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących zasadach dotyczących przetwarzania informacji w tym danych osobowych, określonych w „Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji" i zobowiązuję się ich przestrzegać.

Zobowiązuję się do zachowania w tajemnicy informacji oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, **zarówno w czasie trwania umowy, jak i po jej ustaniu.**

Oświadczam, że zostałem/am poinformowany/a o obowiązujących zasadach dotyczących przetwarzania informacji w tym danych osobowych, określonych w „Dokumentacji Zarządzania Bezpieczeństwem Informacji" i zobowiązuję się ich przestrzegać.

Poinformowano mnie również, że złamanie zasad ochrony danych osobowych, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Jest mi wiadome również, że przestrzeganie powyższych zasad stanowi podstawowy obowiązek pracownika, określony w Kodeksie Pracy - Art. 100 § 2 ust. 4 i 5.

Niezależnie od odpowiedzialności pracowniczej - naruszenie tajemnicy, powodujące szkodę pracodawcy może narazić pracownika na odpowiedzialność karną.

W przypadku ustania zatrudnienia zobowiązuję się do zwrotu wszelkich dokumentów i innych materiałów dotyczących tajemnicy, które sporządziłem/am, zebrałem/am lub otrzymałem/am w trakcie wykonywania pracy, włączając w to ich kopie, odpisy oraz zapisy.

Obowiązek zachowania tajemnicy przedsiębiorstwa obowiązuje w czasie trwania kolejnych umów oraz w okresie 5 lat od dnia rozwiązania lub wygaśnięcia ostatniej umowy.

....., dnia ..... podpis .....

6. Umowa powierzenia danych osobowych

Umowa
powierzenia przetwarzania danych osobowych
stanowiąca uzupełnienie Umowy .....

zawarta dnia ..... w ....., pomiędzy:

..... (**„Administrator"**)

a

..... (**„Przetwarzający"**)

(dalej łącznie jako: **„Strony"**)

Mając na uwadze, że:

i. Strony zawarły umowę ..... (**„Umowa Podstawowa"**), w związku z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;

ii. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;

iii. Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom 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) (**„RODO"**).

Strony postanowiły zawrzeć Umowę o następującej treści:

przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora

1. Opis Przetwarzania

1.1. **Przedmiot. [Art. 28 ust. 3 RODO]** Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.

1.2. **Czas. [Art. 28 ust. 3 RODO]** Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.

1.3. **Charakter i cel. [Art. 28 ust. 3 RODO]** Charakter i cel przetwarzania wynikają z Umowy Podstawowej. W szczególności

1.3.1. charakter przetwarzania określony jest następującą rolą Przetwarzającego [*przykład: obsługa księgowa Administratora*], zaś

1.3.2. celem przetwarzania jest [*przykład: umożliwienie Administratorowi wywiązywania się z prawnych obowiązków związanych z prowadzeniem rachunkowości a także w celu zarządzania finansowego Administratora*]

1.4. **Rodzaj danych. [Art. 28 ust. 3 RODO]** Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („**Dane**"):

Dane zwykłe

(1) imię i nazwisko

(2) numer ewidencyjny PESEL

(3) adres e-mail

(4) adres IP

(5) numery telefonów

(6) adres zamieszkania

(7) data urodzenia

(8) NIP

(9) seria i numer dokumentu tożsamości

(10) imiona rodziców

(11) numer rachunku bankowego

(12) .....

Dane szczególnych kategorii i dane karne:

(13) .....

(14) .....

(15) .....

Dane dzieci

(16) imię i nazwisko

(17) data urodzenia

(18) adres e-mail

(19) pseudonim

(20) .....

Dane nieustrukturyzowane

(21) kontent o potencjalnej i prawdopodobnej zawartości danych osobowych (wpisy, dokumenty tekstowe. obrazy, nagrania, filmy)

1.5. **Kategorie osób. [Art. 28 ust. 3 RODO]** Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:

(1) pracownicy Administratora i podmiotów stowarzyszonych Administratora

(2) klienci usługi/produktu Administratora określonych w Umowie Podstawowej

(3) osoby, z którymi klienci Administratora wchodzą w interakcje społeczne

(4) kontrahenci (odbiorcy i dostawcy) klientów administratora

(5) odbiorcy korespondencji elektronicznej klientów Administratora

(6) .....

(7) .....

(8) .....

