WÓJT GMINY
CZŁUCHÓW

ZARZĄDZENIE NR 11/2022
WÓJTA GMINY CZŁUCHÓW
z dnia 09 luty 2022 r.

w sprawie wprowadzenia Polityki ochrony danych osobowych w Urzędzie Gminy Człuchów

Na podstawie art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz. U. UE.L.2016.119.1) w związku art. 33 ust. 3 pkt ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2022 r. poz. 559) zarządza się co następuje:

§ 1. Wprowadza się w Urzędzie Gminy Człuchów politykę ochronę danych osobowych stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Urzędu Gminy Człuchów do stosowania zasad określonych w polityce ochrony danych osobowych.

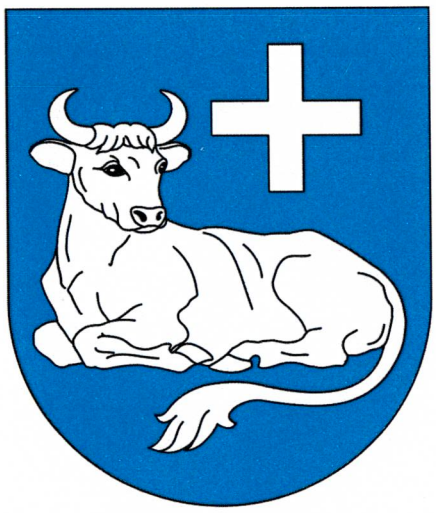
§ 3. Zarządzenie wchodzi w życie z dniem podpisania

WÓJT
Paweł Gibczyński

Załącznik nr 1 do Zarządzenia Nr 11/2022
Wójta Gminy Człuchów z dnia 09 luty 2022 roku

POLITYKA OCHRONY DANYCH OSOBOWYCH

W GMINIE CZŁUCHÓW



Człuchów, luty 2022r.

SPIS TREŚCI

1. Cel polityki ochrony danych

Polityka Ochrony Danych Osobowych została opracowana i wdrożona w strukturze Urzędu Gminy Człuchów w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019r., poz. 1781).

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Polityka ochrony danych osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz struktury Administratora Danych. Polityka ochrony danych osobowych odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego

instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione

Urząd Gminy Człuchów realizując Politykę ochrony danych dokłada szczególnej staranności w celu zabezpieczenia bezpieczeństwa danych osobowych poprzez zapewnienie ich integralności, dostępność, poufności i odporności, w szczególności aby dane te były:

a) przetwarzane zgodnie z prawem;

b) zbierane, w określonym zakresie i czasie dla oznaczonych, zgodnych z prawem celów;

c) merytorycznie poprawne i adekwatne do celów, w jakim są przetwarzane;

d) przetwarzane nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

2. Terminologia

Występujące w Polityce Ochrony Danych Osobowych zwroty oznaczają:

Administrator – jednostka, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (Urząd Gminy Człuchów reprezentowany przez Wójta Gminy Człuchów);

dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

DPIA – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*);

IOD - Inspektor Ochrony Danych;

organ nadzorczy – niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO;

państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego;

podmiot przetwarzający –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych;

Polityka – niniejsza Polityka ochrony danych osobowych;

pracownik – osoba współpracująca z Administratorem na podstawie umowy o pracę lub umowy cywilnoprawnej;

przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;

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);

Unia – Unia Europejska;

Ustawa – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781).

3. Zakres przetwarzanych danych osobowych

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe. procedurach związanych z przetwarzaniem lub ochroną danych osobowych.
2. W Gminie Człuchów prowadzone są następujące rejestry:
    1) Rejestr czynności przetwarzania danych - dla zbiorów danych osobowych, dla których administratorem jest Gmina Człuchów;
    2) Kierownicy referatów są zobowiązani do informowania IOD o planowaniu utworzenia nowego zbioru danych osobowych, który może być wynikiem: - realizacji nowego celu;

    - zidentyfikowania zbioru, który nie został wpisany do rejestru;

- przyjęcia zbioru danych osobowych w wyniku zawarcia umowy powierzenia przetwarzania danych;

3) Tworzenie nowego zbioru w systemie informatycznym może nastąpić po wcześniejszym uzgodnieniu z informatykiem i po akceptacji Administratora.

3. W Urzędzie Gminy Człuchów nie powinny być przetwarzane żadne zasoby danych osobowych, w szczególności zbiory danych osobowych, na które to przetwarzanie nie wyraził zgody Administrator.

4. Ogólne zasady przetwarzania danych osobowych

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:

1) zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),

2) w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),

3) w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),

4) w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),

5) w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),

6) przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),

7) przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),

8) w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).

2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych.

3. Przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy:

    a) Osoba, której dane dotyczą, wyrazi zgodę;

    b) Jest to niezbędne do zrealizowania uprawnień lub spełnienia obowiązku wynikającego z przepisu prawa ciążącego na Administratorze;

    c) Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;

    d) Jest niezbędne do wykonania określonych prawem zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;

    e) Jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą;

    f) Jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

4. Każda z przesłanek wymienionych w ust. 3 jest autonomiczna i może stanowić samodzielną podstawę przetwarzania danych osobowych.

5. Zgoda osoby, której dane dotyczą jest oświadczeniem woli, którego treścią jest zgoda na przetwarzanie danych osobowych w określonym celu, w określonym zakresie, przez określonego administratora danych osobowych. Ponad to Administrator musi być w stanie wykazać, że osoba, której dane dotyczą wyraziła zgodę.

6. Zasady przetwarzania szczególnych danych osobowych określa artykuł 9 Rozporządzenia.

5. Obowiązek informacyjny

1. Motyw 60 preambuły RODO wskazuje nam, że osoba, której dane dotyczą, musi być poinformowana o prowadzeniu operacji przetwarzania i o jego celach. Poza tym administrator powinien podać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

2. W przypadku, gdy zbieramy dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO powinniśmy poinformować ją o:

   a) swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

   b) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;

   c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

   d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

   e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

   f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

3. Poza informacjami, o których mowa w ust. 2, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

   a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

   b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

   c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

   d) informacje o prawie wniesienia skargi do organu nadzorczego (Prezesa Urzędu Ochrony Danych);

   e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do

ich podania i jakie są ewentualne konsekwencje niepodania danych; f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;

4. W przypadku, gdy zbieramy dane osobowe, od innego źródła niż od osoby której dane dotyczą zgodnie z art. 14 ust. 1 i 2 RODO powinniśmy poinformować ją dodatkowo o źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.
5. Powyższe informacje Administrator Danych powinien przekazać w formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej oraz jasnym i prostym językiem w szczególności gdy informacje są kierowane do dziecka (art. 12 ust. 1 RODO),
6. Obowiązek informacyjny możemy spełnić na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jednak jeżeli w treści obowiązku informacyjnego zastosowano znaki, a są one przedstawione elektronicznie, muszą nadawać się do odczytu maszynowego. Dodatkowo spełnienie obowiązku informacyjnego w stosunku do osób musi być wolne od opłat.
7. Klauzule informacyjne, które powinny być stosowane przy zbieraniu danych przygotowuje IOD.
8. Kierownicy referatów w Urzędzie Gminy Człuchów odpowiadają za stosowanie klauzul informacyjnych.

6. Struktura organizacji ochrony danych osobowych

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych,
2. Inspektor Ochrony Danych (IOD),
3. Informatyk (Administrator Systemów Informatycznych),
4. Osoby upoważnione do przetwarzania danych osobowych.

7. Administrator Danych

1. Administrator Danych wyznacza:

A. Inspektora Ochrony Danych - wzór wyznaczenia i dowołania IOD stanowi załącznik nr 12,

B. Administratora Systemów Informatycznych. - wzór wyznaczenia i odwołania ASI stanowi załącznik nr 13.

2. Administrator Danych jest odpowiedzialny za:

a) zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z zasadami przetwarzania danych osobowych określonymi w RODO,

b) wdrożenie procedur ochrony danych osobowych,

c) zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą,

d) prowadzenie rejestru czynności przetwarzania danych osobowych,

e) współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,

f) wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,

g) zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,

h) dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,

i) zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultacje z organem nadzorczym,

j) nadawanie upoważnień do przetwarzania danych osobowych,

k) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

l) zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich.

3. W zakresie Inspektora Ochrony Danych należy:

a) zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,

b) wspieranie IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania,
c) zagwarantowanie by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
d) publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

4. Administrator nadzoruje działania IOD oraz Informatyka oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.
5. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

8. Inspektor Ochrony Danych

1. Funkcję IOD pełni osoba wyznaczona przez Administratora Danych.
2. IOD jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.
3. Zadaniem inspektora ochrony danych jest działanie na rzecz zgodnego z przepisami o ochronie danych przetwarzania danych;
4. Do zadań IOD należy:
    1) Informowanie Administratora, oraz pracowników, którzy przetwarzają dane osobowe na podstawie upoważnienia, o obowiązkach spoczywających na nich na mocy rozporządzenia (RODO) oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tym zakresie;
    2) Monitorowanie przestrzegania przepisów krajowych, rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych;
    3) Podejmowanie działań zwiększających świadomość pracowników poprzez szkolenia personelu uczestniczącego w operacjach przetwarzania;
    4) Prowadzenie okresowych przeglądów stanu zabezpieczenia danych osobowych, audytów i przedstawianie ich wyników Administratorowi;

5) realizacja zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

6) współpraca z organem nadzorczym;

7) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

8) w przypadku incydentu związanego z naruszeniem ochrony danych osobowych pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia (RODO);

9) prowadzenie rejestru czynności;

10) opracowywanie i aktualizacja Polityki, w tym podpisywanie zmodyfikowanych załączników do Polityki oraz ich wdrażanie, w przypadku zaistnienia zmian w Polityce;

11) dokonywanie oceny i szacowania ryzyka celem zastosowania skutecznych metod organizacyjnych i technicznych dla właściwej ochrony danych osobowych u administratora danych osobowych, a w przypadku potrzeby oceny skutków naruszenia ochrony danych osobowych;

12) przygotowywanie do podpisania przez administratora poleceń -upoważnień do przetwarzania danych osobowych;

13)udział w procesach związanych z naruszeniami ochrony danych osobowych, tj.:
- prowadzenie rejestru naruszeń,
- koordynowanie postępowania w sytuacji wykrycia naruszenia (dokumentacja naruszenia, postępowania naprawcze),
- koordynowanie zgłoszenia naruszenia organowi nadzorczemu oraz osobom, których dane dotyczą,

14) opracowywanie unikalnych treści klauzul informacyjnych, klauzul zgód na przetwarzanie danych osobowych, umów powierzenia przetwarzania danych osobowych oraz innych klauzul / postanowień związanych z przetwarzaniem danych osobowych (np. postanowień w zakresie współadministrowania);

15) kontrola podmiotów przetwarzających na polecenie Administratora Danych.

9. Administrator Systemów Informatycznych (Informatyk)

1. Funkcję Administratora systemów informatycznych pełni osoba wyznaczona przez Administratora Danych.
2. Za zabezpieczenie techniczne danych osobowych przetwarzanych w systemie informatycznym odpowiada ASI.
3. Do zdań ASI należy:
   1) zapewnienie wdrożenia wymaganych zabezpieczeń technicznych danych osobowych przetwarzanych w systemach informatycznych;
   2) nadzór nad realizacją oraz aktualizacja postanowień „Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych", stanowiącej Załącznik nr 1 do Polityki;
   3) przekazanie postanowień „Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych" osobom odpowiedzialnym za wykonywanie zadań w niej opisanych;
   4) nadzór nad właściwym funkcjonowaniem systemu informatycznego, w którym przetwarzane są dane osobowe;
   5) nadzór nad rozwiązywaniem sytuacji kryzysowych, pojawiających się w systemie informatycznym,
   6) realizacja decyzji Administratora o dopuszczeniu do eksploatacji systemów informatycznych, osób przetwarzających dane osobowe;
   7) fizyczne nadawanie dostępu do systemu informatycznego osobom upoważnionym do przetwarzania danych osobowych;
   8) usuwanie i modyfikacja uprawnień do dostępu do danych osobowych w systemie informatycznym;
   9) ustalanie i kontrola identyfikatorów dostępu do systemu informatycznego;
   10) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
   11) przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe;

12) przedkładanie do Administratora wniosków dotyczących propozycji zakupu oprogramowania lub sprzętu, w celu realizacji lub podniesienia poziomu bezpieczeństwa systemów informatycznych, bezpieczeństwa kopii zapasowych / bezpieczeństwa nośników pamięci itp.;

13) dokumentowanie zdarzeń, powodujących naruszenia bezpieczeństwa danych osobowych oraz baz danych systemów informatycznych;

14) przekazywanie informacji o nowych programach i systemach informatycznych, serwerach i innych zmianach systemu informatycznego, ważnych ze względu na realizację jego obowiązków, w szczególności do prowadzenia rejestrów czynności;

15) podjęcie niezbędnych i odpowiednich do zagrożeń działań w zakresie zabezpieczenia systemów informatycznych w sytuacji naruszenia ochrony danych osobowych.

3. ASI współpracuje z IOD w zakresie realizacji jego obowiązków, w szczególności poprzez:

1. udział w czynnościach monitorujących ochronę przetwarzania danych osobowych w systemach informatycznych;
2. przekazywanie informacji istotnych w zakresie bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych;
3. opracowywanie opinii dotyczących ochrony danych osobowych w systemach informatycznych.

10. Osoby upoważnione do przetwarzania danych osobowych

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 2 do Polityki.
3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności

karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2020 r., poz. 1320 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.

4. Nadzór nad przestrzeganiem zasad ochrony danych przez osobę upoważnioną realizuje kierownik referatu.
5. Do obowiązków pracowników i innych osób, takich jak stażyści, praktykanci, członkowie zespołów i komisji powołanych przez Administratora, osób realizujących zadania na podstawie umowy cywilno-prawnej, przetwarzających dane osobowe należy:
   1) uczestniczenie w szkoleniach z zakresu ochrony danych osobowych organizowanych przez Administratora;
   2) przetwarzanie tylko tych zasobów danych osobowych, które wynikają z upoważnienia do przetwarzania danych osobowych;
   3) przetwarzanie danych osobowych i ich zabezpieczanie z zachowaniem wszelkich zasad bezpieczeństwa wynikających z właściwych przepisów w zakresie ochrony danych osobowych, RODO, Polityki i innych procedur i instrukcji obowiązujących na terenie Gminy Człuchów;
   4) niezwłoczne informowanie Administratora, IOD oraz Administratora Systemów Informatycznych o sytuacjach podejrzenia naruszenia ochrony danych osobowych;

11. Dopuszczenie osób do przetwarzania danych osobowych

1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3. Upoważnienie do przetwarzania danych osobowych nadawane jest indywidualnie.
4. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera co najmniej takie informacje jak:

- imię i nazwisko osoby upoważnionej,
- zakres upoważnienia,
- data nadania upoważnienia,
- data ustania upoważnienia.

5. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest w formie pisemnej, w tym elektronicznej.
6. Szczegółowa Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych stanowi Załącznik nr 2 do Polityki.

12. Powierzenie przetwarzania danych osobowych

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Wybór podmiotu przetwarzającego powinien być przeanalizowany i uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
    1) przedmiot powierzenia,
    2) czas trwania powierzenia,
    3) charakter i cel przetwarzania,
    4) rodzaj powierzanych danych osobowych,
    5) kategorie osób, których dane dotyczą,
    6) warunki podpowierzenia przetwarzania danych
    7) obowiązki i prawa Administratora Danych,
    8) obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej w tym elektronicznej.

5. Administrator przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym informuje oraz konsultuje z IOD postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych.

13. Udostępnienie Danych Osobowych

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać wskazane w rejestrze czynności przetwarzania danych osobowych.
4. Zabronione jest przetwarzanie danych osobowych, dla których zakres, cel przetwarzania i sposoby przetwarzania nie zostały ustalone przez Administratora, z wyjątkiem danych osobowych wynikających wprost z przepisów prawa.

14. Podejście oparte na ryzyku

1. W zakresie stosowanych rozwiązań odnoszących się do przetwarzania danych osobowych, a w szczególności w zakresie zabezpieczeń, Administrator stosuje zasadę podejścia opartego na ryzyku.
2. Administrator uzależnia sposób realizacji nałożonych na niego obowiązków od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów Administratora.
3. Realizując zasadę podejścia opartego na ryzyku, Administrator Danych:
    1) respektuje to, że RODO szczególny nacisk kładzie na ochronę praw i wolności osób, których dane osobowe są przetwarzane,
    2) dostosowuje środki ochrony danych osobowych do skali ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą,
    3) dokonuje monitorowania i regularnych przeglądów procesów i sposobów organizacji przetwarzania danych osobowych.

4. Zasada podejścia opartego na ryzyku jest procesem ciągłym, wymagającym stałej identyfikacji i szacowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. W strukturze Administratora Danych następuje to, w szczególności poprzez:
    1) przeprowadzanie oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych,
    2) dokonywanie kwalifikacji procesów przetwarzania danych osobowych pod kątem konieczności poddania ich ocenie skutków dla ochrony danych osobowych,
    3) przeprowadzanie oceny skutków dla ochrony danych osobowych,
    4) stosowanie tzw. zasad *privacy by design* i *privacy by default*,
    5) przeprowadzanie audytów zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora,
    6) przeprowadzanie testów równowagi prawnie uzasadnionego interesu Administratora,
    7) stały monitoring otoczenia prawnego mającego wpływ na przetwarzanie danych osobowych przez Administratora Danych (monitoring zewnętrzny),
    8) stały monitoring realizacji wypracowanych założeń w zakresie ochrony danych osobowych w ramach struktury Administratora Danych (monitoring wewnętrzny).
5. Skuteczność wdrożonych środków ochrony danych osobowych jest stale monitorowana i udoskonalana, w szczególności w ramach audytów zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wewnętrznymi.

