Burmistrz Krobi
63-840 Krobia, ul.Rynek 1

Zarządzenie Nr 29/W/2018

Burmistrza Krobi

z dnia 25 maja 2018r.

w sprawie wdrożenia dokumentacji monitorowania, przetwarzania i reagowania na naruszenia ochrony danych osobowych w Urzędzie Miejskim w Krobi

Na podstawie art.31 oraz art.33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U z 2017 r.,poz.1875 z późn.zm.) , w związku z art.35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) zarządzam , co następuje:

§ 1

1.Wprowadzam do stosowania „Regulamin monitorowania i przetwarzania danych osobowych w Urzędzie Miejskim w Krobi stanowiący załącznik nr 1 do zarządzenia.

2.Wprowadzam do stosowania „Regulamin zabezpieczenia systemów informatycznych w zakresie danych osobowych w Urzędzie Miejskim w Krobi" stanowiący załącznik nr 2 do zarządzenia .

§ 2

1.Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych Osobowych .

2. Zobowiązuję pracowników Urzędu Miejskiego w Krobi do zapoznania się z dokumentami przywołanymi w § 1 zarządzenia.

3.Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy.

§ 3

1.Traci moc zarządzenie nr 3/2015 Burmistrza Krobi z dnia 10 lutego 2015r. w sprawie wprowadzenia „Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie

Miejskim w Krobi „ oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Krobi.

2.Zarządzenie wchodzi w życie z dniem podpisania

Otrzymują :

1)Naczelnicy UM w Krobi

2) WO –a/a

BURMISTRZ
Sebastian Czwojda

Sekretarz Gminy
Katarzyna Szablewska

Załącznik Nr 1 do Zarządzenia nr 29/W/2018

REGULAMIN MONITOROWANIA I PRZETWARZANIA DANYCH OSOBOWYCH w Urzędzie Miejskim w Krobi

§ 1

POSTANOWIENIA OGÓLNE

1. Regulamin monitorowania i przetwarzania danych osobowych w Urzedzie Miejskim w Krobi został napisany na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1)
2. Celem regulaminu jest wskazanie podstaw dla właściwego wykonania obowiązków inspektora danych osobowych w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych.
3. Regulamin określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zbiór reguł i zaleceń , regulujących sposób ich zarzadzania ,monitorowania, ochrony fizycznej, organizacyjnej i informatycznej i przetwarzania w Urzędzie Miejskim w Krobi .

4. Regulamin zawiera zestaw informacji dotyczących szacowania procesów przetwarzania danych osobowych oraz obowiązujących zabezpieczeń technicznych i organizacyjnych, zapewniających właściwą ochronę przetwarzania danych osobowych.

§ 2

DEFINICJE I POJĘCIA ZAWARTE W REGULAMINIE

Wszystkie pojęcia i definicje zawarte w regulaminie znajdują wspólne powiązania za warte w niniejszym dokumencie także są powiązane z innymi dokumentami , które obowiązują w Urzędzie Miejskim w Krobi ,w zakresie ochrony danych osobowych .

1. **INSPEKTOR OCHRONY DANYCH OSOBOWYCH** ten, który decyduje o środkach i celach przetwarzania danych osobowych , wyznaczany przez Burmistrza Krobi.

2. **ADMINISTRATOR DANYCH OSOBOWYCH –burmistrz Krobi**

3. **BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH** – zachowanie integralności, poufności i rozliczalności danych osobowych ; ponadto należy brać pod uwagę inne cechy , w szczególności dostępność, niezawodność.

4. **DANE OSOBOWE** – jest to jakakolwiek informacja , która daje możliwość bezpośrednio lub poprzez inne cechy identyfikację osoby fizycznej ,

5. **DANE BIOMETRYCZNE-** oznaczają dane osobowe , które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej umożliwiają lub potwierdzają jednoznaczną identyfikacje osoby, takie jak wizerunek twarzy lub dane daktyloskopijne

6. **ZGODA-**oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przyzwalające na przetwarzanie danych osobowych osoby która ją wyraziła.

7. **PSEUDONIMIZACJA-** to użycie w miejsce np. imienia i nazwiska rzeczywistej osoby, liczby, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje powinny być przechowywane osobno i objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie określonej osobie fizycznej

8. **PODMIOT PRZETWARZAJĄCY** – oznacza osobę fizyczną lub prawną , organ publiczny , jednostkę lub inny podmiot , który przetwarza dane w imieniu administratora

9. **ODBIORCA-** oznacza osobę fizyczną lub prawną , organ publiczny , jednostkę lub inny podmiot , który ujawnia dane osobowe niezależnie od tego czy jest osobą trzecią

10. **OSOBA TRZECIA-** oznacza osobę fizyczną lub prawną , organ publiczny , jednostkę lub podmiot inny niż osoba , której dane dotyczą

11. **PROFILOWANIE-** dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się

12. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.

13. **INTEGRALNOŚĆ DANYCH** – właściwość zapewniająca pewność ,iż nie dokonano zmiany lub zniszczenia danych w sposób nieautoryzowany,

14. **NARUSZENIE OCHRONY DANYCH OSOBOWYCH** – jest to zamierzone lub niezamierzone naruszenie obowiązujących środków technicznych i organizacyjnych

zastosowanych w celu ochrony danych osobowych . W szczególności , gdy stan urządzenia , zawartość zbioru danych osobowych , ujawnione metody pracy, zasady funkcjonowania oprogramowania i komunikacji w sieci telekomunikacyjnej, które mogą wskazywać na naruszenie ochrony danych osobowych.

15. **POUFNOŚĆ** – jest to właściwość dająca pewność że do danych osobowych ma dostęp wyłącznie osoba upoważniona.

16. **ROZLICZALNOŚĆ** – jest to właściwość zapewniająca ,że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

17. **PRZETWARZANIE DANYCH OSOBOWYCH** – są to jakiekolwiek działania wykonywane na danych osobowych , w szczególności takie jak: pozyskiwanie, gromadzenie, wgląd, przenoszenie, utrwalanie, udostępnianie, usuwanie , a również te , które wykonuje się w systemach informatycznych.

18. **ROZPORZĄDZENIE**- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1)

19. **URZĄD**- Urząd Miejski w Krobi, ul.Rynek 1, 63-840 Krobia .

20. **UŻYTKOWNIK SYSTEMU** – osoba posiadająca upoważnienie, identyfikator, hasło dostępu upoważniające do przetwarzania danych osobowych w systemie informatycznym,

21. **UŻYTKOWNIK ZEWNĘTRZNY** – osoba nie będąca pracownikiem Urzędu Miejskiego w Krobi, posiadająca uprawnienia do przetwarzania danych osobowych w związku z wykonywaniem obowiązków na stanowisku pracy.