2. Podpowierzenie

2.1. **Podpowierzenie. [Art. 28 ust. 2 RODO]** Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („**podpowierzenie**") w drodze pisemnej umowy podpowierzenia („**Umowa Podpowierzenia**") innym podmiotom przetwarzającym. („**Podprzetwarzający**"), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

2.2. **Sprzeciw.** Powierzenie przetwarzania Danych Podprzetwarzającym spoza Listy Zaakceptowanych Podprzetwarzających wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia Danych konkretnemu Podprzetwarzającemu. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć Danych Podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu Podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

2.3. **Transfer obowiązków. [Art. 28 ust. 4 RODO]** Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

2.4. **Zobowiązanie względem Administratora.** Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.

2.5. **Zakaz podzlecenia świadczenia głównego [Art. 28 ust. 4 RODO]** Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

3. Obowiązki Przetwarzającego

Przetwarzający ma następujące obowiązki:

3.1. **Udokumentowane polecenia. [RODO 28.3.a]** Przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

3.2. **Nieprzetwarzanie poza EOG. [RODO 28.3.a]** Przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („**EOG**")). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

3.3. **Poinformowanie o zamiarze przetwarzania poza EOG. [RODO 28.3.a]** Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać Dane poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

3.4. **Tajemnica. [RODO 28.3.b]** Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

3.5. **Bezpieczeństwo.[RODO 28.3.c]** Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy .

3.6. **Podprzetwarzanie. [RODO 28.3.d]** Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego).

3.7. **Współpraca przy realizacji praw jednostki. [RODO 28.3.e]** Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO (**„Prawa jednostki"**). Przetwarzający oświadcza, że zapewnia obsługę Praw jednostki w odniesieniu do powierzonych Danych. Szczegóły obsługi Praw jednostki zostaną pomiędzy Stronami uzgodnione. Strony ustaliły procedurę obsługi Praw jednostki odrębnym dokumentem.

3.8. **Wsparcie przy obowiązkach bezpieczeństwa. [RODO 28.3.f]** Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32-36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

3.9. **Legalność poleceń [RODO 28.3 akapit 2].** Jeżeli Przetwarzający powzięmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

3.10. **Projektowanie prywatności. [RODO 25.1.]** Planując dokonanie zmian w sposobie przetwarzania Danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.

3.11. **Minimalizacja. [RODO 25.2.]** Przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.

3.12. **RCPD. [RODO 30.2.]** Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru czynności przetwarzania danych osobowych (wymóg art. 30 RODO). Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

3.13. **Profilowanie. [RODO 13 i 14]** Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4

RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

3.14. **Szkolenie personelu**. Przetwarzający ma obowiązek, aby osoby upoważnione do przetwarzania Danych otrzymały odpowiednie szkolenie z zakresu ochrony danych osobowych.

4. Obowiązki Administratora

4.1. Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

5. Bezpieczeństwo danych

5.1. **Bezpieczeństwo danych osobowych. [Art. 32 RODO]** Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych, udostępnił ją Administratorowi i stosuje się do jej wyników co do organizacyjnych i technicznych środków ochrony danych.

5.2. **Środki bezpieczeństwa.** Strony uzgodniły odrębnym dokumentem poziom zabezpieczeń Danych wymagany po stronie Przetwarzającego.

5.3. **Gwarancje bezpieczeństwa.** Przetwarzający przedstawił Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obie Strony zachowują kopie przedstawionych dokumentów i dowody przedstawienia informacji, dla potrzeb spełnienia wymogu rozliczalności.

6. Powiadomienie o Naruszeniach Danych Osobowych

6.1. **Powiadomienie o naruszeniu.** Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.

6.2. **Rozwinięcie.** Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.

7. Nadzór

7.1. **Sprawowanie kontroli. [Art. 28 ust. 3 lit. h]** Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do (i) wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz (ii) wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.

7.2. **Współpraca przy kontroli. [Art. 28 ust. 3 lit. h]** Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

7.3. Przetwarzający:

(1) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO

(2) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

8. Oświadczenia Stron

8.1. **Oświadczenie Administratora**. Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie w jakim powierzył je Przetwarzającemu.

8.2. **Oświadczenie Przetwarzającego.** Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

8.3. **Referencje.** Na żądanie Administratora Przetwarzający okaże Administratorowi stosowne referencje, wykaz doświadczenia, informacje finansowe lub inne dowody.

9. Odpowiedzialność

9.1. **Odpowiedzialność Przetwarzającego. [Art. 82 ust. 3 RODO]** Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.

9.2. **Odpowiedzialność za Podprzetwarzających. [Art. 28 ust. 4 RODO]** Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

10. Okres Obowiązywania Umowy Powierzenia

8.1 **[Art. 28 ust. 3]** Umowa została zawarta na czas obowiązywania Umowy Podstawowej.