15. Ocena ryzyka

1. Ocena ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych przeprowadzana jest w sytuacjach, gdy istnieje uzasadnione podejrzenie, że dany proces lub sposób organizacji przetwarzania danych osobowych może nieść za sobą ryzyko naruszenia praw lub wolności osób, których dane dotyczą. W szczególności dotyczy to procesów lub sposobu organizacji przetwarzania danych osobowych, które wiążą się

z zastosowaniem technologii, zarówno nowych jak i tych, które uległy znacznej zmianie w stosunku do ich pierwotnego charakteru lub zastosowania.

2. Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych stanowi Załącznik nr 4 do Polityki.

16. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych osobowych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
    1) stan wiedzy technicznej,
    2) koszt wdrażania,
    3) charakter, zakres, kontekst i cele przetwarzania danych,
    4) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Administrator wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. W szczególności, stosowane środki techniczne i organizacyjne muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. Ogólny opis organizacyjnych i fizycznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 10 do Polityki.
6. Ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 11 do Polityki.

17. Ocena skutków dla ochrony danych

1. Administrator Danych dokonuje oceny skutków dla ochrony danych osobowych w celu opisania przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.
2. Ocena skutków dla ochrony danych osobowych stanowi narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.
3. Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*) stanowi Załącznik nr 5 do Polityki.

18. Test równowagi prawnie uzasadnionego interesu Administratora Danych (*balancing test*)

1. W przypadkach, kiedy Administrator przetwarza lub planuje przetwarzać dane osobowe na podstawie art. 6 ust. 1 lit. f) RODO tj. do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych lub przez stronę trzecią, jest on zobowiązany do przeprowadzenia tzw. testu równowagi (*balancing test*).

2. Prawnie uzasadnione interesy Administratora lub strony trzeciej, mogą być podstawą przetwarzania danych wyłącznie wtedy, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z Administratorem Danych nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.
3. Procedura testu równowagi prawnie uzasadnionego interesu Administratora Danych stanowi Załącznik nr 6 do Polityki.

19. Naruszenia ochrony danych

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań

w przypadku wykrycia naruszenia ochrony danych osobowych są: Administrator, IOD, Administartor Systemów Informatycznych, Kierownicy referatów.

2. Procedura postępowania z incydentami ochrony danych osobowych stanowi Załącznik nr 3 do Polityki.

20. Audyt zgodności przetwarzania danych osobowych.

1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IOD.
2. IOD przeprowadza audyt według opracowanego planu audytów.
3. IOD przygotowuje plan audytów na okres nie krótszy niż kwartał i nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt.
4. W planie audytów uwzględnia się w szczególności:
    1) przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
    2) procesy przetwarzania danych osobowych objęte audytem,
    3) konieczność weryfikacji zgodności przetwarzania danych osobowych z:

A. zasadami przetwarzania danych osobowych,

B. zasadami dotyczącymi zabezpieczenia danych osobowych,

C. zasadami przekazywania danych osobowych innym podmiotom.

5. W toku audytu IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
6. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w formie pisemnej, w tym elektronicznej.
7. IOD przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.
8. Wzór sprawozdania z audytu stanowi Załącznik nr 8 do Polityki.

21. Realizacja praw osób, których dane dotyczą.

1. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:
   - prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
   - prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
   - prawo do sprostowania danych (art. 16 RODO),
   - prawo do usunięcia danych (w tym prawo do bycia zapomnianym) (art. 17 RODO),
   - prawo do ograniczenia przetwarzania (art. 18 RODO),
   - prawo do przenoszenia danych (art. 20 RODO),
   - prawo sprzeciwu (art. 21 RODO),
   - prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi Załącznik nr 7 do Polityki.

22. Ogólne zasady bezpieczeństwa ochrony danych

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.

5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta.*
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka (Załącznik nr 15),* która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym procesie indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.

16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.

23. Przeglądy i aktualizacja Polityki Ochrony Danych

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje IOD. Dokonanie przeglądu Polityki może nastąpić, w szczególności w ramach przeprowadzanego audytu zgodności przetwarzania danych osobowych.
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   - procesów funkcjonujących w strukturach Administratora Danych,
   - obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, IOD dokonuje aktualizacji Polityki w wymaganym zakresie.

24. Załączniki

Załącznik nr 1: Instrukcja Zarządzania Systemem Informatycznym

Załącznik nr 2: Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych

Załącznik nr 3: Procedura postępowania z naruszeniami ochrony danych osobowych

Załącznik nr 3A: Kalkulacja oceny ryzyka naruszenia

Załącznik nr 4: Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych

Załącznik nr 4A: Matryca oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych

Załącznik nr 5: Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*)

Załącznik nr 6: Test równowagi prawnie uzasadnionego interesu (*balancing test*)

Załącznik nr 7: Procedura realizacji praw osób, których dane dotyczą

Załącznik nr 8: Wzór sprawozdania z audytu zgodności przetwarzania danych osobowych

Załącznik nr 9: Procedura kontroli podmiotów przetwarzających

Załącznik nr 10: Ogólny opis organizacyjnych środków bezpieczeństwa

Załącznik nr 11: Ogólny opis technicznych środków bezpieczeństwa

Załącznik nr 12: Wzory wyznaczenia oraz odwołania IOD

Załącznik nr 13: Wzory wyznaczenia oraz odwołania Administratora Systemów Informatycznych

Załącznik nr 14: Zasady retencji danych

Załącznik 15: Polityka czystego biurka

Dokument sporządzono: **Data: 09.02.2022** **Miejsce: Człuchów**	**Administrator Danych** WÓJT ..... *Paweł Gibczyński* *podpis, pieczęć*

Załącznik nr 1 do Polityki Ochrony Danych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Przedmiot Instrukcji

Przedmiotem Instrukcji jest określenie zagadnień związanych z bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych, w szczególności gromadzonych, transmitowanych i przechowywanych w systemach informatycznych, a także sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

Instrukcja określa w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym;
3) stosowane metody i środki uwierzytelnienia oraz procedury, związane z ich zarządzaniem i użytkowaniem;
4) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
5) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania;
6) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt. 5 powyżej;
7) sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
8) udostępnianie danych osobowych;
9) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych;
10) przetwarzanie danych osobowych na laptopach;
11) przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż laptopy.

Procedury nadawania, modyfikacji i anulowania uprawnień do przetwarzania danych osobowych w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Dostęp do systemu informatycznego nadaje użytkownikowi Administrator.
2. Uprawnienia w systemie informatycznym przyznawane użytkownikowi, wynikają z zakresu jego obowiązków i powinny być zgodne z upoważnieniem do przetwarzania danych osobowych.
3. Użytkownikom należy przyznawać minimalne uprawnienia, niezbędne do realizacji zadań, wynikających z ich zakresu obowiązków.
4. Informacja o ustaniu stosunku zatrudnienia lub zakończeniu przez użytkownika wykonywania prac, określonych umową o pracę/umową zlecenia / umową o dzieło / o staż / skutkuje blokowaniem dostępu użytkownikowi do systemu.
5. Konto użytkownika zostaje zablokowane przez Administratora w przypadku wystąpienia incydentu bezpieczeństwa.
6. W przypadku naruszania przez użytkownika zasad pracy w systemie informatycznym, administrator może zablokować konto do czasu wyjaśnienia nieprawidłowości.
7. Prace związane z przetwarzaniem danych osobowych w systemie informatycznym, powinna wykonywać osoba będąca pracownikiem Urzędu Gminy Człuchów, która posiada już nadany identyfikator do pracy w systemie,

Rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym.

1. Przyznanie uprawnień w zakresie dostępu do danych przetwarzanych w systemach informatycznych polega na przypisaniu przez Informatyka w systemie dla upoważnionego użytkownika:
    a) Unikalnego identyfikatora i hasła lub unikalnego identyfikatora;
    b) wprowadzeniu do systemu zakresu dostępnych dla danego użytkownika danych i dopuszczalnych operacji.
2. Każdy z użytkowników systemu posiada własny identyfikator.
3. Ustanowione hasło dostępu, w sposób poufny Informatyk przekazuje użytkownikowi.
4. Hasło ustanowione podczas przyznawania uprawnień użytkownik jest zobowiązany zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.

5. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
6. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła.
7. W przypadku anulowania uprawnień użytkownika jego należy niezwłocznie zablokować w systemie oraz unieważnić hasło użytkownika.
8. Za wdrożenie i nadzór nad przestrzeganiem procedury rejestracji uprawnień użytkowników w systemach odpowiedzialny jest Informatyk.

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

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Zmiana hasła użytkownika następuje nie rzadziej niż co 90 dni.
3. Identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być on przydzielany innej osobie.
4. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
8. Przy wyborze hasła obowiązują następujące zasady:
    a) minimalna długość hasła – 8 znaków;
    b) właściwa złożoność hasła - litery duże i małe oraz cyfry lub znaki specjalne.
9. Zakazuje się stosowania haseł:
    a) będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
    b) analogicznych jak identyfikator,
    c) zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci itp.,

d) stanowiących wyrazy słownikowe lub przewidywalne sekwencje znaków np. 12345678 lub abcdefgh.

10. W systemach umożliwiających zapamiętanie hasła nie należy korzystać z tego ułatwienia.
11. Powyższe reguły w zakresie haseł dotyczą obowiązków użytkownika systemu niezależnie od istnienia lub nie mechanizmów wymuszających (ułatwiających) ich stosowanie.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

Przed rozpoczęciem pracy w systemie informatycznym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora i hasła.

1. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu, zablokowania dostępu poprzez zabezpieczony hasłem wygaszacz ekranu lub zablokowanie, wylogowanie sesji użytkownika, np. poprzez użycie kombinacji klawiszy na klawiaturze komputera:
    a) „Ctrl+Alt+Delete" i wybór polecenia „zablokuj ten komputer" lub „wyloguj";
    b) „logo systemu Windows+L" dla zablokowania komputera.
2. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
3. Ustawienie monitora podczas pracy powinno uniemożliwić podgląd jakimkolwiek osobom nieupoważnionym.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów.
5. Przypadki stwierdzenia nieprawidłowości w zakresie działania systemu należy zgłaszać do Informatyka, który po stwierdzeniu przypadku stanowiącego incydent bezpieczeństwa podejmuje działania zgodnie z „ Procedurą postępowania z naruszeniami ochrony danych osobowych"
6. Zabronione jest podejmowanie działań mogących stanowić zagrożenie dla systemu, w tym:
    a) łamanie haseł;
    b) dokonywanie włamań na konta innych użytkowników;
    c) nieprawne uzyskiwanie dostępu do kont administracyjnych;
    d) zakłócanie działania usług;
    e) omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione);

f) doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty;

g) praca na koncie innego użytkownika.

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

1. W celu zagwarantowania bezpieczeństwa danych przechowywanych w systemie wykonywane są ich kopie zapasowe, tj. kopie bezpieczeństwa oraz archiwalne.
2. Za systematyczne przygotowanie kopii zapasowych odpowiada Informatyk.
   W przypadku części aplikacji ich tworzenie odbywa się automatycznie. Mogą one być również wykonywane okazjonalnie przez użytkowników, w celu zabezpieczenia danych szczególnie istotnych dla działalności podmiotu.
3. Bazy danych, oprogramowanie oraz konfiguracja systemów powinny być zabezpieczone w postaci kopii bezpieczeństwa.
4. Należy wykonywać następujące kopie bezpieczeństwa:
   a) przed dokonaniem zmian w konfiguracji systemów lub oprogramowania;
   b) przed dokonaniem zmian w programach (np. zmiana wersji);
   c) zgodnie z przyjętym harmonogramem.
5. Za wdrożenie i nadzór nad stosowaniem zasad i trybu wykonywania kopii zapasowych odpowiedzialny jest Informatyk.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

I. Kopie zapasowe.

1. Kopie zapasowe należy przechowywać w warunkach gwarantujących brak dostępu do nich osób nieupoważnionych, tj. w zabezpieczonych pomieszczeniach, w sejfach lub szafach zamykanych na klucz.
2. W przypadku wykonywania zabezpieczeń długoterminowych lub na nośnikach zewnętrznych, np. taśmach, płytach CD, DVD nośniki te należy sprawdzać pod kątem ich dalszej

przydatności oraz odtwarzalności.

3. Kopie zapasowe należy usunąć niezwłocznie po upływie okresów przechowywania lub w przypadku ustania ich użyteczności.

II. Elektroniczne nośniki informacji.

1. Dopuszcza się używanie służbowych elektronicznych nośników informacji, zwanych dalej nośnikami, w celu przenoszenia i archiwizowania danych osobowych, w tym płyt DVD, dysków zewnętrznych oraz nośników przenośnych typu pendrive.
2. Należy unikać przechowywania danych osobowych na nośnikach.
3. Zabronione jest używanie nośników do przenoszenia danych osobowych na prywatne komputery lub inne, prywatne urządzenia mogące służyć do przechowywania danych.
4. Nośniki, zawierające dane osobowe, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny.
5. Nośniki, zawierające dane osobowe, podlegają szczególnemu nadzorowi i są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w zamykanych szafach biurowych lub kasetkach.
6. W przypadku zaistnienia okoliczności uzasadniających konieczność wyniesienia nośnika zawierającego dane osobowe poza obszar przetwarzania danych osobowych jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia nośnika przed dostępem osób nieupoważnionych, utratą lub zniszczeniem.
7. Nośniki, zawierające dane osobowe, należy transportować w sposób bezpieczny (nie pozostawić ich w miejscach widocznych np. w samochodach, przypiętych do pasków itp.).
8. Nośniki, 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 osoby upoważnionej przez administratora.

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

1. Oprogramowanie stosowane, wdrażane, modyfikowane, zakupione dla Urzędu Gminy Człuchów może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych oraz powinno spełniać wymagania przepisów z zakresu ochrony danych osobowych.
2. Dozwolone jest jedynie uruchamianie oprogramowania związanego merytorycznie z wykonywaną pracą oraz dopuszczonego przez Informatyka do użytkowania w systemach podmiotu.
3. Korzystanie z zasobów informatycznych poprzez sieć publiczną winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w szczególności firewall-i oraz systemu uwierzytelniania użytkowników szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.
4. W celu ochrony systemów przed szkodliwym oprogramowaniem oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym systemu. Za prawidłowość realizacji powyższego obowiązku odpowiada Informatyk.
5. Sprawdzanie dostępności baz wirusów oprogramowania antywirusowego odbywa się automatycznie. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń.
6. Użytkownicy zobowiązani są do niezwłocznego zgłaszania do informatyka każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów). Informatyk podejmuje działania mające na celu eliminację nieprawidłowości.
7. Programy antywirusowe winny być aktywne cały czas podczas pracy danego systemu.
8. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania szkodliwego oprogramowania najnowszą dostępną wersją programu antywirusowego.
9. Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
10. Zabrania się używania elektronicznych nośników informacji niewiadomego pochodzenia.
11. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia.

12. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania, każdy użytkownik winien zawiadomić informatyka o zaistniałym zdarzeniu.

Udostępnianie danych osobowych.

1. Dane osobowe administrowane w Urzędzie Gminy Człuchów mogą być udostępniane:
   a) osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;
   b) innym osobom i podmiotom w przypadku posiadania przez wnioskującego podstaw do legalnego przetwarzania danych.
2. Udostępnienie danych nie może naruszać praw i wolności osób, których dane dotyczą.
3. W przypadku pojawienia się wątpliwości w zakresie możliwości udostępnienia danych osobowych Administrator zasięga opinii IOD.
4. IOD może wydać opinię negatywną udostępnienia danych, jeżeli może to naruszyć bezpieczeństwo i ochronę danych zgromadzonych w systemie informatycznym.
5. W celu nadzoru nad udostępnianiem danych osobowych przypadki przekazania danych należy odnotowywać w systemach.
6. Dane udostępnione w przychodni przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądy, konserwacje lub naprawy systemów i nośników dokonywane są przez osobę upoważnioną do tego typu czynności.
2. Dopuszcza się realizację czynności określonych w ust. 1 przez specjalistyczne firmy świadczące usługi w tym zakresie; w takim przypadku konieczne jest zawarcie stosownej umowy cywilnoprawnej.
3. Umowy w zakresie świadczenia usług teleinformatycznych wiążące się z przetwarzaniem danych osobowych powinny być traktowane jako powierzenie przetwarzania danych osobowych.
4. Pracownicy firm świadczących usługi, o których mowa w ust. 2 powyżej wykonują zlecone zadania tylko za zgodą Administratora danych oraz pod nadzorem Informatyka.

5. W przypadku zdalnego dostępu do komputera (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez Informatyka lub osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania.
6. Przeglądy i konserwacje wykonywane są cyklicznie oraz w przypadku pojawienia się usterki lub awarii systemów informatycznych.
7. Przeglądy mają na celu weryfikację elementów systemu informatycznego i poprawności ich funkcjonowania.
8. Konserwacje mają na celu utrzymanie systemu.
9. Szczegółowy harmonogram i zakres czynności wynikających z przeglądu i konserwacji dla każdego systemu ustala Informatyk.

Przetwarzanie danych osobowych na komputerach przenośnych.

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
2. Na komputerach przenośnych poza obszarem przetwarzania wskazanym w Polityce, odpowiedzialni za ich bezpieczeństwo są ich użytkownicy i są zobowiązani chronić dane przed dostępem do nich osób nieupoważnionych.
3. Komputery przenośne po zakończonej pracy winny być przechowywane przez użytkownika w warunkach zapewniających ich bezpieczeństwo.
4. W przypadku korzystania z komputerów przenośnych poza obszarem przetwarzania należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby postronne.
5. Podczas transportu komputerów przenośnych wynoszonych poza obszar przetwarzania danych osobowych należy zapewnić ich bezpieczeństwo tj. nie należy ich pozostawiać bez nadzoru w samochodzie (lub innym miejscu).
6. Należy unikać przechowywania na komputerach przenośnych danych osobowych.
7. Komputery przenośne muszą być wyposażone w uaktywniony firewall programowy.
8. W przypadku przetwarzania danych osobowych na komputerach przenośnych baza danych osobowych powinna być szyfrowana, zabezpieczona odpowiednim hasłem.

Przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż komputery.