22. **WŁAŚCICIEL ZASOBÓW DANYCH OSOBOWYCH** – osoba kierująca komórką organizacyjną, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce . osoba ta jest zobowiązana zastosować wszelkie środki techniczne i organizacyjne zapewniające właściwą ochronę przetwarzanych danych osobowych , stosowną do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych osobowych przed ich udostępnieniem osobie nieupoważnionej, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych , przed nieautoryzowaną zmianą, utratą , uszkodzeniem lub zniszczeniem.

23. **SYSTEM INFORMATYCZNY** – jest to zespół współpracujących urządzeń , programów, procedur związanych z przetwarzaniem danych osobowych oraz narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

§ 3

OBOWIĄZKI INSPEKTORA DANYCH OSOBOWYCH

1.Inspektor zobowiązany jest do podjęcia wszelkich działań , których celem jest zapewnienie prawidłowej ochrony danych osobowych , w szczególności zapewnienie przetwarzania danych ze szczególną starannością .Do jego obowiązków należą:

1.informowanie administratora (lub podmiotu przetwarzającego) oraz pracowników, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach i doradzanie im w tej sprawie;

2.monitorowanie przestrzegania przepisów o ochronie danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3.udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

4.współpraca z organem nadzorczym;

5.pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami.

§ 4

AKTUALIZACJA DOKUMENTACJI ZWIĄZANEJ Z OCHRONĄ DANYCH OSOBOWYCH

1. Niniejszy regulamin oraz wszystkie dokumenty z nim powiązane powinny być aktualizowane wraz ze zmianami w przepisach prawa dotyczącymi ochrony danych osobowych oraz zmianami wynikającymi z organizacji i funkcjonowania Urzędu .

2. W przypadku potrzeby wynikającej ze zdarzeń związanych z naruszeniem ochrony danych osobowych należy dostosować dokumentację do właściwych procedur, które w sposób skuteczny będą chroniły dane osobowe.
3. W każdym przypadku zmiany zapisów niniejszego regulaminu wymagają aktualizacji inne dokumenty powiązane z nim.

§ 5

ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1. Celem właściwej realizacji zamierzeń a także skutecznej ochrony danych osobowych należy stosować następujące obowiązki:

    1) Przeszkolić pracowników uprawnionych do przetwarzania do przetwarzania danych osobowych w zakresie zasad bezpieczeństwa ,
    2) Przypisać użytkownikom określonych cech pozwalających na ich identyfikację w systemach informatycznych , dających możliwość dostęp do przetwarzania danych osobowych odpowiednio do zakresu upoważnienia,
    3) Okresowo kontrolować użytkowników sposób postepowania przy przetwarzaniu danych osobowych,
    4) W przypadku stwierdzonych nieprawidłowości podejmować stosowne działania celem ich wyeliminowanie,
    5) Na bieżąco wdrażać nowe rozwiązania organizacyjne i techniczne , które wzmocnią bezpieczeństwo przetwarzania danych osobowych.

2. W procesie nadzoru należy szczególnie uwzględniać zabezpieczenie w zakresie integralności, poufności oraz rozliczalności przetwarzania danych osobowych.

3. W procesie zarządzania należy stosować działania , które spowodują, że pracownicy , użytkownicy zewnętrzni będą :
    1) Odpowiednio przygotowani i wprowadzeni do przetwarzania danych osobowych ,
    2) Zapoznają się z obowiązującymi procedurami i zasadami przetwarzania danych osobowych w Urzędzie Miejskim w Krobi .
    3) Na bieżąco informowani o wszelkich zmianach w procedurach,

§ 6

DOKUMENTACJA POWIĄZANA Z REGULAMINEM

Na dokumentację powiązaną z procesem bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Krobi składają się:

Lp.	NAZWA DOKUMENTU	ODPOWIEDZIALNY
1.	Upoważnienie do przetwarzania danych osobowych	Inspektor ochronnych danych osobowych
2.	Ewidencja osób upoważnionych do przetwarzania danych osobowych	Inspektor ochronnych danych osobowych
3.	Ewidencja programów stosowanych przez pracowników do	Inspektor ochronnych danych

	przetwarzania	osobowych
4.	Informacja zgodnie z art. 12 RODO	Inspektor ochronnych danych osobowych
5.	Analiza ryzyka	Inspektor ochronnych danych osobowych
6.	Rejestr czynności przetwarzania	Inspektor ochronnych danych osobowych
7.	Ewidencja przenośnych nośników informacji używanych przez pracowników	Inspektor ochronnych danych osobowych
8.	Ewidencja naruszeń danych osobowych wraz z załącznikami	Inspektor ochronnych danych osobowych
9.	Rejestr upoważnień	Inspektor ochronnych danych osobowych
10.	Zgoda na przetwarzanie danych	Inspektor ochronnych danych osobowych

§ 7

ODPOWIEDZIALNOŚĆ INSPEKTORA

1. INSPEKTOR Danych Osobowych jest odpowiedzialny za prawidłowe przetwarzanie danych osobowych i ich ochronę zgodnie z obowiązującymi przepisami prawa. Ponadto jest obowiązany do stosowania odpowiednich procedur zapewniających prawidłowe przetwarzanie danych osobowych , a także za zapewnienie ochrony przed zmianą ,uszkodzeniem zniszczeniem danych osobowych przez nieuprawnioną osobę.

2. Do kompetencji INSPEKTORA należy :
   1) Wyznaczenie Właścicieli zasobów danych osobowych,
   2) Określenie celów o strategii działań w zakresie ochrony danych osobowych,
   3) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych .
   4) Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu
3. Do obowiązków należy:
   1. Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
   2. Zatwierdzanie opracowanej dokumentacji związanej z ochrona danych osobowych w jednostce,
   3. Nadawanie upoważnień pracownikom oraz użytkownikom zewnętrznym do przetwarzania danych osobowych,
   4. Zapewnienie ochrony fizycznej pomieszczeń , w których są przetwarzane dane osobowe,
   5. Zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych oraz nieinformatycznych,
   6. Zapewnienie środków na szkolenia osób funkcyjnych związanych z ochroną danych osobowych,

1) Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych.
2) Nadzór nad zapewnieniem przez Właścicieli zasobów danych osobowych dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w Rozporządzeniu.
3) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn
4) Kontrola oraz sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

§ 9

ODPOWIEDZIALNOŚĆ ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

1. Obowiązki ASI pełni pracownik wyznaczony przez INSPEKTORA ochrony Danych Osobowych.

2. Do zakresu obowiązków Administratora Systemów Informatycznych należy:

1) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych.
2) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
3) Bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe.
4) W przypadku powstania zagrożenia ochrony danych osobowych bezzwłoczne podjęcie stosowanych działań .
5) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych.
6) Analiza raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych.
7) Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą, Rozporządzeniem , Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym .
8) Instalację i konfigurację oprogramowania i sprzętu używanego do przetwarzania danych osobowych.
9) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem.
10) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania.

11) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.
12) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
13) Przyznawanie na wniosek Właściciela zasobów, za zgodą inspektora Danych Osobowych Informacji ściśle określonych praw dostępu do danych osobowych w danym systemie.
14) Udzielanie pomocy w ramach realizacji serwisu dla potrzeb Urzędu .
15) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego.
16) Wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego.
17) Wykonywanie i przechowywanie dokumentacji należącej do kompetencji ASI.
18) Nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.
19) Wspólnie z ABI współdziałanie w wypełnianiu wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F.
20) Współpraca w trakcie kontroli GIODO w zakresie dotyczącym systemu informatycznego.

§ 11

ODPOWIEDZIALNOŚĆ PRACOWNIKÓW I UZYTKOWNIKÓW SYSTEMU

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.

2. Pracownicy oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Inspektora ochrony danych osobowych

3. Pracownicy / użytkownicy zewnętrzni są zobowiązani do:

1) Postępowania zgodnie z regulaminem.

2) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.

3) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

1. Wykonywania niezbędnych działań i w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym celu powinni:

1) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.

2) Informować Inspektora lub pracowników ochrony o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych,

3) Pracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać inspektorowi projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.

§ 12
ODPOWIEDZIALNOŚĆ ZA NARUSZENIE ZASAD OCHRONY DANYCH OSOBOWYCH

1. Art. 83 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) określający odpowiedzialność pracownika w przypadku naruszenia ochrony danych osobowych.

§ 13
SZKOLENIA

1. Przed rozpoczęciem przetwarzania danych osobowych każdy pracownik, stażysta, praktykant powinien zostać przeszkolony przez Inspektora ochrony danych osobowych Szkolenie powinno obejmować następujące zagadnienia:

1) obowiązuję przepisy w zakresie o ochronie danych osobowych,

2) procedury oraz zasady przetwarzania danych osobowych,

3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych .

4) zasady użytkowania oprogramowania , urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

5) rodzaje zagrożeń jakie mogą być związane z przetwarzaniem danych osobowych w systemach informatycznych,
6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
7) Zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego.
8) odpowiedzialność w przypadku naruszenia ochrony danych osobowych.

2. Szkolenia należy przeprowadzać nie rzadziej niż dwa razy do roku ,a także każdorazowo w przypadku osoby nowozatrudnionej , stażystów i praktykantów,

§ 14
ZASADY SZCZEGÓLNEJ STARANNOŚCI

1. Każdy pracownik dla właściwego sposobu i zasad przetwarzania danych osobowych zobowiązany jest do zachowania szczególnej staranności przy przetwarzaniu danych osobowych a w szczególności:

    1) stosowanie wszelkich metod zabezpieczeń wynikających z Polityki,
    2) zabezpieczenie wydruków elektronicznych a także tych , które mogą być tworzone w trakcie kserowania, kopiowania,
    3) udzielanie informacji zawierających dane osobowe tylko osobom, podmiotom uprawnionym,
    4) prowadzenie rozmów telefonicznych w sposób bezpieczny , na zasadzie by osoba nieuprawniona nie pozyskiwała informacji jeżeli nie jest ona dla niej przeznaczona,

§ 15
MIEJSCA I POMIESZCZENIA PRZEZNACZONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe można przetwarzać wyłącznie w miejscach bezpiecznych i będących pod właściwym nadzorem osoby, która przetwarza i nadzoruje przetwarzanie danych osobowych,
2. Pomieszczenia bezpieczne to takie , które nie są pozostawione bez nadzoru odpowiedzialnego pracownika,
    1) pomieszczenie biurowe,
    2) biuro obsługi interesanta,
    3) archiwum ,
    4) pomieszczenie , w którym znajdują się zbiory danych osobowych ,

3. Pomieszczenia , w których są przetwarzane dane osobowe są zamykane na klucz podczas nieobecności osoby upoważnionej/nadzorującej,

4. Obiekt jak i pomieszczenia są zabezpieczone fizycznie zgodnie z obowiązującymi procedurami i potrzebami,

5. W przypadku potrzeby należy zastosować dodatkowe zabezpieczenie fizyczne takie jak: kraty, rolety antywłamaniowe , szczególnie w przypadku pomieszczeń usytuowanych na parterze budynku,

6. Pomieszczenie powinno być wyposażone w sprzęt ppoż.,

7. W przypadku wykonywania prac naprawczych , remontowych , montażowych przez firmy zewnętrzne , pomieszczenie jest pod stałym nadzorem osoby upoważnionej- pracownika urzędu,

8. Przechowywanie kopii zapasowych powinno być realizowane w innym pomieszczeniu niż znajdują się zasoby podstawowe,

9. Każdy pracownik w przypadku zauważenia uchybień w zabezpieczeniu pomieszczenia zobowiązany jest niezwłocznie poinformować o tym fakcie Inspektora danych osobowych

§ 16
UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika upoważnienia do przetwarzania danych osobowych

2. Wzór upoważnienia stanowi załącznik do regulaminu

3. Pracownik , stażysta, praktykant urzędu podpisuje oświadczenie o przeszkoleniu z zakresu obowiązujących przepisów prawa i procedur zawartych w Polityce Bezpieczeństwa,
4. Pracownik po przeszkoleniu podpisuje oświadczenie o zapoznaniu się z przepisami i procedurami, poniżej treści niniejszego regulaminu.

5. Upoważnienie jest przechowywane w aktach osobowych , oraz w dokumentacji Inspektora

§ 17
EWIDENCJA OSÓB UPOWAŻNIONYCH

1. W Urzędzie Miejskim w Krobi prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych ,

2. Ewidencja jest prowadzona przez Inspektora danych osobowych na bieżąco i starannie,

3. Ewidencja zawiera :
   - Imię i nazwisko osoby upoważnionej ,
   - Stanowisko,
   - Data nadania upoważnienia,
   - Data ustania upoważnienia,
   - Zakres upoważnienia,
   - Login/hasło użytkownika,

§ 19
UDOSTĘPNIANIE DANYCH OSOBOWYCH – ZASADY, PROCEDURY

1. Udostępnianie danych osobowych odbywa się na zasadzie potrzeby koniecznej, w przypadku uzyskania zgody na przetwarzanie danych .Klauzula zgody jest załącznikiem do regulaminu.

