POLITYKA

BEZPIECZEŃSTWA INFORMACJI
-DANYCH OSOBOWYCH-

zgodnie z Rozporządzeniem Parlamentu Europejskiego i Spółka (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).

Rozdzielnik:	Dokument do użytku wewnętrznego
Podmiot: **ADMINISTRATOR DANYCH**	**Improvement Factory Sp. z o.o.** ul. Kręta 1 80-217 Gdańsk
Wersja:	Nr 2
z dnia:	21.05.2025 r
Zatwierdził(a):	..... podpis administratora danych

Spis treści

Procedura zarządzania uprawnieniami
Procedura monitoringu
Procedura pseudonimizacji i szyfrowania danych
Obowiązywanie dokumentu
Wykaz załączników

1. Postanowienia ogólne

Zgodnie z Art. 4 ust. 7 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: „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Administrator danych – **Improvement Factory Sp. z o.o.** ul. Kręta 1 80-217 Gdańsk samodzielnie ustala cele i sposoby przetwarzania danych osobowych".

Polityka Bezpieczeństwa rozumiana jest jako wykaz praw, reguł i wewnętrznych praktyk regulujących sposób zarządzania i ochrony danych osobowych przetwarzanych przez **Improvement Factory Sp. z o.o.** ul. Kręta 1 80-217 Gdańsk **(dalej: Spółka)**
Dokument obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

2. Podstawa prawna

1. Polityka Bezpieczeństwa została opracowana na podstawie:
    a. 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)
    b. Ustawa z 10 maja 2018 r o ochronie danych osobowych (Dz. U 2018 poz. 1000 z póź. Zmianami)
    c. Pozostałe przepisy regulujące system ochrony danych osobowych, w tym przepisy wydane na podstawie art. 40 RODO.
2. Administratorem danych osobowych jest **Improvement Factory Sp. z o.o.** ul. Kręta 1 80-217 Gdańsk
3. Dane są chronione zgodnie z polskim prawem oraz procedurami dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

4. Deklaracja

1. Administrator danych mając świadomość, iż przetwarza dane osobowe deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
2. Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w Motywie 39 RODO oraz artykule 5 ust. 1 ppkt a) – e) RODO.
3. Każdy pracownik upoważniony do przetwarzania danych, świadomy odpowiedzialności, zobowiązany jest postępować zgodnie z przyjętymi zasadami i minimalizować zagrożenia wynikające z błędów ludzkich.

4. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.
5. Dane osobowe w podmiocie przetwarzane są w sposób legalny, zgodny z celem przetwarzania tj.:
    a. w celu zawarcia i realizacji ewentualnej umowy pomiędzy Użytkownikiem, a Administratorem oraz obsługi Użytkownika jako klienta Administratora zgodnie z art. 6 ust. 1 lit. b) RODO;
    b. w celu prowadzenia rozliczeń finansowych z Użytkownikiem będącym klientem Administratora tytułem realizacji ewentualnej umowy zawartej między stronami, a także ewentualnego dochodzenia roszczeń od Użytkownika będącego klientem w ramach prawnie uzasadnionego interesu Administratora zgodnie z art. 6 ust. 1 lit. f) RODO oraz spełnienia obowiązków prawnych Administratora wobec organów podatkowych na podstawie odrębnych przepisów zgodnie z art. 6 ust. 1 lit. c) RODO;
    c. w celu realizacji działań marketingowych Administratora w ramach prawnie uzasadnionego interesu Administratora w rozumieniu art. 6 ust. 1 lit. f) RODO, a także zgodnie z oświadczeniami woli dotyczącymi komunikacji marketingowej złożonymi wobec Administratora. Zgody udzielone w zakresie komunikacji marketingowej (np. na przesyłanie informacji handlowych drogą elektroniczną lub kontakt telefoniczny w celach marketingu bezpośredniego) mogą być wycofane w dowolnym czasie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
    d. w celu realizacji obowiązków prawnych Administratora wobec Użytkownika określonych w RODO, w rozumieniu art. 6 ust. 1 lit. c) RODO.
6. Zakres pozyskiwanych danych wynika z przepisów prawa, o których mowa w pkt 1 niniejszego dokumentu i jest adekwatny do zdefiniowanych celów przetwarzania.

5. Cel

1. Celem niniejszego dokumentu jest wprowadzenie spójnych zasad zachowania bezpieczeństwa danych osobowych przetwarzanych przez **Spółkę.**

2. Polityka bezpieczeństwa informacji jest dokumentem podstawowym z zakresu ochrony danych osobowych przyjętych w Spółce.

3. Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym dane oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy Radnych oraz pracowników obsługujących **Spółkę**, oraz sieci informatycznej w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Osoby mające dostęp do systemu, przetwarzające dane osobowe są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.

4. Zastosowanie niniejszej Polityki Bezpieczeństwa Informacji powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do wyników szacowania ryzyka występującego dla przetwarzanych i przechowywanych danych oraz w systemach informatycznych wykorzystywanych przez **Improvement Factory.**

5. Polityka Bezpieczeństwa Informacji jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników, podmiotów trzecich, które na mocy zawartych umów mają dostęp do

informacji chronionych. Ma ona pomóc w zapewnieniu: poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.

6. Zakres stosowania

1. Politykę Bezpieczeństwa Informacji stosują osoby przetwarzające dane osobowe i inne dane chronione, niezależnie od funkcji. W szczególności mogą być to osoby realizujące pracę na rzecz **Spółki** bez względu na jej formę.
2. Polityka Bezpieczeństwa Informacji obejmuje wszystkie dane osobowe oraz inne informacje podlegające ochronie, przetwarzanych przez Spółkę niezależnie od formy ich przetwarzania. Polityka w zakresie danych osobowych odnosi się:
   a) do danych przetwarzanych w zbiorach tradycyjnych – w tym dokumentacji medycznej, w szczególności kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
   b) do danych przetwarzanych w systemach informatycznych.
3. Dla skutecznej realizacji Polityki Bezpieczeństwa Informacji, Administrator zapewnia:
   a) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony realizowane w przyjętych formach (samokształcenie, szkolenie stacjonarne, szkolenie z wykorzystaniem nowych technik itp.),
   b) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,
   c) okresową ocenę skutków dla ochrony danych osobowych – o ile komunikat Prezesa UOD będzie tych kategorii danych dotyczył,
   d) kontrolę, monitoring i nadzór nad przetwarzaniem danych osobowych,
   e) monitorowanie zastosowanych środków ochrony,
   f) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, w tym między innymi w stosownym przypadku:
      - pseudonimizację i szyfrowanie danych osobowych;
   g) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   h) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   i) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

7. Definicje przyjęte w analizie legalności przetwarzania danych osobowych

1. *Administrator danych* (AD)- **Improvement Factory Sp. z o.o.** ul. Kręta 1, 80-217 Gdańsk
2. *Administrator Systemu Informatycznego ASI* - pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów informatycznych;

3. *dane osobowe* - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4. *dostępność danych* - rozumie się przez to właściwość zapewniającą, że dane są udostępniane dla upoważnionego podmiotu wtedy, gdy ich potrzebuje do przetwarzania;
5. *integralność danych* – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
6. *naruszenie bezpieczeństwa informacji* – wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, obniżenia wymaganego poziomu poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet jeżeli nie prowadzą do negatywnych skutków dla organizacji. Zdarzenia lub działania, które mogą prowadzić do naruszenia praw lub wolności osób fizycznych;
7. *Koordynator Ochrony Danych (KOD)* - osoba powołana przez administratora danych, którego zadaniem jest nadzór nad przetwarzaniem danych osobowych oraz realizacja zadań wskazanych dla Koordynatora ochrony danych (art. 39 RODO);
8. *naruszenie ochrony danych osobowych* - 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;
9. *odbiorca danych* – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem powszechnie obowiązującym, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych, mającymi zastosowanie stosownie do celów przetwarzania. Przy czym przez sformułowanie „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
10. *osoba upoważniona do przetwarzania danych osobowych* – osoba, która złożyła do AD oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez AD, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;
11. *podmiot przetwarzający* – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
12. *przetwarzanie* - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
13. *poufność danych* - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane

nieupoważnionym podmiotom;

14. *rozliczalność danych* - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
15. *RODO* - 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);
16. *usuwanie danych* – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
17. *uwierzytelnianie* – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
18. *użytkownik* - osoba przetwarzająca dane w systemie oraz poza nim, niezależnie od formy zatrudnienia;
19. *zbiór danych* – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
20. *Zgoda na przetwarzanie danych osobowych* - oświadczenie woli osoby, której dane są przetwarzane przez administratora danych, w której wyraża swoją aprobatę dla tego procesu;
21. *Wykaz przetwarzanych zbiorów (RCP – Rejestr Czynności Przetwarzania)* – **Spółka** nie spełnia wskazania dot. RCP wskazanego w art. 30 ust 5 RODO jednak celem dochowania należytej staranności nadzoru nad przetwarzanymi danymi RCP prowadzi.