1. Pracownicy korzystający z teleinformatycznych urządzeń przenośnych, tj. m.in. telefonów służbowych, tabletów, aparatów fotograficznych są zobowiązani chronić dane osobowe zawarte w pamięci tych urządzeń przed dostępem osób nieupoważnionych.
2. Wszelkie dane osobowe wprowadzone do pamięci urządzeń przenośnych powinny być usunięte przed zdaniem urządzenia. Osobą właściwą do ich usunięcia jest pracownik korzystający z danego urządzenia. W przypadku trudności technicznych przy usuwaniu danych osobowych należy kontaktować się z Informatykiem.
3. Kontakt z serwisami zewnętrznymi, dotyczący użytkowanego sprzętu, możliwy jest tylko za pośrednictwem Informatyka.
4. W treści informacji o przyznaniu pracownikowi urządzenia powinny znaleźć się wskazania w zakresie ochrony danych osobowych przetwarzanych przy jego pomocy.

WÓJT
Paweł Gibczyński

Załącznik nr 2 do Polityki Ochrony Danych

Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych

Postanowienia ogólne

Upoważnienia do przetwarzania danych osobowych nadawane są przez Administratora Danych. Administrator Danych może upoważnić konkretną osobę do udzielania w jego imieniu upoważnień do przetwarzania danych osobowych.

1. Osobą odpowiedzialną za administrowanie oraz kontrolę upoważnień do przetwarzania danych osobowych jest IOD oraz kierownik referatu kadr.
2. Osobą odpowiedzialną za informowanie o konieczności nadania upoważnienia do przetwarzania danych osobowych, jego zmiany lub odwołania, jest kierownik referatu kadr.
3. Szczegółowa procedura nadawania upoważnień do przetwarzania danych osobowych, ich zmiany lub odwołania, została wskazana poniżej.

Nadanie upoważnienia

1. W przypadku zatrudnienia nowego pracownika, który w ramach swoich obowiązków służbowych będzie przetwarzał dane osobowe, istnieje konieczność nadania mu stosownego upoważnienia do przetwarzania danych osobowych. To samo tyczy się sytuacji, w której dochodzi do zmiany stanowiska pracownika, która łączy się z uzyskaniem dostępu do danych osobowych.
2. IOD przed nadaniem pracownikowi upoważnienia, organizuje dla niego krótkie szkolenie, podczas którego informuje go o podstawowych aspektach prawnych związanych z ochroną danych osobowych (najważniejsze definicje, odpowiedzialność prawna, obowiązek właściwego zabezpieczenia danych przetwarzanych w formie papierowej oraz w systemach informatycznych).
3. Szkolenie jest przeprowadzone w formie tradycyjnej w siedzibie Administratora Danych lub miejscu przez niego wskazanym, bądź zdalnie.
4. W przypadku szkolenia w formie tradycyjnej:
   4.1 IOD przeprowadza szkolenie w siedzibie Administratora Danych lub miejscu wskazanym przez Administratora Danych,
   4.2 IOD odbiera od osób uczestniczących w szkoleniu podpisy poświadczające ich obecność na szkoleniu.
5. W przypadku szkolenia w formie zdalnej:
   5.1 IOD przesyła upoważnianemu drogą elektroniczną (na służbowy adres email) dane dostępowe do spotkania,
   5.2 jeżeli upoważniany nie posiada służbowego adresu email, dane dostępowe przesyłane są kierownikowi referatu kadr, który jest obowiązany do przekazania danych dostępowych upoważnianemu.
6. Osobie, która ukończyła szkolenie nadawane jest upoważnienie do przetwarzania danych osobowych.
7. Upoważnienie nadawane jest w formie papierowej i przechowywane w dokumentacji pracowniczej.

8. Wydanie każdego upoważnienia jest odnotowywane przez kierownika działu kadr w prowadzonej przez niego ewidencji osób upoważnionych do przetwarzania danych osobowych.

9. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona również przez IOD w postaci elektronicznej.

Zmiana zakresu upoważnienia

1. Zakres nadanego pracownikowi upoważnienia może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań w określonym przedziale czasu.

2. W przypadku zmiany stanowiska pracy łączącej się ze zmianą zakresu danych, które przetwarza pracownik, istnieje konieczność zmiany upoważnienia.

3. Na podstawie otrzymanych informacji IOD zmienia zakres upoważnienia.

4. Zmiana zakresu wydanego upoważnienia jest odnotowywana przez IOD oraz kierownika referatu kadr w prowadzonej ewidencji upoważnień.

Odwołanie upoważnienia

1. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:

   1.1 zmiany stanowiska pracy na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,

   1.2 umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, RODO lub Polityce,

   1.3 rozwiązania stosunku pracy,

   1.4 rozwiązania umowy cywilnoprawnej.

2. Kierownik referatu kadr wysyła do IOD drogą elektroniczną na adres email informację o odwołaniu upoważnienia.

3. Administrator danych odwołuje upoważnienie.

4. Odwołanie upoważnienia następuje poprzez jego wycofanie w ewidencji upoważnień prowadzonej przez IOD.

Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, Wójt Urzędu Gminy Człuchów w Człuchowie (Administrator Danych), na podstawie 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 (Ogólne rozporządzenie o ochronie danych) (RODO), **upoważnia:**

Imię i nazwisko upoważnianej osoby	Zbiory danych objęte zakresem upoważnienia	Data nadania upoważnienia
[imię, nazwisko]	[zbiory danych]	[data nadania upoważnienia] Upoważnienie jest ważne do czasu zakończenia stosunku pracy, stosunku cywilnoprawnego lub odwołania

Osoba upoważniona zobowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, wydanymi na jego podstawie krajowymi aktami wykonawczymi, w szczególności obowiązującej Ustawy o ochronie danych osobowych (Ustawa) i obowiązującymi w strukturze Administratora Danych wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy lub odpowiedzialności cywilnej.

Oświadczenie

Oświadczam, że zapoznałam/em się, w zakresie wynikającym z przydzielonych zadań, z obowiązującymi w odniesieniu do ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w strukturze Administratora Danych (w szczególności z wyciągiem Polityki ochrony danych osobowych). Przyjmuję do wiadomości zawarte w nich obowiązki dotyczące ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub współpracy.

Data i podpis Administratora Danych

Data i podpis upoważnionego

WÓJT
Paweł Gibczyński

Procedura postępowania z naruszeniami ochrony danych osobowych

1. Podmiotami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, są wszyscy pracownicy.
2. Za naruszenie ochrony danych osobowych uważa się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Żeby zaistniało naruszenie ochrony danych osobowych, muszą zostać spełnione łącznie trzy przesłanki:
   3.1 naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Administratora Danych,
   3.2 skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;
   3.3 naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.
4. Wyróżnia się trzy typy naruszeń danych osobowych:
   4.1 naruszenie poufności – polega na ujawnieniu danych osobowych nieuprawnionej osobie (*np. przypadkowe wysłanie danych osobowych do osoby postronnej*),
   4.2 naruszenie dostępności – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych (*np. zgubienie lub kradzież nośnika zawierającego dane osobowe przy braku kopii zapasowej*),
   4.3 naruszenie integralności – polega na zmianie treści danych osobowych w sposób nieautoryzowany (*np. pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „s" na końcu każdego z nich*).
5. Naruszenia mogą dotyczyć zarówno danych osobowych przetwarzanych w formie elektronicznej, jak i papierowej.
6. Pracownik, który powziął wiadomość o złamaniu lub podejrzeniu złamania zasad przetwarzania danych, a w szczególności o sytuacjach udostępnienia danych osobom nieuprawnionym, jest zobowiązany do niezwłocznego (lecz nie później niż w ciągu godziny od zdarzenia) powiadomienia Administratora Danych.

7. Powiadomienie, o którym mowa w pkt 6 powinno zawierać co najmniej następujące informacje:

   7.1 data i miejsce naruszenia,

   7.2 kategorie danych oraz przybliżoną liczbę osób, których dotyczy naruszenie,

   7.3 opis naruszenia,

   7.4 możliwe konsekwencje naruszenia,

   7.5 informacje o ewentualnym podjęciu środków zaradczych.

8. Do czasu powiadomienia Administratora Danych, pracownik:

   8.1 zabezpiecza dostęp do miejsca lub urządzenia,

   8.2 wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,

   8.3 podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

9. Dokonywanie zmian w miejscu naruszenia ochrony danych bez uzyskania zgody Administratora Danych jest możliwe tylko w sytuacji, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

10. Zasady informowania Administratora Danych przez podmiot przetwarzający o naruszeniu ochrony powierzonych mu do przetwarzania danych osobowych, określa zawarta z tym podmiotem umowa powierzenia przetwarzania danych osobowych.

11. Administrator Danych, który wykrył lub został poinformowany o nieprawidłowościach przy przetwarzaniu danych osobowych powinien niezwłocznie zidentyfikować problem, zabezpieczyć dane i przedsięwziąć wszelkie niezbędne kroki, aby uniknąć w przyszłości podobnych zdarzeń. Administrator Danych niezwłocznie powiadamia IOD oraz Informatyka.

12. IOD / Informatyk po otrzymaniu zgłoszenia o naruszeniu dokonuje czynności sprawdzających, w tym w szczególności:

    12.1. ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i zbioru danych,(IOD),

12.2. zabezpiecza oraz utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych, w ramach którego doszło do naruszenia (IOD),

12.3. odbiera wyjaśnienia od osób, które uczestniczyły w naruszeniu oraz innych osób, które merytorycznie odpowiadają za procesy przetwarzania danych, w ramach których doszło do naruszenia (IOD),

12.4. sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych (Informatyk),

12.5. sprawdza sposób działania systemu (w tym również obecność wirusów komputerowych),(Informatyk),

12.6. ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,(IOD/Informatyk),

12.7. dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych w skutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,(Informatyk),

12.8. podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych. (IOD/Informatyk/ADO),

13. Na podstawie informacji uzyskanych w toku czynności sprawdzających, IOD wraz z Administratorem Danych dokonuje kwalifikacji naruszenia. Naruszenie kwalifikowane jest jako:

13.1. nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych,

13.2. skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych,

13.3. skutkujące wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

14. Dokonując oceny ryzyka naruszenia praw lub wolności osób fizycznych IOD bierze pod uwagę następujące kryteria:

14.1. charakter i wrażliwość danych osobowych, których dotyczy naruszenie,

14.2. rodzaj danych osobowych, których dotyczy naruszenie,

14.3. konsekwencje, jakie naruszenie wywołuje względem osoby, których dane dotyczą,

14.4. łatwość identyfikacji osoby, której dane dotyczą,

14.5. charakter podmiotu, któremu zostały ujawnione dane osobowe,

14.6. cechy szczególne osoby, której dane dotyczą, w tym w szczególności czy należy ona do grupy wymagającej szczególnej opieki,

14.7. publiczną dostępność do danych osobowych, których dotyczy naruszenie,

14.8. aktualność i poprawność merytoryczną danych, których dotyczy naruszenie, które to kryteria zostały wskazane w wytycznych przyjętych przez Europejską Radę Ochrony Danych (Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, przyjęte w dniu 3 października 2017 r., ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r., WP250rev.01).

15. Na podstawie wskazanych wyżej w pkt 14 kryteriów, dokonuje się automatycznej kalkulacji ryzyka. Kalkulacja pozwala ustalić, czy naruszenie niesie za sobą ryzyko naruszenia praw lub wolności osób fizycznych i czy to ryzyko jest wysokie. Automatycznej kalkulacji dokonuje się z wykorzystaniem formularza stanowiącego Załącznik nr 3A do Polityki.

16. Każdy przypadek naruszenia, bądź podejrzenia naruszenia ochrony danych osobowych, powinien być poddany dodatkowej, obok automatycznej kalkulacji, analizie. Z tego względu automatyczna kalkulacja ryzyka stanowi jedynie dodatkowe źródło pomocnicze i nie może być samodzielną podstawą podejmowania decyzji.

17. W związku z zastrzeżeniem wskazanym w pkt 16, na ostateczny wynik kwalifikacji naruszenia mają wpływ dodatkowe czynniki indywidualne, uwzględnione przez IOD w toku czynności sprawdzających, w szczególności zaliczymy do nich:

17.1. rodzaj naruszenia,

17.2. ilość danych osobowych,

17.3. cechy szczególne administratora danych,

17.4. liczbę osób fizycznych, na które naruszenie wywiera wpływ,

17.5. okoliczności w jakich doszło do naruszenia,

17.6. stosowane przez Administratora Danych zabezpieczenia danych osobowych, których dotyczy naruszenie.

18. Dokonując kwalifikacji naruszenia, o której mowa w pkt 14 konieczne jest również uwzględnienie:

18.1. powagi zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą oraz

18.2. prawdopodobieństwa wystąpienia tego zdarzenia będącego skutkiem naruszenia.

19. Oceniając ryzyko naruszenia praw i wolności osób, których dane dotyczą, IOD wraz z Administratorem powinien przyjąć perspektywę osób, których dane są przetwarzane i właśnie z tej perspektywy oceniać stopień dotkliwości w przypadku zmaterializowania się zagrożenia.

20. IOD niezwłocznie po dokonaniu czynności sprawdzających sporządza, Protokół z naruszenia ochrony danych osobowych według wzoru, który znajduje się w niniejszym Załączniku.

21. IOD przedstawia Protokół z naruszenia ochrony danych osobowych Administratorowi Danych.

22. Jeżeli naruszenie zostanie zakwalifikowane jako skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych, IOD przygotowuje zgłoszenie naruszenia do organu nadzorczego poprzez wypełnienie odpowiedniego formularza dostępnego na stronie internetowej organu nadzorczego. W zgłoszeniu podaje się następujące informacji:

22.1. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie,

22.2. wskazanie imienia i nazwiska oraz danych kontaktowych IOD lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji,

22.3. opis możliwych konsekwencji naruszenia ochrony danych osobowych,

22.4. wskazanie środków, jakie zostały zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

23. Przygotowane przez IOD zgłoszenie naruszenia, Administrator Danych przekazuje do organu nadzorczego niezwłocznie, lecz nie później niż w ciągu 72 godzin po otrzymaniu Protokołu z naruszenia ochrony danych osobowych, w którym stwierdzone zostało naruszenie. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

24. Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl na 4 sposoby:

24.1. elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl,

24.2. elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP,

24.3. elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl,

24.4. tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

25. Administrator Danych w celu wyjaśnienia sprawy, w zależności od potrzeby, prowadzi korespondencję z organem nadzorczym udzielając wszelkich niezbędnych informacji.

26. Jeżeli naruszenie zostanie zakwalifikowane jako skutkujące wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator Danych informuje osobę, której dane dotyczą, o takim naruszeniu. W szczególności, w skierowanym zawiadomieniu, Administrator Danych podaje osobie, której dane zostały naruszone następujące informacje:

26.1. charakter naruszenia ochrony danych osobowych,

26.2. imię i nazwisko oraz dane kontaktowe IOD lub innego punktu kontaktowego, od którego można uzyskać więcej informacji,

26.3. opis możliwych konsekwencji naruszenia ochrony danych osobowych,

26.4. opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

27. IOD przygotowuje treść zawiadomienia, o którym mowa w pkt 27 oraz rekomenduje formę, w jakiej ma nastąpić zawiadomienie. Komunikat kierowany do osoby, której dane dotyczą musi być jasny i zrozumiały oraz zawierać spójne i logiczne zalecenia dostosowane do konkretnej sytuacji.

28. Zawiadomienie, o którym mowa w pkt 27 nie jest wymagane w następujących przypadkach:

28.1. Administrator Danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

28.2. Administrator Danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

28.3. wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

29. Jeżeli naruszenie danych osobowych ma znamiona przestępstwa, wówczas Administrator Danych informuje odpowiednie organy ścigania.

30. W stosunku do osoby, która zaniedbuje obowiązki związane z ochroną danych osobowych mogą zostać wyciągnięte konsekwencje dyscyplinarne przewidziane Kodeksem Pracy oraz wewnętrznymi regulacjami obowiązującymi w strukturze Administratora Danych.

31. IOD prowadzi rejestr naruszeń ochrony danych osobowych, według wzoru, który znajduje się w niniejszym Załączniku.

Wzór protokołu z naruszenia

PROTOKÓŁ Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH NR .../.....

.....

miejscowość, data

1. Administrator Danych: ...
2. IOD: ...
3. Osoba zgłaszająca naruszenie (*imię, nazwisko, stanowisko*): ...
4. Osoby prowadzące czynności sprawdzające (*imiona, nazwiska, stanowiska*): ...
5. Osoby udzielające informacji na temat naruszenia (*imiona, nazwiska, stanowiska*): ...
6. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (*opcjonalnie, np. podmiot przetwarzający, współadministratora, operator pocztowy itp.*): ...
7. Informacje na temat naruszenia ujawnione w toku czynności sprawdzających:

Data i miejsce naruszenia

...

Kategorie osób, których danych dotyczy naruszenie

potencjalnych pracowników

pracowników / współpracowników

dostawców

kontrahentów

innych osób (*należy określić jakie to osoby*): ...

Kategorie danych osobowych, których dotyczy naruszenie

1) Dane osobowe *zwykłe*

imię

nazwisko

numer telefonu

adres mailowy

adres zamieszkania

adres zameldowania

adres korespondencyjny

PESEL

NIP

inne dane (*należy określić jakie to kategorie danych)*: ...

2) Szczególne kategorie danych osobowych

pochodzenie rasowe lub etniczne

poglądy polityczne

przekonania religijne lub światopoglądowe

przynależność do związków zawodowych

dane genetyczne

dane biometryczne

dane dotyczące zdrowia

seksualność lub orientację seksualną

3) Kategorie danych osobowych podlegające szczególnej ochronie

wyroki skazujące

czyny zabronione lub powiązane środki bezpieczeństwa

Przybliżona liczba osób, których dotyczy naruszenie:

...

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie:

...

Opis naruszenia:

...