§ 20
ODMOWA UDOSTĘPNIENIA DANYCH

1. Administrator danych odmawia osobie, której dane dotyczą, udzielenia informacji, jeżeli spowodowałoby to:

   1) ujawnienie wiadomości zawierających informacje niejawne,

   2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,

   3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,

   3) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

§ 21
POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie danych osobowych odbywa się na zasadach określonych Rozporządzeniu 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. z 2016 r. Nr 119, str. 1) i umowie powierzenia danych
2. Powierzenie danych występuje wówczas , gdy podmiot zewnętrzny ma dostęp do danych osobowych przetwarzanych przez Urząd,
3. Administrator danych może powierzyć innemu podmiotowi współpracującemu z Urzędem na zasadzie wynikającej z umowy powierzenia,
4. Wzór umowy powierzenia stanowi załącznik do regulaminu.

§ 22

ZASADY POSTĘPOWANIA W PRZYPADKU NARUSZENIA LUB PODEJRZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

W przypadku naruszenia ochrony danych osobowych , administrator bez zbędnej zwłoki w miarę możliwości , nie później niż terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi nadzorczemu.Art.33 i 55 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) stosuje się odpowiednio. Ewidencja naruszeń stanowi załącznik do regulaminu.

§ 23

PRAWO DO USUNIĘCIA DANYCH OSOBOWYCH

1.Osoba, której dane dotycząc ma prawo do żądania od administratora niezwłocznego usunięcia dotyczących jej danych a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe w przypadku zaistnienia okoliczności o których mowa w art. 17 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne

rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1), który stosuje się odpowiednio.

§ 24

OCHRONA DANYCH OSOBOWYCH W ZBIORACH NIEINFORMATYCZNYCH

1. Zbiory i dane przetwarzane w tych zbiorach to takie dane , które są przetwarzane w formie tradycyjnej bez wykorzystywania systemów informatycznych .

2. Dane osobowe w formie dokumentów i wydruków podlegają ochronie a także odpowiedniemu ich zabezpieczeniu w meblach biurowych zamykanych na klucz.

3. Dokumenty , wydruki podlegające zniszczeniu należy zniszczyć skutecznie, tak by osoba nieuprawniona nie mogła zapoznać się z treścią tych dokumentów lub wydruków.

4. W trakcie niszczenia dokumentów należy przestrzegać przepisów Ustawy o Narodowym Zasobie Archiwalnym i przepisów wykonawczych do ustawy.

§ 26

POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych w regulaminie mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1)

ZAŁĄCZNIKI

1. Załącznik nr 1 –upoważnienie do przetwarzania danych
2. Załącznik nr 2-ewidencja osób upoważnionych do przetwarzania danych osobowych,
3. Załącznik nr 3 – ewidencja programów stosowanych przez pracowników do przetwarzania danych
4. Załącznik nr 4 – Informacja zgodnie z art. 12 RODO
5. Załącznik nr 5 –analiza ryzyka

6. Załącznik nr 6-Rejestr czynności przetwarzania
7. Załącznik nr 7 Ewidencja przenośnych nośników informacji
8. Załącznik nr 8 –ewidencja naruszeń
9. Załącznik nr 9- rejestr upoważnień
10. Załącznik nr 10-zgoda na przetwarzanie danych
11. Załącznik nr 11–umowa powierzenia przetwarzania danych

Załącznik nr 1 do regulaminu

....., dnia ..... 20..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr .....

Niniejszym, zgodnie z art. 5 ust.1 lit f) w zw. z art. 29 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 (dalej RODO),

upoważniam

Panią/Pana: .....

Stanowisko: .....

do przetwarzania danych osobowych w *podać nazwę podmiotu* w następującym zakresie:

A. **Okres upoważnienia**:
   - na okres zatrudnienia */ do dnia ..... włącznie*

B. **Zakres upoważnienia:**
   - dane przetwarzane na nośnikach papierowych:

     .....
   - system informatyczny oraz urządzenia wchodzące w jego skład:

     .....

(bez ograniczeń*, podgląd danych*, wprowadzanie danych*, opracowywanie danych*, zmienianie danych*, usuwanie danych*, na komputerach przenośnych*).

- dane osobowe przetwarzane w ramach udziału w następujących czynności przetwarzania danych:
  a) *podać nazwę czynności (procesu) zgodnie z rejestrem czynności*
  b) .....
  c) .....

.....

Imię, nazwisko i podpis

/zgodnie z zasadami reprezentacji/

*niepotrzebne usunąć

Załącznik Nr 2 do regulaminu

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Krobi.

L.p.	Imię i nazwisko	Stanowisko	Komórka organizacyjna	Data przeszkolenia	Nr upoważnienia imiennego	Identyfikator	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia*

*Zakres upoważnienia:

wgląd	**D**
wprowadzanie	**W**
modyfikacja	**M**
usuwanie	**U**

Załącznik nr 3 do regulaminu –

ewidencja programów wraz z wykazem programów komputerowych i metod zabezpieczenia dostępu do danych

L.p.	Nazwa programu	przeznaczenie	Wersja na dzień	Data przyjęcia do stosowania
3.				

Załącznik Nr 4 do regulaminu

INFORMACJA URZĘDU MIEJSKIEGO W KROBI

–klauzula informacyjna zgodna z RODO (art. 12)

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) od dnia 25 maja 2018 roku
administrator danych : Burmistrz Krobi z siedzibą w Krobi ul.Rynek 1 , 63-840 zgodnie z wymogami przywołanego wyżej rozporządzenia informuje:

• Administratorem danych osobowych klientów jest :
Burmistrz Krobi, ul.Rynek 1, 63-840 Krobia jako organ uprawniony do reprezentacji Gminy Krobia

• Inspektorem Ochrony Danych Osobowych jest Pani Natalia Ratajewska z którą skontaktować się można pod numerem telefonu; 783479791, każdorazowo zgłoszenie powinno być potwierdzone za pośrednictwem poczty elektronicznej e-mail **kas5.bhp@gmail.com**

Z inspektorem można kontaktować w następujący sposób:

-telefonicznie 783479791

- listownie na adres: Rynek 1, 63-840 Krobia

- przez e-mail: **kas5.bhp@gmail.com**

• Podstawą przetwarzania danych osobowych są przepisy prawa w zakresie prowadzonych postępowań administracyjnych lub indywidualne umowy zawirane w trybie zamówień publicznych

• Odbiorcami Danych Osobowych są podmioty przetwarzają ce dane w imieniu Gminy Krobi oraz organy administracji publicznej właściwe do współpracy

• Administrator danych nie przekazuje danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

• Dane osobowe są przechowywane zgodnie z przepisami prawa dotyczącymi archiwizacji dokumentów urzędowych