11. Usunięcie Danych

11.1. **Usunięcie danych. [RODO 28.3.g]** Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa dalszego przetwarzać powierzonych Danych i jest zobowiązany do:

(1) usunięcia Danych,

(2) usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.

11.2. **Karencja**. Przetwarzający dokona usunięcia Danych po upływie 180 dni od zakończenia Umowy, chyba że Administrator poleci mu to uczynić wcześniej.

11.3. **Oświadczenie**. Po wykonaniu zobowiązania, o którym mowa w punkcie 10.1., Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych.

12. Postanowienia Końcowe

12.1. **Pierwszeństwo.** W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy powierzenia a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy

powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

12.2. **Egzemplarze.** Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

12.3. **Właściwość prawa.** Umowa podlega prawu polskiemu oraz RODO.

Podpis Administratora

Podpis Przetwarzajacego

7. Zgody na przetwarzanie danych, na udostępnienie danych do państwa trzeciego

Na podstawie art. 6 ust 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679/UE z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) oświadczam że wyrażam zgodę na przetwarzanie oraz udostępnianie moich danych osobowych, w celu realizacji zadań związanych z procesem rekrutacji w .....

(Data i podpis kandydata)

Na podstawie art. 6 ust 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679/UE z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) oświadczam że wyrażam zgodę na przetwarzanie oraz udostępnianie moich danych osobowych, w celu realizacji zadań związanych z przyszłymi procesami rekrutacji w .....

(Data i podpis kandydata)

Na podstawie art. 6 ust 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679/UE z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) oświadczam że wyrażam zgodę na przetwarzanie moich danych osobowych podanych w powyższym formularzu, w celu korzystania z Zakładowego Funduszu Świadczeń Socjalnych.

(Data i podpis pracownika)

Na podstawie art. 6 ust 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679/UE z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) oświadczam że wyrażam zgodę na przetwarzanie moich danych osobowych podanych w powyższym formularzu w celu korzystania z Zakładowej Kasy Pożyczkowej.

(Data i podpis pracownika)

8. Obowiązek informacyjny

Klauzula informacyjna o przetwarzaniu danych

Na podstawie art. 13 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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 (dalej: RODO), informuję, że:

Administrator danych:
Administratorem Pani/Pana danych osobowych jest ..... z siedzibą w ....., ul. ....., kod pocztowy ....., e-mail: ....., tel. .....

Przedstawiciel administratora danych:
Przedstawicielem administratora danych osobowych jest ..... Pani/Pan ....., ul. ....., ..., e-mail: ....., tel. .....

Inspektor ochrony danych:
Dane kontaktowe inspektora ochrony danych ..... w ..... z siedzibą w ..... ul. ....., ..., e-mail: ....., tel. .....

Cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania:
Przetwarzanie Pani/Pana danych osobowych odbywać się będzie:

- w celu zawarcia umowy ..... usług na podstawie zainteresowania naszą ofertą (podstawa z art. 6 ust 1 lit. b Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679/UE z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej RODO;
- w celach archiwalnych (dowodowych) będących realizacją naszego prawnie uzasadnionego interesu zabezpieczenia informacji na wypadek prawnej potrzeby wykazania faktów (art. 6 ust. 1 lit. f RODO);
- w celu ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami będącego realizacją naszego prawnie uzasadnionego interesu (podstawa z art. 6 ust. 1 lit. f RODO);
- w celu badania satysfakcji klientów będącego realizacją naszego prawnie uzasadnionego interesu określania jakości naszej obsługi oraz poziomu zadowolenia naszych klientów z produktów i usług (podstawa z art. 6 ust. 1 lit. f RODO);

Okres przechowywania danych osobowych:

- Dane osobowe wynikające z zawarcia umowy będą przetwarzane przez okres, w którym mogą ujawnić się roszczenia związane z tą umową, czyli przez ..... lat od końca roku, w którym wygasła umowa, w tym ..... lat to najdłuższy możliwy okres przedawnienia roszczeń, dodatkowy rok jest na wypadek roszczeń zgłoszonych w ostatniej chwili i problemów z doręczeniem, a liczenie od końca roku służy określeniu jednej daty usunięcia danych dla umów kończących się w danym roku.

- Jeżeli nie dojdzie do zawarcia umowy w przeciągu ..... od złożenia Pani/Panu przez nas oferty, dane osobowe związane z rozmowami o tej umowie zostaną niezwłocznie usunięte z wyjątkiem danych potrzebnych do marketingu bezpośredniego o ile została wyrażona zgoda na przetwarzanie danych w tym celu.
- Dane przetwarzane dla potrzeb marketingu bezpośredniego naszych produktów i usług będą przetwarzane do czasu, aż zostanie zgłoszony sprzeciw względem ich przetwarzania.