Naruszenie polegało na:

zgubienie lub kradzież nośnika/urządzenia

dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

nieuprawnione uzyskanie dostępu do informacji

nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

nieprawidłowa anonimizacja danych osobowych w dokumencie

nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

niezamierzona publikacja

dane osobowe wysłane do niewłaściwego odbiorcy

ujawnienie danych niewłaściwej osoby

ustne ujawnienie danych osobowych

Charakter naruszenia:

naruszenie dotyczące poufności danych

**dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych*

naruszenie dotyczące integralności danych

**dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych*

naruszenie dotyczące dostępności danych

**dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych*

8. Przyczyna naruszenia

wewnętrzne działanie niezamierzone

wewnętrzne działanie zamierzone

zewnętrzne działanie niezamierzone

zewnętrzne działanie zamierzone

9. Ocena naruszenia

Ocena ryzyka z kalkulacji

brak ryzyka

ryzyko

wysokie ryzyko

Końcowa ocena

Naruszenie kwalifikowane jest jako:

nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych

skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych

skutkujące wysokim ryzykiem naruszenia praw lub wolności osób fizycznych

Uzasadnienie

10. Powiadomienie organu nadzorczego

Naruszenie kwalifikowane jest jako:

niewymagające powiadomienia organu nadzorczego

wymagające powiadomienia organu nadzorczego

11. Zawiadomienie osoby, której dane dotyczą

Naruszenie kwalifikowane jest jako:

niewymagające zawiadomienia osoby, której dane dotyczą

wymagające zawiadomienia osoby, której dane dotyczą

12. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

...

13. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

...

14. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

...

15. Załączniki:

Załącznik nr 1 – *Kalkulacja oceny ryzyka naruszenia*

Data i podpis IOD

Otrzymują:

1 x oryginał Administrator Danych

1 x kopia IOD

Wzór rejestru naruszeń ochrony danych osobowych

Lp.	Numer naruszenia	Data i miejsce naruszenia *(dd/mm/rrrr, miejsce)*	Opis naruszenia *(krótki opis naruszenia, w szczególności poprzez odesłanie do sporządzonego Protokołu z naruszenia ochrony danych osobowych)*	Kwalifikacja naruszenia	Zawiadomienie organu nadzorczego *(tak / nie)*	Zawiadomienie osób, których dane dotyczą *(tak / nie)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

WÓJT
Paweł Gibczyński

Załącznik nr 3A do Polityki Ochrony Danych

OCENA RYZYKA NARUSZENIA			
LP	KRYTERIUM	OCENA	UZASADNIENIE
1.	**Charakter i wrażliwość danych** **należy określić, czy dane osobowe, których dotyczy naruszenie mają szczególne znaczenie dla osoby, której dane dotyczą, a ich ujawnienie niesie za sobą poważne konsekwencje np.: dane związane z życiem zawodowym (mniej wrażliwe), dane związane z życiem prywatnym (bardziej wrażliwe). EROD: "ujawnienie imienia i nazwiska oraz adresu danej osoby prawdopodobnie nie wyrządzi jej szkody w normalnej sytuacji. Jednak jeżeli imię i nazwisko oraz adres rodzica adopcyjnego zostaną ujawnione rodzicowi biologicznemu, może mieć to bardzo poważne konsekwencje zarówno dla rodzica adopcyjnego, jak i dziecka"*		
2.	**Rodzaj danych** **należy ocenić rodzaj danych osobowych, których dotyczy naruszenie, także w kontekście kategorii danych osobowych*	dane zwykłe		
		szczególne kategorie danych osobowych		
		dane dotyczące wyroków skazujących i czynów zabronionych		
3.	**Łatwość identyfikacji osoby** **należy ocenić czy osoba / podmiot, który wszedł w posiadanie danych osobowych będzie w stanie dokonać identyfikacji osoby, której dane dotyczą*			
4.	**Konsekwencje** **należy zidentyfikować jakie są konsekwencje naruszenia dla osoby, której dane dotyczą*	Utrata kontroli nad własnymi danymi osobowymi		
		Ograniczenie możliwości realizowania praw z art. 15-22 RODO		
		Ograniczenie możliwości realizowania praw		
		Dyskryminacja		

	Kradzież lub sfałszowanie tożsamości		
	Strata finansowa		
	Naruszenie dobrego imienia		
	Utrata poufności danych osobowych chronionych tajemnicą zawodową		
	Nieuprawnione odwrócenie pseudonimizacji		
	Niemożliwość świadczenie usługi / realizacji umowy		
	inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
	inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
	inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
	inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
	inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
	inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		

5.	**Podmiot niezaufany** **należy określić czy podmiot, który uzyskał / mógł uzyskać dostęp do danych osobowych jest podmiotem niezaufanym (tj. innym niż zaufany)* **podmiot zaufany to taki, z którym Administrator Danych pozostaje w stałych stosunkach, może znać stosowane u niego procedury, historię, inne szczegóły go dotyczące np. podmiot przetwarzający, z którym mamy podpisaną umowę powierzenia przetwarzania danych osobowych*			
6.	**Cechy szczególne osoby** **należy wziąć pod uwagę czy osoby, których danych osobowych dotyczy naruszenie należą do grup osób wymagających szczególnej opieki i / lub można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem Administratora Danych*	osoby starsze (pow. 60 r.ż.)		
		dzieci (pon. 16 r.ż.)		
		osoby niepełnosprawne		
		inne **jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
7.	**Brak publicznej dostępności danych** **należy określić czy dane osobowe, których dotyczy naruszenie nie są dostępne w ogólnodostępnych źródłach informacji np. CEIDG, portale społecznościowe, KRS, strony internetowe*			
8.	**Aktualność danych** **należy określić czy dane osobowe, których dotyczy naruszenie są aktualne oraz poprawne merytorycznie*			

WYNIK KALKULACJI

**niezależnie od wyniku kalkulacji, końcowa ocena naruszenia może się od niego różnić ze względu na dodatkowe czynniki (podnoszące lub obniżające ryzyko) brane pod uwagę przy ustalaniu oceny końcowej naruszenia stanowiącej część Protokołu z naruszenia ochrony danych osobowych*

Brak ryzyka (do 19%)
Ryzyko (20%-49%)
Ryzyko wysokie (50%-100%)

#DZIEL/0!	#DZIEL/0!

WÓJT
Paweł Gibczyński

Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych

1. Administrator Danych jest odpowiedzialny za zapewnienie przeprowadzenia oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych.
2. IOD, na podstawie swojej wiedzy oraz informacji przekazanych mu przez pracowników Administratora Danych przetwarzających dane osobowe, wydaje rekomendacje co do procesów lub sposobów organizacji przetwarzania danych osobowych wymagających przeprowadzenia oceny ryzyka. Wydana przez IOD rekomendacja przekazywana jest do Administratora Danych.
3. Administrator Danych podejmuje ostateczną decyzję o przeprowadzeniu lub nieprzeprowadzeniu oceny ryzyka dla danego procesu lub sposobu organizacji przetwarzania danych osobowych.
4. Za właściwą koordynację oceny ryzyka odpowiada Administrator Danych , który w tym zakresie ścisłe współpracuje z IOD.
5. W ocenie ryzyka biorą udział pracownicy Administratora Danych, którzy posiadają szczegółową wiedzę na temat procesu lub sposobu organizacji przetwarzania danych osobowych, która podlega ocenie.
6. Ocena ryzyka przeprowadzana jest przy wykorzystaniu matrycy, której wzór stanowi Załącznik nr 4A do Polityki.
7. Ocena ryzyka składa się z czterech etapów:
    1. Etap 1 – ustalanie kontekstu dla procesu lub sposobu organizacji przetwarzania danych osobowych, tj. określenie zaangażowanych aktywów,
    2. Etap 2 – ustalanie mechanizmów kontrolnych, tj. wskazanie zabezpieczeń stosowanych w kontekście każdego ze zdefiniowanych aktywów,
    3. Etap 3 – szacowanie ryzyka, tj. określenie prawdopodobieństwa wystąpienia zagrożenia będącego naruszeniem praw lub wolności osób fizycznych, których dane dotyczą, co następuje na podstawie zdefiniowanych w Etapie 2 zabezpieczeń,
    4. Etap 4 – działania zapobiegawcze i korygujące, tj. wskazanie środków naprawczych, w kontekście zagrożeń, w odniesieniu do których występuje prawdopodobieństwo ich urzeczywistnienia.
8. Podczas Etapu 4, tj. szacowania ryzyka, uwzględnia się:
    1. wagę zdefiniowanego zagrożenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą,

2. prawdopodobieństwa wystąpienia określonego zagrożenia będącego naruszeniem.

9. Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy, w ramach której stwierdza się, czy z procesem lub sposobem organizacji przetwarzania danych osobowych wiąże się ryzyko i jaki jest jego stopień.

10. Końcowym wynikiem oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą, jest określenie poziomu ryzyka dla danego procesu lub sposobu organizacji przetwarzania danych osobowych. Poziom ryzyka określa się jako:

    1. brak ryzyka,
    2. niski,
    3. średni,
    4. wysoki.

11. IOD przedkłada Administratorowi Danych przeprowadzoną ocenę ryzyka.

12. Jeżeli w wyniku oceny ryzyka zostało stwierdzone ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych, na podstawie przedłożonej mu oceny, podejmuje ostateczną decyzję w zakresie postępowania z tym ryzykiem. W szczególności, decyzja ta może polegać na zarządzeniu:

    1. modyfikacji (redukcji) ryzyka –. obniżenie poziomu ryzyka poprzez realizację określonych w Etapie 4 działań zapobiegawczych i korygujących,
    2. zachowania (akceptacji) ryzyka – świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w procesie lub sposobie organizacji przetwarzania danych osobowych, pomimo stwierdzonego ryzyka,
    3. unikania ryzyka – unikanie działań, które powodują powstanie określonych zagrożeń, co może wiązać się z koniecznością rezygnacji z danego procesu lub sposobu organizacji przetwarzania danych osobowych,
    4. dzielenia (przeniesienia) ryzyka – wykupienie ubezpieczenia lub scedowanie skutków ryzyka na inny podmiot, co nie będzie stanowiło eliminacji ryzyka niezastosowania się przez Administratora Danych do przepisów RODO.

13. IOD koordynuje wdrożenie działań, o których mowa w pkt 12.1 powyżej.

14. Szacowanie ryzyka należy traktować jako proces ciągły, a ochrona danych osobowych powinna być zapewniona na każdym etapie procesu przetwarzania danych i na każdym etapie funkcjonowania wdrożonego w strukturach Administratora Danych systemu przetwarzania danych osobowych.

WÓJT
Paweł Gibczyński

Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*)

1. Administrator Danych jest odpowiedzialny za zapewnienie przeprowadzenia oceny skutków dla ochrony danych osobowych (*data protection impact assessment*).
2. Za właściwą koordynację DPIA odpowiada IOD.
3. Przeprowadzenie DPIA jest obowiązkowe zawsze, gdy:
    1. dany rodzaj przetwarzania został wskazany w wykazie ustanowionym przez organ nadzorczy jako podlegający wymogowi dokonana oceny,
    2. ze względu na swój charakter, zakres, kontekst i cele, przetwarzanie danych może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
4. IOD dokonuje analizy, czy dany rodzaj operacji będzie podlegał obowiązkowi przeprowadzenia DPIA.
5. Analizie poddawana jest, w szczególności każda operacja (proces) przetwarzania danych osobowych ujawniona w rejestrze czynności przetwarzania Administratora Danych.
6. Niezależnie od powyższego, analizie może zostać poddana każda inna operacja przetwarzania danych osobowych, w tym w szczególności operacja planowana. Taka analiza odbywa się zgodnie z szablonem Analizy planowanej operacji przetwarzania, której wzór znajduje się w niniejszym Załączniku.
7. Administrator Danych jest zobowiązana do poinformowania IOD o planowanym wdrożeniu nowej operacji przetwarzania oraz planowanych zmianach w trwającej operacji przetwarzania.
8. Administrator Danych przekazuje IOD szczegółowe informacje dotyczące operacji poddawanej analizie.
9. W razie konieczności, w toku prowadzonej analizy, IOD konsultuje się z kierownikami działów. W tym zakresie, kierownicy są zobowiązani udzielić wszelkich niezbędnych informacji na temat operacji podlegającej analizie, o której mowa w pkt 4.
10. Jeżeli w toku dokonywania analizy, IOD wskaże, że dany rodzaj operacji przetwarzania został ujawniony w wykazie ustanowionym przez organ nadzorczy jako podlegający wymogowi dokonana oceny, DPIA dla tej operacji przetwarzania przeprowadzana jest obowiązkowo.
11. W przypadkach innych niż wskazane w pkt 10, IOD weryfikuje, czy dany rodzaj operacji może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W tym zakresie bierze pod uwagę, w szczególności, czy planowana operacja wiąże się z:
    1. dokonywaniem ocen lub punktacji,
    2. zautomatyzowanym podejmowaniem decyzji o skutku prawnym lub podobnie znaczącym skutku,
    3. systematycznym monitorowaniem,

4. przetwarzaniem szczególnych kategorii danych lub danych osobowych podlegających szczególnym warunkom przetwarzania,
5. przetwarzaniem danych osobowych na dużą skalę,
6. dopasowywaniem lub łączeniem zbiorów danych,
7. przetwarzaniem danych dotyczącym osób wymagających szczególnej opieki,
8. innowacyjnym wykorzystaniem lub stosowaniem nowych rozwiązań technologicznych lub organizacyjnych,
9. przetwarzaniem uniemożliwiającym osobom, których dane dotyczą, wykonywanie praw, korzystanie z usługi lub realizację umowy.

12. Za operacje mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych uważa się, w szczególności operacje, które spełniają co najmniej dwa ze wskazanych w pkt 11 kryteriów. W niektórych przypadkach, IOD może jednak uznać, że:
    1. przetwarzanie spełniające tylko jedno z kryteriów będzie wymagało przeprowadzenia oceny,
    2. przetwarzanie spełniające dwa lub więcej kryteriów nie będzie wymagało przeprowadzenia oceny.
13. We wskazanych w pkt 12.1 i pkt 12.2 przypadkach, IOD szczegółowo uzasadnia swoje stanowisko, w szczególności powołując się na decyzje organów nadzorczych, wytyczne Europejskiej Rady Ochrony Danych, orzecznictwo, praktykę doktryny lub na własne doświadczenia w tym zakresie.
14. IOD przedkłada Administratorowi Danych analizę, o której mowa w pkt 4.
15. Na podstawie przedstawionej przez IOD analizy, Administrator Danych podejmuje ostateczną decyzję o przeprowadzeniu lub nieprzeprowadzeniu DPIA dla danej operacji przetwarzania.
16. Administrator Danych oraz IOD opracowują wspólnie harmonogram przeprowadzenia DPIA, który wskazuje, w szczególności na:
    1. osoby uczestniczące w dokonywaniu oceny,
    2. datę rozpoczęcia oceny,
    3. przewidywaną datę zakończenia oceny.
17. Dokonując oceny uwzględnia się co najmniej:
    1. opis procesu przetwarzania danych osobowych (operacja i cele przetwarzania, a jeżeli ma to zastosowanie również prawnie usprawiedliwione interesy realizowane przez Administratora Danych),
    2. ocenę niezbędności i proporcjonalności tego przetwarzania
    3. ocenę ryzyka naruszenia praw lub wolności osób fizycznych,
    4. wykaz środków, mających zaradzić ewentualnie stwierdzonemu ryzyku (zabezpieczenia oraz środki i mechanizmy bezpieczeństwa).

18. W przypadku, jeśli przetwarzanie danych osobowych dokonywane jest przy udziale podmiotu przetwarzającego, podmiot ten powinien uczestniczyć w przeprowadzeniu oceny skutków dla ochrony danych oraz udzielać niezbędnych informacji.

19. W sytuacji, w której operacja przetwarzania dotyczy współadministratorów, ich obowiązki powinny zostać dokładnie określone i rozdzielone. DPIA powinna jasno wskazywać, która strona jest odpowiedzialna za stosowanie odpowiednich środków przewidzianych do zaradzenia ryzyku oraz ochrony praw osób, których dane dotyczą.

20. DPIA dokonywana jest z wykorzystaniem narzędzia opracowanego przez francuski organ ochrony danych osobowych, które dostępne jest na stronie internetowej tego organu https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

21. Po przeprowadzeniu DPIA, IOD przedkłada Administratorowi Danych Raport z przeprowadzonej oceny skutków dla ochrony danych osobowych zgodny z wzorem znajdującym się w niniejszym Załączniku.

22. Jeżeli w wyniku oceny zostało stwierdzone prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych, Administrator Danych na podstawie przedłożonego mu Raportu z oceny skutków dla ochrony danych osobowych, podejmuje ostateczną decyzję w zakresie realizacji określonego Planu naprawczego. W szczególności, dotyczy to akceptacji wskazanych w Planie naprawczym środków, które powinny zostać podjęte w celu zaradzenia stwierdzonemu ryzyku bądź jego zminimalizowaniu.

23. Na podstawie Planu naprawczego zatwierdzonego przez Administratora Danych, IOD oraz kierowncy działów ustalają harmonogram wdrożeń środków wskazanych w Planie naprawczym.

24. W sytuacji, w której przeprowadzona ocena wykaże, że przetwarzanie danych powodowałoby wysokie ryzyko, gdyby Administrator Danych nie zastosował środków w celu zminimalizowania ryzyka, przed rozpoczęciem przetwarzania, Administrator Danych konsultuje się z organem nadzorczym w trybie art. 36 RODO.

25. Konsultując się z organem nadzorczym Administrator Danych przedstawia mu:

    1. gdy ma to zastosowanie – odpowiednie obowiązki Administratora Danych, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu,
    2. cele i sposoby zamierzonego przetwarzania,
    3. środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą,
    4. dane kontaktowe IOD,
    5. ocenę skutków dla ochrony danych, o której mowa w pkt 21,
    6. wszelkie inne informacje, których żąda organ nadzorczy.

26. IOD wspiera Administratora Danych w konsultacjach z organem nadzorczym, o których mowa w pkt 24 i 25 powyżej, w szczególności, przy współudziale kierowników działów kompletuje oraz przygotowuje wymagane dokumenty i oświadczenia.