• Każdemu podmiotowi (klientowi), który udostępnia swoje dane osobowe przysługują następujące prawa związane z przetwarzaniem danych osobowych:

a. prawo wycofania zgody na przetwarzanie danych,

b. prawo dostępu do danych osobowych,

c. prawo żądania sprostowania danych osobowych,

d. prawo żądania usunięcia danych osobowych,

e. prawo żądania ograniczenia przetwarzania danych osobowych,

f. prawo wyrażenia sprzeciwu wobec przetwarzania danych ze względu na T szczególną sytuację – w przypadkach, kiedy przetwarzamy dane na podstawie naszego prawnie uzasadnionego interesu,

g. prawo do przenoszenia danych osobowych, tj. prawo otrzymania od nas danych osobowych, w ustrukturyzowanym, powszechnie używanym formacie informatycznym nadającym się do odczytu maszynowego. Można przesłać te dane innemu administratorowi danych lub zażądać, abyśmy przesłali te dane do innego administratora. Jednakże wykonane zostanie to tylko jeśli takie przesłanie jest technicznie możliwe. Prawo do przenoszenia danych osobowych przysługuje tylko co do tych danych, które przetwarzamy na podstawie umowy lub na podstawie zgody,

Aby skorzystać z powyższych praw, skontaktuj się z nami lub z naszym inspektorem ochrony danych (dane kontaktowe w punktach 1 i 2 powyżej.

• Każdy podmiot (klient), który udostępnia swoje dane osobowe ma prawo do cofnięcia zgody na ich przetwarzanie .Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Zgodę można wycofać poprzez wysłanie oświadczenia o wycofaniu zgody na nasz adres korespondencyjny, nasz adres mailowy.

• Każdy podmiot (klient) , który udostępnia swoje dane osobowe ma prawo do wniesienia skargi do organu nadzorczego- Prezesa Urzędu Ochrony Danych Osobowych.

• Podanie danych osobowych jest warunkiem zawarcia umowy z urzędem oraz prowadzenia postępwoania administracyjnego
•Nieudostępnienie danych osobowych uniemożliwia świadczenie usług oferowanych przez urząd

Załącznik Nr 5 do regulaminu

	Zagrożenie	Skutki	Prawdopodobieństwo wystąpienia	Istotność ryzyka (iloczyn prawdopodobnieństwa i skutku)	Działania zapobiegawcze	Poziom ryzyka
1	Ryzyko naruszenia przez Administratora Danych Osobowych przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1)	Naruszenie przepisów rozporządzenia 3	3	9	Przestrzeganie przepisów , przeszkolenie pracowników	średnie
2	Ryzyko nieuprawnionego fizycznego dostępu do danych osobowych - nieuprawnionego udostępnienia, modyfikacji, wyniesienia, usunięcia danych osobowych przetwarzanych	Naruszenie przepisów rozporządzenia Odpowiedzialność karna 3	4	12	Przestrzeganie wewnętrznych procedur	wysokie
3	Ryzyko nieuprawnionego	Naruszenie przepisów rozporządzenia	2	2	Przestrzeganie wewnętrznyc	niskie

	informatycznego dostępu do danych osobowych, ich modyfikacji lub usunięcia, w wyniku niedostatecznego zabezpieczenia systemu informatycznego jednostki lub w wyniku niedostatecznego zabezpieczenia komóterów i systemów operacyjnych	Odpowiedzialność karna 1			h procedur	
4	Ryzyko naruszenia przez Administratora Danych Osobowych przepisów rozporządzenia parlamentu europejskiego (RODO)w procesie rekrutacji	Naruszenie przepisów rozporządzenia 2	2	4	Wdrożenie i przestrzeganie procedur wewnętrznych	Średnie
5	Ryzyko naruszenia przez Administratora Danych Osobowych przepisów rozporządzenia (RODO)w kontaktach z klientami urzędu	Naruszenie przepisów rozporządzenia 2	3	6		średnie
6	Ryzyko naruszenia przepisów rozporządzenia –monitoring gminy	Naruszenie ochrony danych wizerunku 3	3	9		średnie

Załącznik nr 7 do regulaminu –

ewidencja przenośnych nośników informacji

L.p.	Nazwa nośnika	przeznaczenie	Osoba odpowiedzialna	Zakres czasowy stosowania nośnika

Załącznik nr 8 do regulaminu-**Wzór ewidencji naruszeń ochrony danych**

Wyjaśnienie

Zgodnie z art. 33 ust. 5 RODO, administrator ma obowiązek dokumentowania wszystkich naruszeń ochrony danych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych. Grupa Robocza Art. 29 rekomenduje utworzenie wewnętrznego rejestru naruszeń ochrony danych. Poniżej w formie tabeli podany jest przykładowy zakres informacji, który powinien znaleźć się w rejestrze naruszeń.

1	2	3	4	5	6	7
Administrator (nazwa, adres siedziby)	Jeżeli do naruszenia doszło u podmiotu przetwarzającego - wskazanie nazwy i adresu podmiotu	Data i godzina wystąpienia incydentu prowadzącego do naruszenia	Data i godzina stwierdzenia naruszenia	Miejsce incydentu prowadzącego do naruszenia	Nośniki danych osobowych, których dotyczy naruszenie	Charakter naruszenia ochrony danych (opis incydentu/naruszenia ochrony danych)

8	9	10	11	12	13	14
Kategorie osób, których danych osobowych dotyczy naruszenie	Przybliżona liczba osób, których danych osobowych dotyczy naruszenie	Kategorie danych osobowych, których dotyczy naruszenie	Przybliżona liczba wpisów (rekordów) danych osobowych, których dotyczy naruszenie	Możliwe konsekwencje naruszenia ochrony danych osobowych dla osób fizycznych	Środki zastosowane w celu zaradzenia naruszeniu ochrony danych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków	Ocena ryzyka naruszenia praw i wolności osób fizycznych wynikającego z naruszenia ochrony danych

15	16	17	18	19	20
Czy naruszenie zostało zgłoszone do organu nadzorczego	Jeżeli tak: data i godzina zgłoszenia naruszenia do organu nadzorczego i link do treści zgłoszenia	Jeżeli nie: wyjaśnienie powodów braku zgłoszenia naruszenia do organu nadzorczego	Czy osoby, których dane dotyczą zostały zawiadomione o naruszeniu ochrony danych	Jeżeli tak: sposób i data wysłania zawiadomienia oraz link do jego treści	Jeżeli nie: wyjaśnienie powodów braku zawiadomienia osób, których dane dotyczą

Wzór zawiadomienia osoby, której dane dotyczą, o naruszeniu jej danych osobowych

Urząd Miejski w Krobi, ul.Rynek 1 , 63-840 Krobia
e-mail: krobia@krobia.pl

Pani.....