Prawo dostępu do danych osobowych:
Posiada Pani/Pan prawo dostępu do treści swoich danych osobowych, prawo do ich sprostowania, usunięcia oraz prawo do ograniczenia ich przetwarzania. Ponadto także prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, prawo do przenoszenia danych oraz prawo do wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych osobowych.

Prawo wniesienia skargi do organu nadzorczego:
Przysługuje Pani/Panu prawo wniesienia skargi do Generalnego Inspektora Ochrony Danych Osobowych (Prezesa Urzędu Ochrony Danych Osobowych, ul. .....) gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

Konsekwencje niepodania danych osobowych:
Podanie przez Panią/Pana danych osobowych jest warunkiem zawarcia umowy, a ich niepodanie będzie skutkowało brakiem możliwości zawarcia powyższej umowy.

Odbiorcy danych:

Dane osobowe mogą zostać ujawnione innym podmiotom; naszym partnerom, czyli firmom, z którymi współpracujemy łącząc produkty lub usługi.

Do danych mogą też mieć dostęp nasi podwykonawcy (podmioty przetwarzające), np. firmy księgowe, prawnicze, informatyczne, likwidatorzy szkód, wykonawcy usług w ramach likwidacji szkód.

Przekazanie danych do państwa trzeciego/organizacji międzynarodowej:

Pani/Pana dane osobowe mogą być przekazywane do państwa trzeciego/organizacji międzynarodowej.

Zautomatyzowane podejmowanie decyzji, profilowanie:
1.Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany i nie będą profilowane.

_____
(data i podpis klienta)

9. Wniosek o udostępnienie danych osobowych.

WNIOSEK O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do.....

.....

(dokładne oznaczenie administratora danych)

2.Wnioskodawca.....

.....

(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy nr ewidencyjny NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych

.....

.....

4. Wskazanie przeznaczenia dla udostępnienia danych:

.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:

.....

6. Zakres żądanych informacji ze zbioru:

.....

.....

.....

7. Informacje umożliwiające wyszukanie w zbiorze danych:.....

.....

.....

(data, podpis)

10. Raport z naruszenia bezpieczeństwa informacji

RAPORT

z naruszenia bezpieczeństwa informacji

w .....

Data naruszenia: .....
(dd.mm.rr)

Godzina naruszenia: .....
(gg:mm)

Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

Zgłoszenie do UODO: ☐ tak ☐ nie

Data zgłoszenia do UODO: .....

Godz. zgłoszenia do UODO: .....

Kategorie osób , których naruszenie dotyczy: ☐ dane zwykłe,

☐ dane podlegające szczególnej ochronie:

Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

Sposób naruszenia:

.....
...

.....

(np. włamanie)

Konsekwencje i straty:

.....

...

.....

(np. ujawnione zostały dane osobowe, adres i miejsce zamieszkania)

Proponowane środki zabezpieczeń :

.....

...

.....

(np. zakup sprzętu IT, szkolenie pracowników)

Zastosowane środki zabezpieczeń :

.....

.....

(np. uniemożliwiono dostęp osobom nieupoważnionym)

7. Postępowanie wyjaśniające:

.....

.....

Zawiadomienie osób, których dane dotyczą

Nie zawiadamiano, gdyż:

☐ ADO wdrożył odpowiednie środki techniczne i organizacyjne,

☐ ADO zastosował działania mające na celu wyeliminowanie ryzyka naruszenia praw i wolności osób,

☐ Zawiadomienie wymagałoby niewspółmiernych środków

Zawiadomiono poprzez:

☐ Wysłano pismo ze szczegółowym wyjaśnieniem,

☐ Opublikowano komunikat w środkach masowego przekazu (gazeta, radio itp.).

....

(data, podpis Inspektor Ochrony Danych) (data, podpis Administrator Danych)

11. Dokumenty powiązane

1) Polityka Bezpieczeństwa Informacji.
2) Polityka Ochrony Danych Osobowych.
3) Instrukcja Postępowania w Sytuacji Naruszeń.
4) Instrukcja Zarządzania Systemem Informatycznym.
5) Analiza i szacowanie ryzyka w bezpieczeństwie informacji.
6) Rejestry utrzymywane na podstawie niniejszej dokumentacji.

.....
(podpis Administratora Danych)