WÓJT
Paweł Gibczyński

Procedura testu równowagi prawnie uzasadnionego interesu Administratora Danych (*balancing test)*

1. Test równowagi polega na porównaniu prawnie uzasadnionych interesów realizowanych przez Administratora Danych w związku z konkretnymi czynnościami przetwarzania danych osobowych z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą.
2. IOD informuje Administratora Danych o konieczności przeprowadzenia testu równowagi dla konkretnego procesu przetwarzania danych osobowych. Administrator Danych podejmuje ostateczną decyzję w zakresie rozpoczęcia realizacji testu równowagi.
3. Test równowagi przeprowadzany jest przez IOD, przy współpracy z Administratorem oraz pracownikami Administratora Danych uczestniczącymi w procesie przetwarzania danych osobowych, który podlega testowi równowagi.
4. Test równowagi składa się z następujących etapów:
   4.1. zidentyfikowanie prawnie uzasadnionych interesów Administratora Danych lub strony trzeciej, realizowanych w związku z przetwarzaniem danych osobowych w określonym celu,
   4.2. zidentyfikowanie interesów lub podstawowych praw i wolności osoby, której dane dotyczą, a które mogą być naruszone przez przetwarzanie danych osobowych,
   4.3. ustalenie, czy przetwarzanie danych osobowych w danych okolicznościach jest konieczne do zrealizowania prawnie uzasadnionego interesu Administratora Danych lub strony trzeciej,
   4.4. dokonanie ważenia interesów Administratora Danych lub strony trzeciej i osoby, której dane dotyczą.
5. Ważenie interesów podczas przeprowadzanego testu równowagi, polega na określeniu, czyje interesy mają charakter nadrzędny. Podczas ważenia interesów uwzględnia się, w szczególności:
   5.1. charakter danych osobowych,
   5.2. kategorie osób, których dane dotyczą,
   5.3. relacje zachodzące pomiędzy Administratorem Danych, a osobą, której dane dotyczą,
   5.4. uzasadnione oczekiwania osób, których dane dotyczą,
   5.5. sposób przetwarzania danych,
   5.6. ewentualne szkody Administratora Danych związane z zaniechaniem przetwarzania,
   5.7. zastosowane środki bezpieczeństwa.
6. IOD wykonuje test równowagi zgodnie ze wzorem wskazanym w niniejszym Załączniku, tj. poprzez uzupełnienie:
   6.1. wzoru *Testu równowagi prawnie uzasadnionych interesów Administratora Danych* - obligatoryjnie,

6.2. wzoru *Załącznika do Testu równowagi prawnie uzasadnionego interesu Administratora Danych* – fakultatywnie, tj. wyłącznie wówczas, gdy IOD uzna, że z uwagi na charakter i sposób przetwarzania danych osobowych w analizowanym procesie, zachodzi potrzeba dodatkowego przeanalizowania stosowanych zabezpieczeń ochrony danych.

7. IOD dokumentuje przeprowadzaną przez siebie analizę oraz wynik testu równowagi.

8. Wynik testu równowagi może być:

8.1. pozytywny dla Administratora Danych tj. interesy osoby, której dane dotyczą nie są nadrzędne wobec interesów Administratora Danych lub strony trzeciej,

8.2. negatywny dla Administratora Danych tj. interesy osoby, której dane dotyczą są nadrzędne wobec interesów Administratora Danych lub strony trzeciej.

9. Wynik testu równowagi jest negatywny dla Administratora Danych w szczególności wówczas, gdy istnieje możliwość zrealizowania tego samego celu bez konieczności przetwarzania danych osobowych lub ograniczając ich przetwarzanie.

10. IOD przekazuje Administratorowi Danych wynik testu równowagi.

11. Jeżeli wynik testu równowagi jest negatywny dla Administratora Danych, wraz z tym wynikiem IOD przekazuje Administratorowi Danych rekomendacje w zakresie dalszego przetwarzania danych osobowych. Rekomendacje mogą dotyczyć, w szczególności:

11.1. wdrożenia odpowiednich środków naprawczych mających wpływ na wzajemne interesy Administratora Danych lub stron trzecich i osoby, której dane dotyczą,

11.2. zmiany podstawy prawnej przetwarzania danych osobowych w procesie,

11.3. zaprzestania przetwarzania danych osobowych w procesie.

12. Na podstawie przedstawionego wyniku testu równowagi Administrator Danych podejmuje decyzję odnośnie do dalszego przetwarzania danych osobowych w procesie.

13. Jeżeli wynik testu równowagi jest negatywny dla Administratora Danych i podjął on decyzję o wdrożeniu rekomendowanych przez IOD odpowiednich środków naprawczych, wówczas za koordynację ich wdrożenia odpowiada Administrator Danych współpracując przy tym z IOD.

14. Po wdrożeniu środków, o których mowa w pkt 13, IOD ponownie przeprowadza test równowagi na zasadach opisanych w niniejszym Załączniku.

15. W przypadkach, kiedy już po przeprowadzeniu testu równowagi, proces przetwarzania uległ znaczącej zmianie w stosunku do jego pierwotnego charakteru i może mieć wpływ na wzajemne interesy Administratora Danych lub strony trzeciej i osoby, której dane dotyczą, test równowagi powinien zostać wykonany ponownie, na zasadach opisanych w niniejszym Załączniku.

TEST RÓWNOWAGI PRAWNIE UZASADNIONEGO INTERESU ADMINISTRATORA DANYCH		
1	**Administrator Danych**	
2	**Imię i nazwisko osoby wykonującej test** *IOD lub inna osoba działająca w imieniu Administratora Danych*	
3	**Ogólny opis operacji przetwarzania** *Należy opisać proces biznesowy w ramach którego będzie dochodziło do przetwarzania danych.*	
Spojrzenie na proces przetwarzania z perspektywy Administratora Danych lub strony trzeciej		
4	**Czy i jaki jest interes jest realizowany przez Administratora Danych lub stronę trzecią? Czy przetwarzanie jest realizowane w ramach interesu społecznego?** *Należy w sposób konkretny opisać na czym polega interes Administratora Danych lub strony trzeciej, przy założeniu, że interes taki musi mieć znaczenie gospodarcze oraz musi być:* *- zgodny prawem (prawem UE i krajowym),* *- jasno i konkretnie wyrażony,* *- być interesem rzeczywistym, (a nie opartym na przypuszczeniach),* *- zgodny z przedmiotem działalności Administratora Danych.* *Interes społeczny występuje wtedy, gdy korzyść z przetwarzania może osiągnąć także społeczeństwo lub określone grupy społeczeństwa.*	☐ tak *(należy wskazać jaki)*: ... ☐ nie
5	**Jakie korzyści wynikają z przetwarzania danych? Jakie ewentualne szkody mogą wyniknąć, jeżeli przetwarzanie danych nie będzie miało miejsca?** *Należy ocenić korzyści wynikające z przetwarzania danych dla Administratora Danych lub strony trzeciej (lub społeczność) oraz ewentualne szkody poniesione przez nich, jeżeli przetwarzanie danych nie będzie miało miejsca.*	

6.	**Czy przetwarzanie danych jest niezbędne?** *Należy ustalić czy przetwarzanie danych osobowych jest faktycznie niezbędne dla osiągnięcia celu Administratora Danych, czy też istnieje inna, mniej ingerująca w prywatność metoda zapewniająca osiągnięcie interesu.* *Niezbędność zachodzi także wtedy, gdy osiągnięcie zakładanego interesu bez przetwarzania danych wiązałoby się z niewspółmiernym wysiłkiem czasem lub kosztami.*	☐ tak (*należy określić na czym polega*): ... ☐ nie
	Spojrzenie na proces przetwarzania z perspektywy osoby, której dane dotyczą	
7.	**Jakie prawa i wolności / interesy występują po stronie osoby, której dane dotyczą?** *Należy opisać jaki jest interes, po stronie osoby, który wymaga ochrony danych osobowych lub jakie są prawa i wolności po stronie osoby, które wymagają ochrony.* *Takimi prawami, będą w szczególności prawa zagwarantowane w Karcie Praw Podstawowych UE, Europejskiej Konwencji Praw Człowieka, Konstytucji.*	
8.	**Jaka relacja zachodzi między Administratorem Danych, a osobą, której dane dotyczą?** *Należy określić, jaka relacja łączy Administratora Danych z osobą, której dane dotyczą, w szczególności może to nastąpić poprzez określenie kategorii osób, których dane są przetwarzane (kandydat do pracy, który wysłał swoje dokumenty aplikacyjne, pracownik, współpracownik, osoba, która wyraziła zgodę na otrzymywanie informacji handlowych, klient z aktywną umową, uśpiony klient, etc.).* *Jeśli wskazano więcej niż jedna kategorię osób, których dane dotyczą, należy w przybliżeniu procentowo oszacować udział każdej z kategorii.*	☐ tak (*określić jaka relacja*): ... ☐ brak relacji

9.	**Czy osoba, której dane dotyczą spodziewa się, że jej dane będą przetwarzane w tym celu?** *Należy ocenić czy w świetle rozsądnych oczekiwań osoba może się spodziewać przetwarzania jej danych.*	☐ tak *(opis z czego to wynika)*: ... ☐ nie	
10.	**Czy osoba, której dane dotyczą ma kontrolę nad przetwarzanymi danymi?** *Należy określić w jaki sposób osoba jest informowana o swoich prawach oraz w jaki następuje realizacja każdego ze wskazanych praw:*	☐ tak *(należy wskazać poniżej):* - prawo dostępu do danych: ... - prawo do sprostowania: ... - prawo do usunięcia: ... - prawo do ograniczenia przetwarzania: ... - prawo do sprzeciwu: ... ☐ nie *(powód braku kontroli): ...*	
11.	**Czy przetwarzane dane będą dotyczyły osób wymagających szczególnej opieki?**	☐ dzieci (*należy określić wiek*): ... ☐ osoby starsze ☐ osoby niepełnosprawne ☐ inne (*należy określić jakie*): ... ☐ nie	
12.	**Jaki rodzaj danych osobowych będzie przetwarzany?** *Należy wskazać jakie kategorie danych będą przetwarzane, tj.: dane zwykłe, szczególne kategorie danych (art. 9 RODO) lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych (art. 10 RODO).*	Dane zwykłe: ☐ imię ☐ nazwisko ☐ adres zamieszkania ☐ adres prowadzenia działalności gospodarczej ☐ adres email ☐ data urodzenia ☐ PESEL ☐ NIP ☐ inne *(należy określić jakie): ...*	Szczególne kategorie danych: ☐ pochodzenie rasowe lub etniczne ☐ poglądy polityczne ☐ przekonania religijne lub światopoglądowe ☐ przynależność do związków zawodowych ☐ dane genetyczne ☐ dane biometryczne ☐ dane dotyczące zdrowia ☐ seksualność lub orientacja seksualna Dane osobowe dotyczą: ☐ wyroków skazujących ☐ czynów zabronionych lub powiązanych środków bezpieczeństwa
Organizacja przetwarzania danych osobowych			

13.	**Jak duża jest planowana skala przetwarzania?** *Należy określić jaka jest skala przetwarzania danych.*	Szacowana liczba osób, których dane dotyczą: ...
		Szacowana liczba rekordów przetwarzanych danych: ...
		Szacowana ilość osób mających dostęp do przetwarzanych danych: ...
14.	**W jaki sposób dane będą przetwarzane?** **Należy wskazać czy dane będą przetwarzane w sposób zautomatyzowany i wykorzystywane 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.* *** Należy wskazać czy w ramach przetwarzania danych będzie dochodziło do podejmowania decyzji, opierających się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołujących wobec osoby, której dane dotyczą skutki prawne lub w podobny sposób istotnie na nią wpływających.* **** Należy wskazać czy w ramach planowanej operacji przetwarzania wykorzystywane będą innowacyjne rozwiązania technologiczne lub organizacyjne (np. takie jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu, obserwacja, monitorowanie lub kontrolowanie osób, których dane dotyczą etc.).* ***** Dot. np. przypadku zamieszczania danych na ogólnodostępnych stronach www.*	Profilowanie*: ☐ tak *(należy opisać w jaki sposób)* ☐ nie
		Zautomatyzowane podejmowanie decyzji**: ☐ tak *(należy opisać w jaki sposób)* ☐ nie
		Innowacyjne rozwiązania technologiczne lub organizacyjne***: ☐ tak (*należy wskazać jakich*): ... ☐ nie
		Ujawnianie wielu osobom lub publikacja****: ☐ tak (*należy wskazać jaki sposób*): ... ☐ nie
15.	**Czy w przetwarzaniu danych będą brały udział inne podmioty?** *Należy wskazać czy dane osobowe będą (mogą być) przekazywane innym podmiotom, a jeżeli tak, to jakie to będą kategorie podmiotów i cel przekazania.* *Należy wskazać czy będzie dochodziło do współadministrowania danymi osobowymi w rozumieniu art. 26 RODO.*	Przekazywanie danych: ☐ w ramach grupy Administratora Danych *(należy określić kategorie odbiorców oraz cel)*: ... ☐ podmiotom upoważnionym do otrzymania danych na podstawie przepisów prawa *(należy określić kategorie odbiorców oraz cel): ...* ☐ innym podmiotom zewnętrznym (w ramach EOG) *(należy określić kategorie odbiorców oraz cel): ...* ☐ innym podmiotom zewnętrznym (poza EOG) *(należy określić kategorie odbiorców oraz cel): ...*
		Współadministrowanie: ☐ tak ☐ nie

16	**Czy i w jaki sposób określono okresy retencyjne?** *Należy określić szacunkowy czas przetwarzania danych osobowych*	Szacowany czas przetwarzania danych wynosi: ...
17	**Jakie będą stosowane środki zabezpieczeń organizacyjnych, fizycznych i technicznych?** *Należy określić konkretne środki zabezpieczeń stosowane w odniesieniu do przetwarzania danych w procesie którego dotyczy Test, np.: wdrożenie określonych Polityk Ochrony Danych, szkolenia pracowników, szyfrowanie danych, itp.* *W przypadku, gdy istnieje już dokument opisujący stosowane środki zabezpieczeń, należy powołać się na ten dokument podając jego pełną nazwę oraz (gdy to możliwe) datę wdrożenia.* **Zalecane w odniesieniu do:* *- złożonych procesów przetwarzania danych, w tym takich w których stosowane są zaawansowane rozwiązania technologiczne lub organizacyjne (np. pkt. 14 powyżej),* *- procesów w których przetwarzane są dane na dużą skalę,* *-procesów w których przetwarzane są szczególne kategorie danych lub dane dotyczące wyroków skazujących i czynów zabronionych.*	Środki zabezpieczeń organizacyjnych ☐ tak (*należy wskazać jakie, w tym poprzez odwołanie się do określonych procedur*): ... ☐ brak
		Środki zabezpieczeń technicznych ☐ tak (*należy wskazać jakie, w tym poprzez odwołanie się do określonych procedur*): ... ☐ brak
		Środki zabezpieczeń fizycznych ☐ tak (*należy wskazać jakie, w tym poprzez odwołanie się do określonych procedur*): ... ☐ brak
		(*opcjonalnie*) Załącznik nr 1 – *Opis stosowanych zabezpieczeń** ☐ tak ☐ nie (*brak potrzeby*)
18	**Czy zastosowano dodatkowe środki ochronne?** *W oparciu o wytyczne z Opinii Grupy Roboczej art. 29 ds. Ochrony Danych nr. 6/2014 z dnia 9 kwietnia 2014 r. w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46*	☐ minimalizacja danych (*wskazać w jaki sposób np. poprzez ograniczenie ilości zbieranych danych do minimum, natychmiastowe usunięcie danych po ich wykorzystaniu*): ... ☐ łatwo dostępny mechanizm *opt-out* ☐ bezpośredni dostęp do danych (za pośrednictwem udostępnionych narzędzi IT) ☐ zwiększona przejrzystość przetwarzania np. poprzez stosowanie symboli graficznych ☐ oddzielenie funkcjonalne danych

	Podsumowanie	
19.	**Czy interes lub podstawowe prawa i wolności osoby, której dane dotyczą są nadrzędne wobec interesu Administratora Danych lub strony trzeciej?** *Udzielając odpowiedzi należy wziąć pod uwagę całokształt okoliczności przetwarzania wynikający z udzielonych w Teście odpowiedzi.* *Odpowiedź "tak" oznacza, że Administrator Danych nie może zastosować przesłanki prawnie uzasadnionego interesu z art. 6 ust. 1 lit. f RODO.* *Należy zaznaczyć odpowiedź "tak" zawsze wtedy, gdy osoba której dane dotyczą jest dzieckiem.*	☐ tak ☐ nie Uzasadnienie: ...
20.	**Czy Administrator Danych może przetwarzać dane osobowe w ramach opisanej operacji przetwarzania na podstawie art. 6 ust. 1 lit. f RODO?**	☐ tak ☐ nie Uzasadnienie: ...
21.	**Rekomendacje** *Jeżeli wynik testu równowagi jest negatywny dla Administratora Danych należy określić rekomendacje w zakresie dalszego przetwarzania danych osobowych.* *Rekomendacje mogą dotyczyć w szczególności:* *- wdrożenia odpowiednich środków naprawczych mających wpływ na wzajemne interesy Administratora Danych lub stron trzecich i osoby, której dane dotyczą,* *- zmiany podstawy prawnej przetwarzania danych osobowych w procesie,* *- zaprzestania przetwarzania danych osobowych w procesie.*	
Załącznik (opcjonalnie): 1) Opis stosowanych zabezpieczeń		
		.... Data i podpis

Wzór (*opcjonalnego*) Złącznika do Testu równowagi prawnie uzasadnionego interesu Administratora Danych

OPIS STOSOWANYCH ZABEZPIECZEŃ		
I. ZABEZPIECZENIA ORGANIZACYJNE		
1.	**Imię, nazwisko oraz stanowisko osoby udzielającej odpowiedzi na pytania** *Ta część powinna zostać uzupełniona przez osobę (osoby) posiadającą wiedzę na temat stosowanych zabezpieczeń organizacyjnych ochrony danych osobowych*	
2.	**Czy wyznaczono osobę odpowiedzialną za ochronę danych osobowych** *Należy wskazać, czy w strukturze Administratora Danych wyznaczono osobę odpowiedzialną za ochronę danych osobowych*	☐ wyznaczono Inspektora Ochrony Danych ☐ wyznaczono inną osobę (*należy wskazać jaką*): ... ☐ brak
3.	**Kompetencje osoby odpowiedzialnej za ochronę danych osobowych** *Należy wskazać, jakie kompetencje ma osoba odpowiedzialna za ochronę danych osobowych w strukturze Administratora Danych*	☐ doświadczenie zawodowe w obszarze ochrony danych osobowych, lata doświadczenia ... ☐ wykształcenie kierunkowe (np. prawnicze, informatyczne) (*jakie*): ... ☐ studia podyplomowe w zakresie ochrony danych osobowych ☐ studia podyplomowe w zakresie bezpieczeństwa informacji ☐ certyfikaty ISO (*jakie*): ... ☐ inne (*jakie*): ...
4.	**Czy wyznaczono osobę odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych** *Należy wskazać, czy w strukturze Administratora Danych wyznaczono osobę odpowiedzialną za ochronę danych osobowych w systemach informatycznych*	☐ wyznaczono Administratora Systemów Informatycznych ☐ wyznaczono inną osobę (*należy wskazać jaką*): ... ☐ brak

5.	**Dokumentacja ochrony danych osobowych** *Należy wskazać które z wymienionych dokumentów / procedur zostały wdrożone i są stosowane w strukturze Administratora Danych*	Polityka ochrony danych osobowych: ☐ tak ☐ nie Rejestr czynności przetwarzania: ☐ tak ☐ nie ☐ nie dotyczy Rejestr kategorii czynności przetwarzania: ☐ tak ☐ nie ☐ nie dotyczy Zasady privacy by design oraz privacy by default: ☐ tak ☐ nie Zasady retencji danych osobowych: ☐ tak ☐ nie Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych: ☐ tak ☐ nie Procedura postępowania z incydentami ochrony danych osobowych: ☐ tak ☐ nie Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*): ☐ tak ☐ nie Procedura realizacji praw osób, których dane dotyczą: ☐ tak ☐ nie Procedura tworzenia kopii zapasowych: ☐ tak ☐ nie Procedury IT (np. procedury odtwarzania systemu po awarii, procedury testowania systemów, etc.): ☐ tak (*jakie*): ... ☐ nie

6.	**Szkolenia** *Należy wskazać czy Administrator Danych szkoli pracowników/ współpracowników z zasad ochrony danych osobowych, a jeśli tak w jaki sposób są przeprowadzane np. w formie elektronicznej (e-learning), stacjonarnej, zdalnej (za pośrednictwem narzędzi do komunikacji na odległość)*	☐ tak *(w jaki sposób)*: ... ☐ nie

...
...
...
...
...
...
...
...
...
...
...
...
...
...
...
...
...
.....
.....
...