Zawiadomienie o naruszeniu ochrony Pani danych osobowych

Szanowna Pani,

W ostatnich dniach doszło do incydentu, wskutek którego Pani dane osobowe mogły znaleźć się w posiadaniu osób nieupoważnionych. Poniżej przekazujemy informacje dotyczące tego incydentu, a także działań, jakie w związku z tym podejmujemy. Podajemy też informacje o krokach, które Pani może podjąć w związku z incydentem. Prosimy o uważną lekturę niniejszego zawiadomienia.

Co się stało?

Dnia ... omyłkowo wysłaliśmy wystawioną na Panię fakturę za nasze usługi do innego klienta. Chodzi tutaj o fakturę dotyczącą reprezentowania Pani w postępowaniu sądowym w sprawie o zapłatę przeciwko Budowanie Domów sp. z o.o.

Faktura zawierania następujące dane osobowe dotyczące Pani: imię i nazwisko, numer NIP, adres zamieszkania, informację na temat świadczonych przez nas usług (reprezentowanie w postępowaniu sądowym przeciwko Budowanie Domów sp. z o.o.), oraz kwotę do zapłaty.

Możliwe konsekwencje dla Pani

Wskutek wysłania faktury wystawionej na Pani może dojść do tego, że dostęp do tych danych uzyska osoba nieupoważniona. Osoba ta miałaby więc informacje o Pani imieniu i nazwisku, adresie zamieszkania, numerze NIP, a także informacje o tym, że między Panią a Budowanie Domów sp. zo.o. toczy się sprawa o zapłatę. Ponadto na fakturze widnieje kwota do zapłaty, co może pośrednio dotyczyć Pani zobowiązań finansowych.

Na chwilę obecną nie mamy żadnych sygnałów, że dokument z Pani danymi został gdzieś upubliczniony lub jest wykorzystywany przez osobę niepowołaną. Istnieje jednakże ryzyko, że ktoś będzie próbował wykorzystać Pani dane osobowe w celu podszycia się pod Panią (tzw. kradzież tożsamości). Rozumiemy także, że upublicznienie Pani danych osobowych mogłoby wywołać u Pani stres lub inne negatywne odczucia.

Działania podjęte przez nas

Wysłaliśmy zawiadomienie do naszego klienta, któremu omyłkowo wysłaliśmy fakturę przeznaczoną dla Pani. Wyjaśniliśmy klientowi , że faktura z ostała do niego wysłana omyłkowo i poprosiliśmy o jej

zniszczenie lub odesłanie do nas. Jak tylko otrzymamy odpowiedź od naszego klienta z potwierdzeniem zniszczenia faktury lub jeśli klient odeśle nam fakturę, poinformujemy Panią o tym.

Na bieżąco monitorujemy, czy Pani dane zostały gdzieś upublicznione lub wykorzystane przez osobę nieuprawnioną. Na chwilę obecną nie mamy żadnych sygnałów o takim nieuprawnionym wykorzystaniu Pani danych lub o ich upublicznieniu.

Co może Pani zrobić?

W związku z ryzykiem kradzieży tożsamości, prosimy o ostrożność przy podawaniu Pani danych osobowych innym osobom. Dotyczy to szczególnie podawania danych za pośrednictwem Internetu lub przez telefon.

Jeżeli dowie się Pani o upublicznieniu lub wykorzystaniu Pani danych przez osobę nieuprawnioną, bardzo prosimy o natychmiastowe przekazanie nam tej informacji.

Więcej informacji

Jeżeli ma Pani jakiekolwiek pytania, lub chciałaby nam Pani przekazać dodatkowe informacje w związku z zagubieniem dokumentu z Pani danymi osobowymi, prosimy o kontakt z naszym inspektorem ochrony danych – .....Poniżej podajemy dane kontaktowe inspektora ochrony danych:
- listownie na adres: ul. Urząd Miejski w Krobi, ul.Rynek 1 , 63-840 Krobia
- przez e-mail: krobia@krobia.pl
- telefonicznie: 655711111

Załącznik Nr 9 do regulaminu

Rejestr upoważnień pracowników do przetwarzania danych osobowych w Urzędzie Miejskim w Krobi.

L.p.	Imię i nazwisko	Stanowisko	Data przeszkolenia	Nr upoważnienia imiennego	Numer upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia*

Załącznik nr 10 do regulamiu

Klauzula zgody na przetwarzanie danych osobowych zgodnej z RODO

1. Wyrażam zgodę na przetwarzanie moich danych osobowych przez administratora danych Gminę Krobia z siedzibą w Krobi, ul. Rynek 1, 63-840 Krobia, ... w celu .....

2. Podaję dane osobowe dobrowolnie i oświadczam, że są one zgodne z prawdą.

3. Zapoznałem(-am) się z treścią klauzuli informacyjnej, w tym z informacją o celu i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawiania.

Załącznik nr 11 do regulaminu

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w _____

pomiędzy

_____, zwanym dalej „Administratorem"

a

_____, zwanym dalej „Powierzającym"

1. DEFINICJE

Dla potrzeb niniejszej umowy, Administrator i Przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

1) **Umowa Powierzenia** – niniejsza umowa;

2) **Umowa Główna** – [*umowa, w związku z którą zawierana jest umowa powierzenia – przetwarzanie danych jest konieczne do wykonania Umowy Głównej*]

3) **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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1).

2. OŚWIADCZENIA STRON

Strony oświadczają, że niniejsza Umowa Powierzenia została zawarta w celu wykonania obowiązków, o których mowa w art. 28 RODO w związku z zawarciem Umowy Głównej,

3. PRZEDMIOT UMOWY

3.1. W trybie art. 28 ust. 3 RODO, Administrator powierza Przetwarzającemu do przetwarzania dane osobowe wskazane w pkt 4.1.-4.2. poniżej, a Przetwarzający zobowiązuje się do ich przetwarzania zgodnego z prawem i niniejszą Umową Powierzenia.

3.2. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie Powierzenia, oraz zgodnie z innymi udokumentowanymi poleceniami Administratora, przy czym za takie udokumentowane polecenia uważa się postanowienia Umowy Powierzenia oraz ewentualne inne polecenia przekazywane przez Administratora drogą elektroniczną na adres _____ lub na piśmie.

4. CEL, ZAKRES I CHARAKTER PRZETWARZANIA

4.1. Przetwarzający zobowiązuje się do przetwarzania danych osobowych następujących kategorii osób, których dane dotyczą:

a) _____

b) _____

4.2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje:

a) co do [*kategoria osób*]:

i. _____

b) co do [*kategoria osób*]:

i. _____

4.3. Celem przetwarzania danych osobowych wskazanych w pkt 4.1.-4.2. powyżej jest wykonanie Umowy Głównej, w szczególności _____.