Data i podpis osoby udzielającej odpowiedzi na pytania

OPIS STOSOWANYCH ZABEZPIECZEŃ	
ZABEZPIECZENIA FIZYCZNE *dotyczy pomieszczeń w których będą/mogą być przetwarzane dane w procesie, którego dotyczy Test*	
1. **Imię, nazwisko oraz stanowisko osoby udzielającej odpowiedzi na pytania –** *Ta część powinna zostać uzupełniona przez osobę (osoby) posiadającą wiedzę na temat stosowanych zabezpieczeń fizycznych dotyczących pomieszczeń w których będą/mogą być przetwarzane dane w procesie, którego dotyczy Test:*	
2. **Zabezpieczenia pomieszczeń** *Należy określić stosowane zabezpieczenia w pomieszczeń w których będą/mogą być przetwarzane dane:*	<u>Dostęp do pomieszczeń</u> ☐ Klucze, ☐ Karty magnetyczne/ karty chipowe ☐ Ochrona obiektu przez firmę ochroniarską, ☐ Systemy alarmowe ☐ Kamery monitoringu CCTV <u>Pozostałe środki</u> ☐ Zamykane szafy/ szuflady, ☐ Systemy przeciwpożarowe, ☐ Niszczarki na dokumenty/ dedykowane pojemniki do bezpiecznego niszczenia dokumentów, ☐ inne (*jakie*): …
4. **Zabezpieczenia serwerowni** *Należy określić stosowane zabezpieczania w odniesieniu do pomieszczenia serwerowni:*	<u>Dostęp do pomieszczeń</u> ☐ Klucze, ☐ Karty magnetyczne/ karty chipowe ☐ Ochrona przez firmę ochroniarską, ☐ Systemy alarmowe ☐ Kamery monitoringu CCTV <u>Pozostałe środki</u> ☐ Systemy przeciwpożarowe, ☐ inne (*jakie*): …

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Data i podpis osoby udzielającej odpowiedzi na pytania

OPIS STOSOWANYCH ZABEZPIECZEŃ	
ZABEZPIECZENIA TECHNICZNE *dotyczy narzędzi informatycznych które będą/ mogą być wykorzystywane do przetwarzania danych w procesie którego dotyczy Test*	
Imię, nazwisko oraz stanowisko osoby udzielającej odpowiedzi na pytania *Ta część powinna zostać uzupełniona przez osobę (osoby) posiadającą wiedzę na temat stosowanych zabezpieczeń technicznych dotyczących narzędzi informatycznych które będą/ mogą być wykorzystywane do przetwarzania danych w procesie którego dotyczy Test*	
Stosowane zabezpieczenia	☐ zapora firewall, ☐ indywidualny login i hasło dla każdego użytkownika, ☐ uprawnienia dostępu dostosowane do potrzeb użytkowników ☐ szyfrowanie, ☐ pseudonimizacja ☐ tworzenie kopii zapasowych ☐ zasilanie awaryjne (UPS), ☐ ochrona antywirusowa, ☐ mechanizm odnotowywania logów systemowych, ☐ inne *(jakie)* ...

... ... *Data i podpis osoby udzielającej odpowiedzi na pytania*

WÓJT

Paweł Gibczyński

Załącznik nr 7

Procedura realizacji praw osób, których dane dotyczą

1. Każda osoba, której dane dotyczą, ma prawo do wystąpienia do Administratora Danych z żądaniem realizacji praw przysługujących jej w związku przetwarzaniem jej danych osobowych. W szczególności dotyczy to prawa do:
   1.1. wycofania wyrażonej zgody na przetwarzanie danych osobowych (art. 7 ust. 3 RODO),
   1.2. dostępu do danych osobowych (art. 15 RODO),
   1.3. sprostowania danych osobowych (art. 16 RODO),
   1.4. usunięcia danych osobowych (w tym prawa do bycia zapomnianym) (art. 17 RODO),
   1.5. ograniczenia przetwarzania danych osobowych (art. 18 RODO),
   1.6. przenoszenia danych osobowych (art. 20 RODO),
   1.7. wniesienia sprzeciwu wobec przetwarzania danych osobowych (art. 21 RODO),
   1.8. niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych (art. 22 RODO).
2. Osoba, której dane dotyczą może wnieść swoje żądanie w dowolnej formie (papierowej, ustnej lub elektronicznej). W szczególności, żądanie może zostać złożone za pośrednictwem dedykowanej skrzynki mailowej: iod@ugczluchow.pl.
3. Żądanie realizacji praw może zostać również złożone za pośrednictwem podmiotu przetwarzającego, któremu Administrator Danych powierzył przetwarzanie danych osobowych. W takich przypadkach, podmiot przetwarzający informuje Administratora Danych o wniesieniu żądania zgodnie z postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych.
4. Pracownik, do którego wpłynęło żądanie realizacji praw, jest zobowiązany do:
   4.1. poinformowania osoby składającej żądanie o jego przyjęciu i przekazaniu do rozpoznania,
   4.2. weryfikacji / potwierdzenia tożsamości osoby występującej z tym żądaniem,
   4.3. przekazania żądania do IOD.
5. Jeżeli pracownik, do którego wpłynęło żądanie, ma uzasadnione wątpliwości co do tożsamości osoby, od której to żądanie pochodzi, może zażądać od niej dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości.
6. Poinformowania o przyjęciu żądania oraz weryfikacji tożsamości osoby występującej z żądaniem dokonuje się w tej samej formie w jakiej zostało złożone żądanie.

7. Pracownik, do którego wpłynęło żądanie realizacji praw przekazuje je do IOD niezwłocznie, jednak nie później niż w terminie 48 godzin od jego otrzymania.

8. Po otrzymaniu żądania realizacji praw, IOD dokonuje jego analizy, a w szczególności ustala:

   8.1. jaki jest zakres żądania,

   8.2. czy dane osobowe, których dotyczy żądanie są przetwarzane przez Administratora Danych,

   8.3. czy w odniesieniu do danych osobowych, których dotyczy żądanie Administrator Danych występuje w roli ich administratora w rozumieniu art. 4 pkt 7 RODO, czy też w roli podmiotu przetwarzającego, w rozumieniu art. 4 pkt 8 RODO,

   8.4. czy dane prawo przysługuje osobie występującej z żądaniem.

9. W toku analizy, o której mowa w pkt 7, IOD konsultuje się z osobami merytorycznie zaangażowanymi w proces przetwarzania danych osobowych osoby występującej z żądaniem.

10. Jeżeli w toku analizy pojawią się uzasadnione wątpliwości co do zakresu zgłoszonego żądania, w szczególności, gdy z uwagi na treść żądania nie jest oczywiste, z którego z praw osoba, której dane dotyczą chce skorzystać, IOD na podstawie zebranych informacji przygotowuje odpowiedź z prośbą o skonkretyzowanie żądań.

11. Jeżeli w toku dalszej analizy, stwierdzone zostanie, że:

   11.1. Administrator Danych nie przetwarza danych osobowych stanowiących przedmiot żądania,

   11.2. dane prawo nie przysługuje osobie występującej z żądaniem,

   IOD przygotowuje odpowiedź odmowną realizacji prawa.

12. Odpowiedź odmowna realizacji prawa przekazywana jest osobie, która wniosła żądanie niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania. Odpowiedź odmowna zawiera, w szczególności informacje o:

   12.1. samym fakcie niespełnienia żądania,

   12.2. powodach niespełnienia żądania,

   12.3. możliwości wniesienia skargi do organu nadzorczego,

   12.4. możliwości skorzystania ze środków ochrony prawnej przed sądem.

13. Jeżeli w toku analizy, stwierdzone zostanie, że dane prawo przysługuje osobie występującej z żądaniem lub przysługuje jej w określonym zakresie, IOD w porozumieniu z osobami merytorycznie zaangażowanymi w proces przetwarzania danych osobowych:

   13.1. ustala sposób realizacji prawa,

13.2. przygotowuje odpowiedź wskazującą na sposób realizacji prawa.

14. Przekazywanie odpowiedzi na żądanie realizacji praw oraz prowadzenie jakiejkolwiek komunikacji z osobami, których dane dotyczą, odbywa się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

15. Odpowiedzi przekazuje się w formie pisemnej lub elektronicznej. Przekazanie informacji w formie ustnej może nastąpić wyłącznie wtedy, gdy osoba, której dane dotyczą, tego zażąda i to wyłącznie pod takim warunkiem, że innymi sposobami potwierdzi się jej tożsamość.

16. Spełnienie żądania realizacji prawa następuje bez zbędnej zwłoki, nie później jednak niż w terminie jednego miesiąca od dnia otrzymania żądania.

17. Termin, o którym mowa w pkt 16 może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań pochodzących od tej samej osoby. W terminie miesiąca od otrzymania żądania, informuje się osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

18. IOD prowadzi rejestr zgłoszonych żądań realizacji praw, według wzoru, który znajduje się w niniejszym Załączniku.

19. Podejmowanie działań w związku z realizacją praw osób, których dane dotyczą jest co do zasady wolne od opłat.

20. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator Danych może:

    20.1. pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo

    20.2. odmówić podjęcia działań w związku z żądaniem.

21. Działania osoby, której dane dotyczą, o których mowa w pkt 20 mają charakter nadużycia prawa, przez co należy rozumieć korzystanie z prawa i używanie instrumentów służących jego realizacji nie w celu zrealizowania wartości, którym to prawo ma służyć, chociaż z powoływaniem się na nie. W szczególności, za nadużycie prawa do informacji na gruncie RODO należy uznać takie działania osób, których dane dotyczą, które:

    21.1. nie służą realizacji prawa do ochrony danych osobowych oraz

    21.2. są nieuzasadnione lub nadmierne.

22. IOD dokonuje oceny, czy zostały spełnione przesłanki, o których mowa w pkt 21 tj. czy działania osoby, której dane dotyczą można uznać za nadużycie prawa.

23. Dokonana ocena, przedkładana jest Administratorowi Danych przez IOD. Na jej podstawie Administrator Danych podejmuje ostateczną decyzję o nałożeniu opłaty lub odmowie podjęcia działań.

24. Ogólne zasady realizacji poszczególnych praw osób, których dane dotyczą znajdują się poniżej w niniejszym Załączniku.

Prawo do wycofania zgody (art. 7 RODO)

1. W sytuacji, jeżeli przetwarzanie danych odbywa się na podstawie zgody osoby, której dane dotyczą, osoba ta ma prawo do jej odwołania w dowolnym momencie.
2. Skutkiem odwołania zgody jest brak możliwości przetwarzania danych osobowych z powołaniem się na tę właśnie podstawę przetwarzania danych w przyszłości.
3. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Prawo dostępu do danych (art. 15 RODO)

1. Prawo dostępu do danych daje osobie, której dane dotyczą prawo do:
    1. uzyskania od Administratora Danych potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli tak, również dodatkowych informacji dotyczących tego przetwarzania (m.in. w zakresie celu przetwarzania, kategorii przetwarzanych danych, kategorii odbiorców jej danych osobowych, etc.),
    2. uzyskania kopii danych osobowych podlegających przetwarzaniu.
2. Osoba, której dane dotyczą może wedle swego uznania, choć w ramach katalogu zamkniętego określonego w art. 15 RODO, kształtować zakres uzyskanych informacji czy danych przekazanych w postaci kopii. Realizując przyznane uprawnienia, może więc żądać przekazania zarówno każdej, jak i wszystkich wskazanych w art. 15 RODO informacji, jak również żądać kopii czy wglądu do wybranych bądź wszystkich danych.
3. Rezultatem wykonania prawa dostępu do danych osobowych powinno być udzielenie osobie, której dane dotyczą, żądanych przez nią informacji.
4. W wyniku realizacji prawa dostępu do danych osobowych, osoba, której dane dotyczą, może uzyskać kopię danych osobowych we wskazanym przez siebie formacie. Jeżeli jednak nie zastrzeże tego formatu w swoim żądaniu informacje powinny zostać przekazane za pomocą tego samego środka porozumiewania się, przy użyciu, którego osoba, której dane dotyczą, skierowała swoje żądanie do Administratora Danych.

Prawo do sprostowania danych (art. 16 RODO)

1. Osoba, której dane dotyczą posiada uprawnienie do:
    1. sprostowania nieprawidłowych danych osobowych,
    2. uzupełnienia niekompletnych danych osobowych.
2. Osoba, której dane dotyczą swoim żądaniem powinna wykazać, że jej żądanie jest w istocie zasadne tj. Administrator Danych przetwarza dane nieprawidłowe lub niekompletne.

3. Tylko po spełnieniu warunku wskazanego w pkt 2 Administrator Danych będzie zobowiązany do niezwłocznego sprostowania danych nieprawidłowych lub do uzupełnienia danych niekompletnych.

4. Zgodnie z art. 19 RODO Administrator Danych informuje o sprostowaniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Prawo do usunięcia danych (art. 17 RODO)

1. Prawo do usunięcia danych składa się z dwóch uprawnień cząstkowych:
    1. możliwości żądania usunięcia danych osobowych przez Administratora Danych,
    2. możliwości żądania, aby Administrator Danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje (tzw. prawo do zapomnienia).
2. Możliwość skorzystania z uprawnienia do żądania usunięcia danych przez innych administratorów jest uzależniona od możliwości skorzystania z żądania usunięcia danych osobowych przez pierwotnego Administratora Danych.
3. Osoba, której dane dotyczą, może żądać usunięcia swoich danych osobowych we wskazanych w art. 17 ust. 1 RODO przypadkach, tj. m.in. w sytuacji, jeżeli jej dane osobowe nie są już niezbędne do celów, w których były przetwarzane, wycofała ona zgodę na przetwarzanie danych, wniosła sprzeciw od takiego przetwarzania, czy też jej dane przetwarzane były niezgodnie z prawem.
4. Przez usunięcie danych osobowych należy rozumieć całkowite zniszczenie danych (w tym nośników, na których były one zapisane) lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (tzw. anonimizacja danych). Efektem działania Administratora Danych powinien być brak możliwości dalszego dokonywania jakichkolwiek operacji na tych danych.
5. W przypadku prawa do bycia zapomnianym mamy do czynienia jedynie z obowiązkiem informacyjnym Administratora Danych wobec innych administratorów. Administrator Danych nie ma obowiązku dopilnowania, aby dane faktycznie zostały przez tych administratorów usunięte. Dodatkowo zakres obowiązku poinformowania innych administratorów jest ograniczony przez: dostępną technologię, koszt realizacji obowiązku poinformowania, odwołanie do podejmowania rozsądnych działań w wykonaniu tego obowiązku.

Prawo do ograniczenia przetwarzania (art. 18 RODO)

1. Osoba, której dane dotyczą ma prawo do żądania ograniczenia przetwarzania danych osobowych. Ograniczenie przetwarzania danych osobowych polega na konieczności ograniczenia przetwarzania danych wyłącznie do ich przechowywania.

2. Administrator Danych jest zobowiązany do ograniczenia przetwarzania danych, jeżeli zaistnieje jedna ze wskazanych w art. 18 RODO przesłanek, tj. osoba, której dane dotyczą:

    1. kwestionuje prawidłowość danych osobowych (ograniczenie przetwarzania następuje automatycznie na okres pozwalający Administratorowi Danych sprawdzić prawidłowość tych danych),

    2. sprzeciwia się usunięciu danych osobowych przetwarzanych niezgodnie z prawem,

    3. żąda zastosowania ograniczenia przetwarzania w stosunku do danych, które powinny zostać usunięte, ale które są jej niezbędne do ustalenia, dochodzenia lub obrony przysługujących jej roszczeń,

    4. wniosła sprzeciw wobec przetwarzania danych osobowych (ograniczenie przetwarzania następuje automatycznie, na okres pozwalający Administratorowi Danych stwierdzić czy sprzeciw jest zasadny).