4.4. Przetwarzający zobowiązuje się do przetwarzania danych osobowych w sposób stały. Przetwarzający będzie w szczególności wykonywał następujące operacje dotyczące powierzonych danych osobowych: _____. Dane osobowe będą przez Przetwarzającego przetwarzane w formie elektronicznej w systemach informatycznych oraz w formie papierowej.

4.5. Przetwarzający będzie zbierał/otrzymywał dane osobowe od _____ [*sposób, źródła zbierania danych*].

5. ZASADY POWIERZENIA PRZETWARZANIA

5.1. Przed rozpoczęciem przetwarzania danych osobowych Przetwarzający musi podjąć środki zabezpieczające dane osobowe, o których mowa w art. 32 RODO, a w szczególności:

a) 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, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Przetwarzający powinien odpowiednio udokumentować zastosowanie tych środków, a także uaktualniać te środki w porozumieniu z administratorem,

b) zapewnić, by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora w celach i zakresie przewidzianym w Umowie Powierzenia,

c) prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 ust. 2 RODO i udostępniać go Administratorowi na jego żądanie, chyba że Przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.

5.2. Przetwarzający zapewnia, aby osoby mające dostęp do przetwarzanych danych osobowych zachowały je oraz sposoby zabezpieczeń w tajemnicy, przy czym obowiązek zachowania tajemnicy istnieje również po realizacji Umowy Powierzenia oraz ustaniu zatrudnienia u Przetwarzającego.

6. DALSZE OBOWIĄZKI PRZETWARZAJĄCEGO

6.1. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO.

6.2. W sytuacji podejrzenia naruszenia ochrony danych osobowych, Przetwarzający zobowiązuje się do:

a) przekazania Administratorowi informacji dotyczących naruszenia ochrony danych osobowych w ciągu 24 godzin od jego wykrycia, w tym informacji, o których mowa w art. 33 ust. 3 RODO,

b) przeprowadzenia wstępnej analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą, i przekazania wyników tej analizy do Administratora w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych,

c) przekazania Administratorowi – na jego żądanie – wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 RODO, w ciągu 48 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.

6.3. Przetwarzający zobowiązuje się pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO. W szczególności Przetwarzający zobowiązuje się – na żądanie Administratora – do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą, w ciągu 3 dni od dnia otrzymania żądania Administratora.

6.4. Przetwarzający zobowiązuje się stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.

6.5. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych przez Przetwarzającego, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych danych osobowych, skierowanej do Przetwarzającego, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy.

7. PODPOWIERZENIE PRZETWARZANIA

[*Komentarz: Jeżeli nie przewiduje się możliwości podpowierzenia przetwarzania, należy usunąć postanowienia pkt 7.*]

7.1. Administrator dopuszcza możliwość podpowierzenia przetwarzania powierzonych danych osobowych podwykonawcom Przetwarzającego (tzw. subprocesorom). Jeżeli Przetwarzający zamierza podpowierzyć przetwarzanie danych osobowych swoim podwykonawcom, musi uprzednio poinformować Administratora o zamiarze podpowierzenia oraz o tożsamości (nazwie) podmiotu, któremu ma zamiar podpowierzyć przetwarzanie danych, a także o charakterze podpowierzenia, zakresie danych, celu i czasie trwania podpowierzenia. O ile Administrator nie wyrazi sprzeciwu wobec podpowierzenia w terminie 7 dni od daty zawiadomienia, Przetwarzający uprawniony będzie do dokonania podpowierzenia.

7.2. W przypadku podpowierzenia przetwarzania danych osobowych, podpowierzenie przetwarzania będzie mieć za podstawę umow , na podstawie której podwykonawca

(subprocesor) zobowiąże się do wykonywania tych samych obowiązków, które na mocy niniejszej Umowy Powierzenia nałożone są na Przetwarzającego. Umowa będzie zawarta w tej same formie co niniejsza Umowa Powierzenia.

7.3. Administratorowi będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podwykonawcy (subprocesora). W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia, Przetwarzający poinformuje o tym fakcie Administratora w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.

7.4. Przetwarzający nie może przekazywać powierzonych mu przetwarzania danych osobowych do podmiotów znajdujących się w państwach spoza Europejskiego Obszaru Gospodarczego.

8. AUDYT PRZETWARZAJĄCEGO

8.1. Administrator jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających RODO oraz niniejszej Umowy Powierzenia przez Przetwarzającego, poprzez prawo żądania udzielenia wszelkich informacji dotyczących powierzonych danych osobowych.

8.2. Administrator ma także prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową Powierzenia. Audyty lub inspekcje, o których mowa w zdaniu poprzedzającym, mogą być przeprowadzane przez podmioty trzecie upoważnione przez Administratora.

8.3. Przetwarzający zobowiązuje się niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wydane jemu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

9. ZAKOŃCZENIE POWIERZENIA PRZETWARZANIA

9.1. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Przetwarzający zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie.

10. POSTANOWIENIA KOŃCOWE

_____

_____

_____

Załącznik Nr 2 do Zarządzenia Nr 29/W/2018 z dnia 25 maja 2018r.

REGULAMIN ZABEZPIECZENIA SYSTEMÓW INFORMATYCZNYCH W ZAKRESIE DANYCH OSOBOWYCH

w URZĘDZIE MIEJSKIM W KROBI

§ 1.

POSTANOWIENIA OGÓLNE

1) Regulamin określa zasady , tryb postępowania, które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych,
2) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
3) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
4) zasady i procedury rozpoczynania i kończenia pracy,
5) zasady i częstotliwość tworzenia kopii bezpieczeństwa.
6) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,
7) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
9) zasady postępowania w zakresie komunikacji w sieci komputerowej,
10) regulamin opracowany został zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1)

§ 2.

DEFINICJE

Ilekroć w regulaminie jest mowa o :

1) **rozporządzenie** - 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. z 2016 r. Nr 119, str. 1)
2) **Jednostka** – rozumie się przez to Urząd Miejski w Krobi

3) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) **hasło** - rozumie się przez to ciąg nie mniej niż 8 znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne
6) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
7) **teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
8) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
13) **Inspektor danych osobowych** - rozumie się przez to osobę wyznaczoną przez (kierownika jednostki), nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
14) **Administrator Systemu Informatycznego (ASI), zwanego też Administratorem Systemu** - rozumie się przez to osobę zatrudnioną przez kierownika jednostki, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

15) **użytkownik systemu informatycznego** - rozumie się przez to upoważnioną przez kierownika jednostki , pracownika do przetwarzania danych osobowych w systemie informatycznym , który odbył stosowne szkolenie w zakresie ochrony danych.

§ 3.

ZASADY DOSTĘPU UZYTKOWNIKA DO SYSTEMU

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Inspektora Danych osobowych .