3. Przykładami ograniczenia przetwarzania są:

    1. czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania,

    2. uniemożliwienie użytkownikom dostępu do wybranych danych,

    3. czasowe usunięcie opublikowanych danych ze strony internetowej.

4. W każdym przypadku, dane, w odniesieniu do których ograniczono przetwarzanie, powinny być wyraźnie odróżnione od pozostałych danych oraz nie mogą podlegać dalszemu przetwarzaniu ani modyfikacjom.

Prawo do przenoszenia danych (art. 20 RODO)

1. Osobie, której dane dotyczą przysługuje prawo do przenoszenia danych, na które składają się dwa uprawnienia:

    1. prawo otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła Administratorowi Danych,

    2. prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła Administratorowi Danych, innemu administratorowi, bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

2. Uprawnienia, o których mowa w pkt 1 mogą być wykonywanie niezależnie od siebie i niezależnie od uprawnienia do uzyskania kopii danych osobowych podlegających przetwarzaniu.

3. Osoba, której dane dotyczą, może skorzystać z prawa do przenoszenia danych osobowych, jeżeli łącznie spełnione są dwa warunki:

1. przetwarzanie danych odbywa się na podstawie zgody lub w celu wykonania umowy, oraz
2. przetwarzanie danych odbywa się w sposób zautomatyzowany (prawo do przenoszenia danych nie obejmuje tzw. zbiorów papierowych).

4. Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo, które to dane ta osoba świadomie i aktywnie przekazała. Nie obejmuje natomiast danych wywnioskowanych przez Administratora Danych w procesie ich przetwarzania.

Prawo do wniesienia sprzeciwu (art. 21 RODO)

1. Osoba, której dane dotyczą, ma prawo do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych:
   1. opartego na interesie publicznym lub prawnie uzasadnionych interesach, w tym wobec profilowania na podstawie tych przepisów, z przyczyn związanych z jej szczególną sytuacją,
   2. na potrzeby marketingu bezpośredniego,
   3. do celów badań naukowych lub historycznych lub do celów statystycznych, z przyczyn związanych z jej szczególną sytuacją.
2. W razie otrzymania skutecznego sprzeciwu wobec przetwarzania danych osobowych, Administrator Danych powinien niezwłocznie zaprzestać przetwarzania danych w zakresie objętym tym sprzeciwem.
3. Jeżeli Administrator Danych uzna sprzeciw za pozbawiony podstaw, w szczególności z takiej przyczyny, że w jego ocenie nie zachodzi szczególna sytuacja uzasadniająca wniesienie sprzeciwu, ewentualny nakaz uwzględnienia sprzeciwu może zostać wydany przez organ nadzorczy na skutek skargi wniesionej przez zainteresowaną osobę.

Prawo do niepodlegania zautomatyzowanym decyzjom (art. 22 RODO)

1. Osoba, której dane dotyczą ma prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym na profilowaniu. Prawo to dotyczy sytuacji, w których zautomatyzowane podejmowanie decyzji:
   1. wywołuje skutki prawne wobec osoby, której dane dotyczą,
   2. wpływa istotnie na osobę, której dane dotyczą, w podobny sposób do skutków prawnych.
2. Podejmowanie przez Administratora Danych zautomatyzowanych decyzji, o których mowa w pkt 1, możliwe jest tylko pod warunkiem, że:
   1. jest ono niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem Danych,

2. jest dozwolone prawem Unii lub prawem państwa członkowskiego,

3. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3. Jeżeli automatyczne podejmowanie decyzji jest niezbędne do zawarcia lub wykonania umowy albo gdy odbywa się na podstawie wyraźnej zgody, Administrator Danych powinien wdrożyć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, o co najmniej prawa do uzyskania interwencji ludzkiej, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Oznacza to konieczność zapewnienia możliwości odwołania się osoby, której dane dotyczą, od automatycznego rozstrzygnięcia. Takie odwołanie powinno być rozpatrywane przez człowieka.

Wzór rejestru zgłoszonych żądań realizacji praw

Lp.	Numer żądania	Data wpływu żądania *(dd/mm/rrrr)*	Osoba, której dane dotyczą *(imię, nazwisko, ew. inne dane identyfikujące)*	Przedmiot żądania	Data wysłania odpowiedzi na żądanie *(dd/mm/rrrr)*	Rodzaj odpowiedzi *(realizacja prawa / odmowa realizacji prawa / częściowa realizacja prawa)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

WÓJT
Paweł Gibczyński

Załącznik nr 8

Wzór sprawozdania z audytu zgodności przetwarzania danych osobowych

SPRAWOZDANIE Z AUDYTU ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

.....

miejscowość, data

1. Administrator Danych:

2. IOD: ...

3. Data rozpoczęcia audytu: ...

4. Data zakończenia audytu: ...

5. Przedmiot audytu:

.....
.....

.....
.....

6. Zakres audytu:

.....
.....

.....
.....

7. Wykaz czynności podjętych w toku audytu:

.....
.....

.....
.....

8. Opis stanu faktycznego stwierdzonego w toku audytu oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

.....
.....
.....
.....

9. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym audytem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

LP.	STWIERDZONY PRZYPADEK NARUSZENIA	DZIAŁANIA PRZYWRACAJĄCE STAN ZGODNY Z PRAWEM / REKOMENDACJE	
		DZIAŁANIA IOD	DZIAŁANIA ADMINISTRATORA DANYCH
1.			
2.			
3.			

10. Załączniki:

.....
Data i podpis IOD

WÓJT
Paweł Gibczyński

Procedura kontroli podmiotów przetwarzających

1. Administrator Danych dopuszcza, by dane osobowe, których jest administratorem w rozumieniu art. 4 pkt 7 RODO, były przetwarzane poza jego strukturami organizacyjnymi przez podmioty przetwarzające.
2. Przetwarzanie danych osobowych przez podmioty przetwarzające może się odbywać wyłącznie w określonym celu i zakresie, na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
3. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych z punktu widzenia zgodności tego przetwarzania z:
    1. przepisami prawa,
    2. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,
    3. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności.
4. Kontrola, o której mowa w pkt 3 prowadzona jest w postaci audytu podmiotu przetwarzającego.
5. Szczegóły dotyczące audytu podmiotu przetwarzającego określa zawarta z tym podmiotem umowa powierzenia przetwarzania danych osobowych. W szczególności, dotyczy to postanowień w zakresie sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu.
6. W sytuacji, gdy umowa powierzenia przetwarzania danych osobowych nie określa sposobu i terminu przekazywania podmiotowi przetwarzającemu informacji o terminie i zakresie audytu, kwestie te ustalane są z tym podmiotem w formie porozumienia przed przeprowadzeniem pierwszego audytu, z zastrzeżeniem, że poczynione ustalenia pozostają właściwe dla przyszłych audytów.
7. Audyt podmiotu przetwarzającego może zostać przeprowadzony, w szczególności w następujących przypadkach:
    1. powierzenie przetwarzania obejmuje szczególne kategorie danych osobowych i/lub dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa,
    2. powierzenie przetwarzania obejmuje dane osobowe osób poniżej 16 r.ż.,
    3. powierza się przetwarzanie danych osobowych na dużą skalę,
    4. Administrator Danych otrzymał informację o incydentach z zakresu ochrony danych osobowych występujących u podmiotu przetwarzającego.

8. Decyzję o przeprowadzeniu audytu podmiotu przetwarzającego podejmuje Administrator Danych:

   1. samodzielnie,

   2. na podstawie złożonego wniosku o przeprowadzenie audytu.

9. Z wnioskiem o przeprowadzenie audytu podmiotu przetwarzającego może wystąpić IOD.

10. Wniosek o przeprowadzenie audytu podmiotu przetwarzającego składany jest do Administratora Danych.

11. Wniosek o przeprowadzenia audytu podmiotu przetwarzającego zawiera co najmniej:

    1. nazwę oraz siedzibę podmiotu przetwarzającego,

    2. uzasadnienie konieczności przeprowadzenia audytu.

12. Na podstawie otrzymanego wniosku, Administrator Danych podejmuje ostateczną decyzję o przeprowadzeniu audytu podmiotu przetwarzającego. Gdy jest to zasadne, przed podjęciem decyzji, Administrator Danych konsultuje się z IOD.

13. Audyt podmiotu przetwarzającego realizowany jest przez IOD. Jeżeli jest to zasadne, IOD realizuje audyt przy współpracy z innymi osobami upoważnionymi przez Administratora Danych, których wiedza może mieć kluczowe znaczenie dla merytorycznej poprawności przeprowadzanego audytu.

14. Audyt podmiotu przetwarzającego realizowany jest:

    14.1. w siedzibie podmiotu przetwarzającego,

    14.2. w głównym miejscu przetwarzania powierzonych danych osobowych, lub

    14.3. zdalnie.

15. IOD oraz osoba odpowiedzialna za bezpośrednią współpracę i utrzymywanie stałych kontaktów z podmiotem przetwarzającym opracowują wspólnie harmonogram przeprowadzania audytu, który wskazuje w szczególności na:

    15.1. termin audytu,

    15.2. miejsce audytu,

    15.3. zakres audytu,

    15.4. osoby biorące udział w audycie.

16. IOD, przy współpracy z osobą odpowiedzialną za bezpośrednią współpracę i utrzymywanie stałych kontaktów z podmiotem przetwarzającym, informuje ten podmiot o terminie, miejscu i zakresie audytu.

17. IOD przeprowadza audyt z wykorzystaniem formularza audytu, którego wzór znajduje się w niniejszym Załączniku.

18. Formularz audytu uzupełniany jest:

18.1. w przypadku audytu w siedzibie podmiotu przetwarzającego lub w głównym miejscu przetwarzania powierzonych danych osobowych – przez IOD oraz inne osoby realizujące audyt, o których mowa w pkt 14,

18.2. w przypadku audytu zdalnego – przez osoby upoważnione do tego przez podmiot przetwarzający.

19. Po przeprowadzonym audycie IOD sporządza Protokół poaudytowy, według wzoru znajdującego się w niniejszym Załączniku.

20. IOD przedkłada Protokół poaudytowy

20.1. Administratorowi Danych,

20.2. podmiotowi przetwarzającemu.

21. Podmiot przetwarzający ma 7 dni na ustosunkowanie się do treści przedstawionego mu Protokołu poaudytowego, z zastrzeżeniem, że umowa powierzenia przetwarzania danych osobowych zawarta z tym podmiotem może określać inny termin.

22. Jeżeli w wyniku audytu stwierdzono niezgodność przetwarzania powierzonych danych osobowych z:

22.1. obowiązującymi przepisami prawa, lub

22.2. postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych,

22.3. wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności,

Administrator Danych, na podstawie przedłożonego mu Protokołu poaudytowego, podejmuje ostateczną decyzję w zakresie dalszej współpracy z podmiotem przetwarzającym.

23. Formularz audytu podmiotu przetwarzającego jest stosowany przez Administratora Danych również w stosunku do podmiotów, z którymi Administrator Danych chce nawiązać współpracę tj. potencjalnych podmiotów przetwarzających. W odniesieniu do takich podmiotów, niniejszą Procedurę kontroli podmiotów przetwarzających stosuje się odpowiednio z wyłączeniem pkt 5-6 oraz pkt 22.2.

FORMULARZ AUDYTU PODMIOTU PRZETWARZAJĄCEGO			
Administrator Danych	**Nazwa:** **Siedziba:**		
Podmiot przetwarzający	**Nazwa:** **Siedziba:**		
Data i miejsce audytu *w przypadku audytu zdalnego należy wskazać datę uzupełnienia Formularza*			
Osoby reprezentujące podmiot przetwarzający biorące udział w audycie *w przypadku audytu zdalnego należy wskazać osoby odpowiedzialne za uzupełnienie Formularza*	1. *...(imię, nazwisko, stanowisko, dane kontaktowe)...* 2. *...(imię, nazwisko, stanowisko, dane kontaktowe)...* 3. *...(imię, nazwisko, stanowisko, dane kontaktowe)...*		
Osoby reprezentujące Administratora Danych biorące udział w audycie *w przypadku audytu zdalnego należy wskazać osoby do których Formularz jest wysyłany*	1. *...(imię, nazwisko, stanowisko, dane kontaktowe)...* 2. *...(imię, nazwisko, stanowisko, dane kontaktowe)...* 3. *...(imię, nazwisko, stanowisko, dane kontaktowe)...*		
Lp.	**Obszar**	**Pytania pomocnicze**	**Stan faktyczny**
1.	Usługi świadczone na rzecz Administratora Danych	1. Jaki jest rodzaj usług świadczonych przez podmiot przetwarzający, w związku z którymi dochodzi do powierzenia przetwarzania danych osobowych?	
2.	Zakres przetwarzanych danych osobowych	1. Kogo dane osobowe są przetwarzane?	
		2. Czy przetwarzane są dane osób poniżej 16 r.ż.?	
		3. Jakie kategorie danych osobowych są przetwarzane?	
		4. Czy przetwarzane są szczególne kategorie danych? (*jakie*)	

		5. Czy przetwarza się dane dotyczące wyroków skazujących i naruszeń prawa?	
3	**Struktura organizacyjna**	1. Czy wyznaczono Inspektora Ochrony Danych? (*imię, nazwisko oraz dane kontaktowe*)	
		2. Jeżeli nie wyznaczono IOD, czy wyznaczono osobę o podobnym stanowisku, nadzorującą kwestie związane z ochroną danych osobowych? (*funkcja, imię, nazwisko oraz dane kontaktowe*)	
		3. Czy wyznaczono osobę odpowiedzialną za zabezpieczenia danych osobowych przetwarzanych za pomocą systemów informatycznych? (*imię, nazwisko, stanowisko oraz dane kontaktowe*)	
4	**Polityki ochrony danych osobowych**	1. Jakie polityki w zakresie ochrony danych osobowych zostały wdrożone?	
		2. W jaki sposób polityki ochrony danych osobowych zostały wdrożone? (*np. formalnie zatwierdzone i wprowadzone w życie procedury dot. środków ochrony danych osobowych*)	
		3. Czy jest przeprowadzana regularna aktualizacja polityk ochrony danych osobowych?	
5	**Audyt**	1. Czy wdrożono program audytowy obejmujący zgodność z regulacjami w zakresie ochrony danych osobowych?	
		2. Jeżeli tak, kto jest odpowiedzialny za przeprowadzanie audytów?	

		3. Jakie są metody przeprowadzania audytów, ich częstotliwość oraz zakres?	
6.	Incydenty	1. Czy wdrożono procedurę postępowania z incydentami z zakresu ochrony danych osobowych?	
		2. Czy osoby posiadające dostęp do powierzonych danych osobowych zostali przeszkoleni w zakresie zgłaszania incydentów z zakresu ochrony danych osobowych?	
		3. Czy w okresie ostatnich trzech lat miały miejsce incydenty z zakresu ochrony danych osobowych? (*rodzaj, ilość*)	
		4. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem postępowania ze strony urzędów zajmujących się ochroną danych osobowych? (*rodzaj, ilość*)	
		5. Czy w okresie ostatnich trzech lat działalność podmiotu przetwarzającego była przedmiotem działań prawnych dotyczących zarzutów naruszenia prywatności lub ochrony danych osobowych? (*rodzaj, ilość*)	
		6. Czy w okresie ostatnich trzech lat podmiot przetwarzający zgłosił jakiekolwiek naruszenia bezpieczeństwa danych odpowiednim organom / urzędom (uwzględniając organy związane z ochroną danych osobowych) oraz / lub podmiotom zajmującym się ochroną danych osobowych?	

		7. Czy podmiot przetwarzający jest zdolny do powiadomienia Administratora Danych o jakimkolwiek naruszeniu bezpieczeństwa, które mogłoby mieć negatywne skutki dla ochrony powierzonych do przetwarzania danych osobowych oraz praw i wolności osób, których te dane dotyczą, bez opóźnienia, tj. w ciągu 24 godzin od chwili powzięcia informacji o naruszeniu?	
7.	**Osoby posiadające dostęp do powierzonych danych osobowych w strukturze podmiotu przetwarzającego**	1. Czy stosuje się politykę lub procedurę ograniczającą dostęp do powierzonych danych osobowych?	
		2. W jaki sposób podejmowane są decyzje o tym, kto powinien otrzymać dostęp do powierzonych danych osobowych i w jaki sposób jest to sprawdzane i potwierdzane?	
		3. Jaka jest forma współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych? (*umowa o pracę, umowa cywilnoprawna, umowa o współpracy*)	
		4. Czy osoby posiadające dostęp do powierzonych danych osobowych odbywają szkolenia w zakresie przetwarzania i ochrony prywatności danych oraz zgodności z przepisami prawa w zakresie ochrony danych osobowych? (*forma szkoleń, częstotliwość*)	
		5. Czy osobom posiadającym dostęp do powierzonych danych osobowych nadawane są upoważnienia do przetwarzania danych osobowych?	

		6. Czy osoby posiadające dostęp do powierzonych danych osobowych składają oświadczenia o zachowaniu tych danych w poufności przez okres trwania współpracy jak i po jej zakończeniu?	
		7. Czy prowadzona jest ewidencja osób posiadających dostęp do powierzonych danych osobowych?	
		8. Czy w przypadku zakończenia współpracy z osobami posiadającymi dostęp do powierzonych danych osobowych, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
8.	**Forma przetwarzania powierzonych danych osobowych**	1. W jakiej formie przetwarzane są powierzone dane osobowe? (*papierowa, elektroniczna*)	
		2. Jeżeli dane osobowe przetwarzane są w formie elektronicznej, za pomocą systemów informatycznych, proszę podać nazwy tych systemów.	
9.	**Miejsce przetwarzania powierzonych danych osobowych**	1. W jakich lokalizacjach ma miejsce przetwarzanie powierzonych danych osobowych? (*dane osobowe przetwarzane na bieżąco, wersje archiwalne, kopie zapasowe*)	
		2. Czy jest prowadzona aktualna ewidencja dotycząca lokalizacji i przemieszczania sprzętu i nośników elektronicznych, które mogą zawierać powierzone dane osobowe?	