3. Rejestracja, o której mowa w ust. l, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§ 4.

IDENTYFIKATOR

1. Identyfikator składa się z minimum sześciu znaków.

2. W identyfikatorze pomija się polskie znaki diakrytyczne.

3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z Inspektorem nadaje inny identyfikator.

§ 5.

H A S Ł A

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

3. Zmiana hasła powinna następować nie rzadziej niż co 30 dni z zastrzeżeniem § 6.Sytem wymusza zmianę hasła po tym terminie.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§ 6.

WYREJESTROWANIE UZYTKOWNIKA

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek kierownika komórki organizacyjnej.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

3) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
4) zawieszenie w pełnieniu obowiązków służbowych,
5) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§ 7.

ROZPOCZĘCIE PRACY W SYSTEMIE

Rozpoczęcie pracy w systemie odbywa się poprzez:

1) przygotowanie stanowiska pracy,
2) włączenie stacji roboczej,
3) wprowadzenie swojego identyfikatora i hasła.

§ 8.

ZAKOŃCZENIE PRACY W SYSTEMIE

Zakończenie pracy w systemie odbywa się poprzez:

1) zamknięcie aplikacji,
2) odłączenie się od zas obów systemowych,

3) zamknięcie systemu operacyjnego,
4) wyłączenie stacji roboczej.

§ 9.

ZASADY PRACY W SYSTEMIE

1. Zabrania się użytkownikom pracującym w systemie:

1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
3) używania nielicencjonowanego oprogramowania.
4) korzystania z zewnętrznych dysków i urządzeń przenoszących dane nieszyfrowanych

§ 10.

NARUSZENIE BEZPIECZEŃSTWA SYSTEMU

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Inspektora danych osobowych , a w szczególności:

1) naruszenia bezpieczeństwa systemu informatycznego,
2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. Inspektorowi danych osobowych zgłasza się w szczególności przypadki:

1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Inspektora Danych Osobowych , pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,

6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemu jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. Użytkownik sieci i Administrator Systemu w porozumieniu z Inspektorem danych osobowych ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 11.

KOPIE ZAPASOWE

1. Kopie awaryjne tworzy się z następującą częstotliwością:
1) kopie systemu finansowo - księgowego – dwa razy w miesiącu,
2) kopie pozostałe - nie rzadziej niż raz na miesiąc.

2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.

3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych
do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

4. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność
do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia Administratora Systemu do ich zniszczenia.

§ 12.

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.

2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemu nie rzadziej niż raz w tygodniu przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.

4. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

§ 12.

ZASILANIE AWARYJNE

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne .

§ 13.

NAPRAWA, SERWIS URZĄDZEŃ

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Inspektora Danych Osobowych

2. Urządzenia, o których mowa w ust. l przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.

3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.

4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 14.

PRZEGLĄD , KONSERWACJE

1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu doraźnie.

2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na miesiąc .

3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na miesiąc.

§ 15.

BEZPIECZEŃSTWO KOMUNIKACJI

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 16

KOMUNIKACJA WEWNĘTRZNA

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 18.

Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

§ 17.

OZNACZANIE NOŚNIKÓW DANYCH

Nośniki informatyczne zawierające dane osobowe powinny szyfrowane i winny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

§ 18.

BEZPIECZEŃSTWO NOSNIKÓW,URZĄDZEŃ

l. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 20 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.

§ 19.

PRZENOSNY KOMPUTER

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej. Bez zgody pracodawcy

lub osoby upoważnionej nie jest możliwe korzystanie z komputerów przenośnych poza miejscem pracy za wyjątkiem osoby informatyka urzędu.

§ 20.

WYDRUKI

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu. Sporządzenie i odebranie wydruku na drukarkach znajdujących się w na korytarzach urzędu jest możliwe po wcześniejszym wpisaniu hasła celem rozpoczęcia procesu drukowania.

2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie .

§ 21.

ODPOWIEDZIALNOŚĆ

Naruszenie obowiązków wynikających z niniejszego regulaminu oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) podlega sankcjom karnym w szczególności wynikającym z przepisów tego rozporządzenia .

§ 22.

OBOWIĄZKI ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji , którą będą wykorzystywali,

2) zapoznanie użytkowników z treścią regulaminu,
3) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę

danych osobowych w nich przetwarzanych,

4) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,
5) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,
6) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w

tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień ,

6) utrzymanie systemu w należytej sprawności technicznej,
7) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych,
8) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe.

§ 23.

ZABEZPIECZENIE FIZYCZNE AKT I MIENIA URZĘDU (z uwzględnieniem danych osobowych)

1) Akta, pieczątki, inne przedmioty (urządzenia służbowe) powinny być zabezpieczone przed dostępem osób trzecich.

2)Zezwoleń na pozostanie w biurze poza godzinami pracy udziela Sekretarz lub wyznaczony przez niego pracownik Urzędu.

3)Pracownik, który uzyskał zezwolenie pozostania w biurze poza godzinami służbowymi zobowiązany jest zgłosić dyżurującemu pracownikowi obsługi, że po zakończonej pracy opuszcza biuro.

4) Pracownicy są informowani o osobach posiadających klucze do budynku Urzędu. Informacje te stanowią tajemnicę służbową.
5)Pracownik biura obsługi klienta prowadzi ewidencję kluczy.
6) Klucze do biur odbierają pracownicy poszczególnych biur każdego dnia przed rozpoczęciem pracy .Po zakończeniu pracy ostatni wychodzący z biura pracownik zamyka biuro.
7) Pracownik obsługi (sprzątaczka) po zakończeniu sprzątania pomieszczeń zamyka wszystkie biura oddając klucze do Biura obsługi klienta
8)Klucze od drzwi głównych urzędu posiadają osoby upoważnione. W przypadku nieobecności osób upoważnionych każdorazowe przekazanie kluczy jest odnotowywane w ewidencji przez pracownika biura obsługi klienta i zatwierdzane przez sekretarza ,.

9)Klucze do kancelarii tajnej, archiwum zakładowego oraz pomieszczenia, w którym znajduje się serwer podlegają szczególnej ochronie wynikającej z odrębnych przepisów.
10)Dorabianie kluczy do pomieszczeń służbowych wymaga zgody Sekretarza

11)Pracownik korzystający z urządzeń elektrycznych a w szczególności z komputerów, drukarek, kserokopiarek jest zobowiązany odłączyć kabel zasilania urządzenia elektrycznego z wtyczki, każdego dnia po zakończeniu pracy.

12)Pracownik jest zobowiązany do odpowiedniego zabezpieczenia dokumentów każdego dnia po zakończeniu pracy zamkniętych na klucz , nieprzezroczystych szafach i szufladach.(zasada czystego biurka).

W sprawach nieuregulowanych w niniejszym regulaminie mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) stosuje się odpowiednio.