10	**Podpowierzanie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są podpowierzane innym podmiotom?	
		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych podpowierzanych poszczególnym podmiotom*)	
		3. Czy z podmiotami, którym podpowierza się dane osobowe zawarto umowę podpowierzenia?	
		4. Czy zawarta umowa podpowierzenia przewiduje nałożenie na podmiot, któremu dane są podpowierzane te same obowiązki ochrony danych jakie zostały nałożone na podmiot przetwarzający na mocy umowy powierzenia z Administratorem Danych?	
		5. Czy podmiot przetwarzający monitoruje lub dokonuje audytu zgodności przetwarzania podpowierzonych danych osobowych z przepisami prawa oraz postanowieniami zawartej umowy podpowierzenia przetwarzania danych osobowych? (*zakres, częstotliwość audytów, metody, odpowiedzialność*)	
		6. Czy w przypadku zakończenia współpracy z podmiotem, któremu dane są podpowierzane, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu współpracy? (*sposób odbioru dostępu*)	
11	**Udostępnianie powierzonych danych osobowych**	1. Czy powierzone dane osobowe są udostępniane innym podmiotom? (*zakres udostępnianych danych, nazwy podmiotów*)	

		2. Jeżeli tak, jakim podmiotom i w jakim zakresie? (*nazwy podmiotów, zakres danych udostępnianych poszczególnym podmiotom*)	
12.	**Przekazywanie powierzonych danych osobowych do państw trzecich**	1. Czy powierzone dane osobowe są przekazywane do państw trzecich?	
		2. Jeżeli tak, do jakich państw trzecich, jakim podmiotom, w jakim zakresie i na jakiej podstawie? (*państwo trzecie, nazwy podmiotów, zakres przekazywanych danych poszczególnym podmiotom, podstawa prawna*)	
13.	**Zabezpieczenia fizyczne**	1. Jakie zabezpieczenia fizyczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia fizyczne, w szczególności to jak zostały zabezpieczone pomieszczenia, w których przetwarzane są powierzone dane osobowe (polityki i procedury dostępu do pomieszczeń, rodzaj drzwi, rodzaj zamków, formy kontroli dostępu, formy zabezpieczenia przed osobami z zewnątrz, monitoring, ochrona, alarm, etc.) oraz to jak przechowuje się nośniki, na których przetwarzane są powierzone dane osobowe (rodzaje szaf, dane osobowe w formie papierowej (rodzaj szaf, zabezpieczenia fizyczne komputerów, niszczarki do dokumentów, etc.)*	
14.	**Zabezpieczenia techniczne**	1. Jakie zabezpieczenia techniczne wdrożono dla ochrony powierzonych danych osobowych? **Należy opisać wdrożone zabezpieczenia techniczne, w szczególności jakie środki wdrożone zostały dla ograniczenia dostępu do powierzonych danych osobowych (kontrola dostępu poprzez ograniczanie uprawnień, indywidualny login i hasło, wymagania dotyczące złożoności hasła, okresowa kontrola uprawnień, etc.), jakie środki techniczne są stosowane do zapewnienia bezpieczeństwa systemu (antywirus, firewall, IPS, IDS, etc.), jakie środki wdrożone zostały dla zagwarantowania rozliczalności, poufności i integralności powierzonych danych osobowych**	

... ... Data i podpis osoby wypełniającej Formularz

Wzór protokołu poaudytowego

PROTOKÓŁ POAUDYTOWY NR .../.....

.....

miejscowość, data

1. Administrator Danych: .....
.....

2. Podmiot przetwarzający: .....
.....

3. Data rozpoczęcia audytu: .....
.....

4. Data zakończenia audytu: .....
.....

5. Miejsce audytu: .....
.....

6. Osoby prowadzące czynności audytowe (*imiona, nazwiska, stanowiska*):

.....
.....

7. Osoby upoważnione przez podmiot przetwarzający do udzielania wyjaśnień w trakcie czynności audytowych (*imiona, nazwiska, stanowiska*):

.....
.....

8. Zakres audytu:

………

……………………..

9. Wykaz czynności podjętych w toku audytu:

………

……………………..

10. Wnioski poaudytowe:

………

……………………..

Kluczowe wnioski:

… . . . . . … … … .

……………………………………………..

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z obowiązującymi przepisami prawa:

… . . . . . … … … .

……………………………………………..

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z postanowieniami zawartej umowy powierzenia przetwarzania danych osobowych:

………

………………

Stwierdzone niezgodności przetwarzania powierzonych danych osobowych z wytycznymi i rekomendacjami organów nadzorczych oraz organów doradczych w zakresie ochrony danych i prywatności

………

………………

Rekomendacje:

………

………………

11. Załączniki:

1) Formularz audytu podmiotu przetwarzającego z dnia .../.../.....

.....

Data i podpis

WÓJT
Paweł Gibczyński

Ogólny opis organizacyjnych środków bezpieczeństwa

ŚRODKI ORGANIZACYJNE		
LP.	Stosowane środki organizacyjne	Uwagi
1.	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.	tak, szkolenia
2.	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.	Tak
3.	Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy.	Tak
4.	Wyznaczono Inspektora Ochrony Danych (IOD)	Tak
5.	Wyznaczono Administratora Systemów Informatycznych	Tak
6.	Opracowano i wdrożono Politykę ochrony danych osobowych.	Tak
7.	Opracowano i wdrożono procedurę nadawania upoważnień do przetwarzania danych osobowych.	Tak
8.	Wprowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych.	Tak
9.	Opracowano i wdrożono zasady retencji danych.	Tak
10.	Opracowano i wdrożono procedurę postępowania z incydentami.	Tak
11.	Opracowano i wdrożono procedury realizacji praw osób, których dane dotyczą.	Tak
12.	Opracowano i wdrożono procedurę oceny skutków dla ochrony danych *(data protection impact assessment)*.	Tak
13.	Opracowano i wdrożono procedury *privacy by design* oraz *privacy by default.*	Tak
14.	Opracowano i wdrożono rejestr czynności przetwarzania administratora	Tak
15.	Opracowano i wdrożono rejestr kategorii czynności przetwarzania procesora	Nie
16.	INNE	

ŚRODKI OCHRONY FIZYCZNEJ		
LP	Stosowane środki ochrony fizycznej	Uwagi
1.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały drzwiami zwykłymi.	Tak
2.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały drzwiami antywłamaniowymi.	Nie
3.	Okna, w pomieszczeniach, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą krat.	Tak, na niskim parterze
4.	Okna, w pomieszczeniach, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą rolet antywłamaniowych.	Nie
5.	Okna, w pomieszczeniach, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą folii antywłamaniowej.	Nie
6.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą alarmu przeciwwłamaniowego.	Tak
7.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą systemu kontroli dostępu.	Tak - kasa oraz księgowość podatkowa
8.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą systemu monitoringu.	Nie ma, monitoring na zewnatrz budynku, wejście, klatka schodowa
9.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą nadzoru służby ochrony podczas nieobecności pracowników.	Tak
10.	Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone zostały za pomocą nadzoru służby ochrony.	Całodobowo
11.	Dane osobowe w formie papierowej przechowywane są na otwartych regałach.	Nie
12.	Dane osobowe w formie papierowej przechowywane są w zamkniętej niemetalowej szafie.	Tak
13.	Dane osobowe w formie papierowej przechowywane są w zamkniętej metalowej szafie.	Tak
14.	Dane osobowe w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej.	Tak
15.	Kopie zapasowe / archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej szafie.	Nie
16.	Kopie zapasowe / archiwalne danych osobowych przechowywane są w zamkniętej metalowej szafie.	Nie
17.	Kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.	Tak
18.	Dane osobowe przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.	Nie
19.	Pomieszczenia, w którym przetwarzane są dane osobowe zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.	Tak

20.	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.	Tak
21.	Komputery mobilne, na których przetwarzane są dane osobowe zabezpiecza się za pomocą kabli zabezpieczających.	Nie
22.	Komputery mobilne, na których przetwarzane są dane osobowe zabezpiecza się za pomocą szafek zabezpieczających.	Tak szafka na klucz
23.	Monitory komputerów ustawione zostały w sposób uniemożliwiający wgląd osobom nieupoważnionym.	Tak
24.	Monitory komputerów zabezpiecza się za pomocą filtrów prywatyzujących.	Nie
25.	INNE	

WÓJT
Paweł Gibczyński

WOLT

Privacy Policy

Załącznik nr 11

Ogólny opis technicznych środków bezpieczeństwa

ŚRODKI TECHNICZNE		
LP.	**Stosowane środki techniczne**	**Uwagi**
1.	zapora firewall	
2.	indywidualny login i hasło dla każdego użytkownika	
3.	uprawnienia dostępu dostosowane do potrzeb użytkowników	
4.	tworzenie kopii zapasowych	
5.	ochrona antywirusowa	
6.	mechanizm odnotowywania logów systemowych	
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

WÓJT
Paweł Gibczyński

Załącznik nr 12

Wyznaczenie Inspektora Ochrony Danych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy Człuchów z siedzibą w Człuchowie ul. Szczecińska 33 z dniem 01/04/2021 r.,

wyznaczam

Panią

do pełnienia funkcji **Inspektora Ochrony Danych (IOD)** w Urzędzie Gminy Człuchów w Człuchowie.

Upoważniam Panią do przetwarzania danych osobowych we wszystkich zbiorach Administratora Danych w zakresie niezbędnym dla należytego wykonywania funkcji Inspektora Ochrony Danych.

Zakres pozostałych obowiązków oraz warunki pełnienia funkcji Inspektora Ochrony Danych określone zostały w Polityce ochrony danych osobowych wdrożonej w Urzędzie Gminy Człuchów.

Data i podpis osoby wyznaczanej do pełnienia funkcji IOD

Data i podpis Administratora Danych

Odwołanie Inspektora Ochrony Danych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy Człuchów z siedzibą w Człuchowie ul. Szczecińska 33 z dniem .....

odwołuję

Panią / Pana .....

z pełnienia funkcji **Inspektora Ochrony Danych (IOD)** w Urzędzie Gminy Człuchów.

.....

Data i podpis osoby odwoływanej z pełnienia funkcji IOD

.....

Data i podpis Administratora Danych

WÓJT
Paweł Gibczyński

Załącznik nr 13

Wyznaczenie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy Człuchów z siedzibą w Człuchowie ul. Szczecińska 33 z dniem.....,

wyznaczam

Panią / Pana .....

do pełnienia funkcji **Administratora Systemów Informatycznych** w Urzędzie Gminy Człuchów w Człuchowie.

Zakres obowiązków oraz warunki pełnienia funkcji Informatyka określone zostały w Polityce ochrony danych osobowych wdrożonej w Urzędzie Gminy Człuchów.

Data i podpis osoby wyznaczanej do pełnienia funkcji ASI

Data i podpis Administratora Danych

WÓJT
Paweł Gibczyński

Odwołanie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - Urząd Gminy Człuchów z siedzibą w Człuchowie ul. Szczecińska 33 z dniem.....,

odwołuję

Panią / Pana .....

z pełnienia funkcji **Administratora Systemów Informatycznych** w Urzędzie Gminy Człuchów w Człuchowie.

Data i podpis osoby odwoływanej z pełnienia funkcji ASI	Data i podpis Administratora Danych

WÓJT
Paweł Gibczyński

Zasady retencji danych osobowych

RODO nakłada na Administratora Danych obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Po osiągnięciu celu dane osobowe powinny zostać usunięte lub poddane anonimizacji. W tym celu, Administrator Danych jest zobowiązany do stałego nadzorowania zawartości administrowanych zbiorów danych oraz występujących w ich ramach procesów przetwarzania, pod kątem konieczności usuwania danych zbędnych, albo do których przetwarzania przestał być upoważniony.

Zasady ustalania okresu retencji danych osobowych

1. Ustalając okres retencji danych osobowych należy od początku procesu przetwarzania ustalić jego cel i stale monitorować czy z upływem czasu cel ten jest nadal aktualny.
2. Ustalając okres retencji należy wziąć pod uwagę, czy przepisy szczególne nie określają przez jaki czas należy przechowywać dane (np. prawo pracy). W sytuacji, gdy do jednego procesu przetwarzania danych osobowych zastosowanie mają różne przepisy, należy wybrać przepis najbardziej adekwatny.
3. W sytuacji, gdy nie ma przepisów prawa ustalających okres retencji, Administrator Danych jest zobowiązany do samodzielnego ustalenia okresów retencji dla poszczególnych procesów na zasadzie adekwatności. Należy również mieć na uwadze fakt, że z upływem czasu przydatność danych maleje, a dane często stają się nieaktualne.
4. Należy ustalić, kiedy rozpoczyna się i kończy okres retencji:
   4.1. w sytuacji, gdy można określić dokładnie początek okresu retencji (np. otrzymanie danych) należy wyliczyć okres retencji zgodnie z wewnętrznymi regulacjami (np. 3 lata po zebraniu danych, 10 lat po wygaśnięciu umowy o pracę),
   4.2. w sytuacji, gdy nie jest możliwe dokładnie określenie początku okresu retencji, jej koniec powinno określać konkretne zdarzenie (np. CV kandydatów powinny być usunięte niezwłocznie po zakończeniu procesu rekrutacji).
5. W pewnych sytuacjach okres retencji może ulegać wydłużeniu lub skróceniu:
   5.1. okres retencji ulega wydłużeniu np. gdy dane są przetwarzane dla dwóch różnych celów (tj. wykonanie umowy i dla celów dowodowych),
   5.2. okres retencji ulega skróceniu np. gdy osoba, której dane dotyczą wniesie zasadny sprzeciw wobec przetwarzania jej danych osobowych albo właściwy organ publiczny zwróci się z żądaniem usunięcia określonych danych – w takiej sytuacji należy zdecydować jakie dane należy usunąć, a jakie zostawić, ze względu na nadrzędny cel np. przepis prawa.
6. Należy wprowadzić wewnętrzne regulacje, które określą okresy retencji dla wszystkich procesów przetwarzania danych osobowych. Przy określeniu okresu retencji należy wziąć pod uwagę, w szczególności:
   6.1. rodzaj danych osobowych,

6.2. cel przetwarzania,

6.3. właściwe przepisy prawa.

7. Należy ustalić osoby odpowiedzialne za retencje danych osobowych w poszczególnych procesach przetwarzania danych osobowych.

Zasady stosowania retencji danych osobowych

1. Rozpoczynając proces usuwania danych należy wziąć pod uwagę czas, który jest potrzebny na znalezienie i usunięcie tych danych (np. jeżeli uznaje się, że usuniecie danych zajmie tydzień, należy rozpocząć ten proces najpóźniej tydzień przed upływem okresu retencji).

2. Należy ustalić metody usuwania danych, uwzględniając podział na dane osobowe przechowywane w formie papierowej i elektronicznej oraz mając na uwadze przepisy prawa i inne regulacje wewnętrzne.

Anonimizacja jako alternatywa dla usuwania danych osobowych

1. W sytuacji, gdy kończy się okres retencji, a dane są nadal potrzebne (np. do celów statystycznych czy analitycznych) można zachować te dane pod warunkiem ich anonimizacji.

2. Anonimizacja oznacza przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej albo jeżeli przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań.

WÓJT
Paweł Gibczyński

Załącznik nr 15

Polityka czystego biurka i czystego ekranu

1. Niniejsza Polityka czystego biurka i czystego ekranu (dalej: Polityka) obowiązuje wszystkich pracowników Urzędu Gminy Człuchów, od dnia 11.02.2022r. na terenie całego zakładu pracy.

2. Na potrzeby niniejszej Polityki za pracowników Administratora Danych uważa się pracowników w rozumieniu art. 2 ustawy z 26 czerwca 1974 r. – Kodeks Pracy zatrudnionych u Administratora danych oraz wszystkie pozostałe osoby, które wykonują u Administratora Danych pracę na innej podstawie niż stosunek pracy, a także osoby prowadzące jednoosobowe działalności gospodarcze współpracujące z Administratorem Danych oraz osoby, które zostały przyjęte na praktyki.

3. Pracownicy zobowiązani są do przechowywania na biurku tylko tych dokumentów, które są im niezbędne w danym momencie do wykonania bieżących zadań.

4. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy. Klucz do szafy należy odłożyć w wyznaczone miejsce lub przekazać innemu pracownikowi. Na osobę, której klucz powierzono, przechodzi pełna odpowiedzialność za realizację Polityki.

5. Obowiązki określone w pkt 4 pracownik powinien wykonać również w przypadku gdy musi opuścić stanowisko pracy na czas dłuższy niż 1 godzina.

6. W sytuacjach nagłych, związanych w szczególności ze stanem zdrowia pracownika lub przedłużającą się nieobecnością w biurze, za realizację Polityki w jego imieniu odpowiadają solidarnie pracownicy, którzy go zastępują.

7. Pracownik może pozostawić na biurku jedynie telefon stacjonarny oraz materiały biurowe, takie jak np. długopis, zszywacz.

8. Obowiązuje zakaz trzymania na biurku wszelkich produktów spożywczych, których posiadanie grozi rozlaniem płynu.

9. Pracownik zobowiązany jest na bieżąco niszczyć te dokumenty, które przestały mu być potrzebne. Dokumenty powinny być niszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji.

10. Pracownik jest zobowiązany do ustawienia wygaszacza ekranu na użytkowanym przez niego komputerze. Wygaszacz powinien włączać się automatycznie po okresie bezczynności użytkownika, trwającym nie dłużej niż 5 minut.
    W przypadku wznowienia aktywności, powrót do pracy z komputerem powinien być możliwy jedynie po podaniu odpowiedniego hasła.

11. W przypadku czasowego opuszczenia stanowiska pracy, pracownik jest zobowiązany do każdorazowego blokowania komputera poprzez włączenie wygaszacza ekranu.

12. Po zakończeniu pracy pracownik powinien wylogować się z systemu.

WÓJT
Paweł Gibczyński