8. Obowiązki osób przetwarzających dane osobowe

1. Każda osoba przetwarzająca dane osobowe na potrzeby **Spółki** jest obowiązana zapoznać się z treścią Polityki Bezpieczeństwa oraz bezwzględnie stosować się do jej zapisów. Osoby przetwarzające dane osobowe czynią to na podstawie wydanego przez Administratora Danych - upoważnienia (załącznik nr 1 do niniejszej Polityki).
2. Użytkownicy są zobowiązani do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:
   a) bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
   b) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,
3. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z RODO, czy Ustawy, stosuje się przepisy tych ustaw.
4. Użytkownicy przetwarzający dane osobowe obowiązani są dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:
   a) przetwarzane zgodnie z powszechnie obowiązującym prawem i regulacjami wewnętrznymi,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

e) oraz by wypełniany był obowiązek informacyjny, w przypadkach wskazanych w przepisach prawa powszechnie obowiązującego.

5. Naruszenie postanowień Polityki Bezpieczeństwa Informacji może skutkować zablokowaniem dostępu użytkownika do informacji chronionych i systemów. W przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego lub karnego. W przypadku poniesienia strat w wyniku naruszenia, **Spółka** może dochodzić roszczeń odszkodowawczych na drodze sądowej.
6. W razie wykrycia naruszenia ochrony informacji chronionych każdy użytkownik ma obowiązek postępować zgodnie z procedurami zawartymi w Dokumentacji.
7. Cofnięcie upoważnień do przetwarzania informacji chronionych powinno nastąpić niezwłocznie po zakończeniu pracy bez względu na formę jej świadczenia.
8. Rozliczenie użytkownika z aktywów związanych z przetwarzaniem informacji chronionych powinno odbywać się na podstawie procedur określonych przez Administratora Danych.

9. Obszary przetwarzania danych osobowych

1. W **Spółce** dane osobowe przetwarzane są w ramach zbiorów danych osobowych, a obszary możliwego przetwarzania danych osobowych określa załącznik nr 2 do niniejszej Polityki Bezpieczeństwa Informacji.
2. Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane tylko w wyznaczonych do tego miejscach z zachowaniem dedykowanego do tej czynności - sprzętu oraz wszelkich innych urządzeń.
3. Wynoszenie zbiorów danych osobowych (danych osobowych w każdej postaci) poza obszar przetwarzania możliwy jest za wyłączną zgodą Administratora Danych.

10. Charakterystyka zbiorów danych osobowych

1. Wykaz prowadzonych w **Spółce** zbiorów danych osobowych (RCP) stanowi załącznik nr 3 do niniejszej Polityki Bezpieczeństwa Informacji.
2. Przetwarzanie danych osobowych, zgodnie z celem działalności, jest możliwe, jeżeli jest to niezbędne do wypełnienia usprawiedliwionych interesów Administratora, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Przetwarzanie jest również dozwolone, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych lub 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. W szczególności można przetwarzać dane osobowe, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, a także gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
3. Osoby przetwarzające zgromadzone dane są zobowiązane w szczególności do:

a) przetwarzania danych zgodnie z aktami prawa powszechnie obowiązującego lub aktami prawa wewnętrznego, w zakresie zgodnym z upoważnieniem podpisanym przez Administratora;

b) przechowywania danych osobowych we właściwych zbiorach danych, zgodnie z celem utworzenia zbiorów;

c) modyfikowania i usuwania danych, zgodnie z wnioskiem złożonym przez osobę, której dane dotyczą oraz ograniczenia przetwarzania danych.

11. Organizacja systemu ochrony danych osobowych

1. Administrator Danych Osobowych odpowiada za zakres i bezpieczeństwo przetwarzania danych osobowych w **Spółce.** Spółka jest podmiotem prawa handlowego.
2. Administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie (tzw. zasada rozliczalności RODO). Administrator zapewnia:

   a) przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"),

   b) zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu").

   c) adekwatność danych osobowych; dane osobowe powinny być stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

   d) prawidłowość danych osobowych i w razie potrzeby ich uaktualnianie; podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").

   e) przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").

   f) przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

   g) Administrator danych zapewnia i stosuje odpowiednie środki informatyczne, techniczne i organizacyjne (wykaz w/w środków stanowi załącznik nr 8 do niniejszej Polityki), zapewniając ochronę przetwarzanych danych osobowych odpowiednią do wyników analizy ryzyka, a w szczególności:

      - podejmuje decyzje o celach i środkach przetwarzania danych osobowych,
      - podejmuje decyzje o technicznych i organizacyjnych zabezpieczeniach oraz wdraża zasady i procedury postępowania mające na celu zapewnienie adekwatnego poziomu

bezpieczeństwa przetwarzanych danych,

- upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków,
- podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych,
- prowadzi kontrolę przestrzegania procedur przetwarzania danych osobowych,
- zapewnia środki techniczne oraz organizacyjne w celu zapewnienia działań wymaganych przez przepisy prawa dotyczące ochrony danych osobowych,
- zapewnia realizację praw osób, których dane osobowe są przetwarzane (m.in. prawo wglądu, poprawiania danych i wniesienia sprzeciwu wobec przetwarzanych danych),
- reprezentuje **Spółkę** w postępowaniach przed organami publicznymi oraz w kontaktach z podmiotami trzecimi w sprawach związanych z pozyskiwaniem, przetwarzaniem, ochroną i powierzeniem danych osobowych,
- zapewnia bezpieczne usunięcie danych osobowych w przypadku uzasadnionego żądania niezwłocznego usunięcia danych osobowych, bez zbędnej zwłoki.

3. Powołanie Koordynatora ochrony danych:

   a) Administrator wskazał **Koordynatora Ochrony Danych (dalej: KOD)**, który jest odpowiedzialny za nadzór nad stosowaniem środków organizacyjnych i technicznych, zapewniających ochronę przetwarzanych danych, w szczególności przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, kradzieżą, uszkodzeniem lub zniszczeniem.

4. Obowiązki **Koordynatora Ochrony Danych**:

   a) Koordynator Ochrony Danych realizuje obowiązki w imieniu i z upoważnienia Administratora zgodnie z wymaganiami obowiązującego prawa przy uwzględnieniu ryzyka i oceny skutków związanych z czynnościami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania,

   b) Koordynator Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z przepisami prawa powszechnie obowiązującego i regulacjami wewnętrznymi,

   c) Koordynator Ochrony Danych zobowiązany jest w szczególności do:

   - informowania Administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy powszechnie obowiązujących przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych i doradzanie im w tej sprawie,
   - nadzorowania i monitorowania przestrzegania przepisów prawa o ochronie danych oraz aktów prawa wewnętrznego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu Administratora i podmiotów trzecich uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów,
   - udziału w ocenie skutków dla ochrony danych zgodnie z art. 35 RODO oraz monitorowanie wykonania zaleceń opracowanych w wyniku wykonania oceny (o ile ma zastosowanie zgodnie z komunikatem Prezesa UOD),
   - weryfikacji zgodności przetwarzania danych osobowych z przepisami o ochronie danych

osobowych.

- aktualizowania Polityki Bezpieczeństwa Danych Osobowych oraz dokumentów związanych z przetwarzaniem danych osobowych,
- wspieranie administratora w przygotowywaniu odpowiedzi na żądania osób, których dane dotyczą, uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, uzyskanie dostępu do nich wraz z zakresem właściwych informacji o danych osobowych,
- informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania osób, które wystąpiły z takim żądaniem,
- prowadzenia i aktualizacji rejestru naruszeń bezpieczeństwa, zgodnie ze wzorem wskazanym w załączniku do Polityki Bezpieczeństwa Informacji,
- przygotowania i przekazywania do podpisu do Administratora zgłaszania o naruszeniu ochrony danych osobowych do organu nadzorczemu oraz zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych – zgodnie z postanowieniami art. 33 i 34 RODO,
- prowadzenia i aktualizacji rejestru umów powierzenia przetwarzania danych, zgodnie ze wzorem wskazanym w załączniku do Polityki Bezpieczeństwa Informacji (o ile ma zastosowanie),
- nadzorowania i monitorowania procesu profilowania (o ile taki ma miejsce),
- nadzorowania i monitorowania realizacji obowiązku informacyjnego, zgodnie z wymogami RODO,
- informowanie Administratora o wystąpieniu incydentu,
- gromadzenia potwierdzenia (dotyczy formy papierowej) wywiązania się z obowiązku informacyjnego oraz weryfikacji prawidłowości gromadzenia potwierdzeń w systemach informatycznych,

d) Koordynator Ochrony Danych jest uprawniony w szczególności do:

- wstępu do pomieszczeń, w których przetwarzane są dane osobowe,
- odbierania wyjaśnień od osób przetwarzających dane osobowe,
- dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania jego zadań wynikających z RODO, Ustawy, aktów prawa wewnętrznego i zakresu jego obowiązków/zakresu umowy o świadczenie usług.

5. Sposób udzielania upoważnień do przetwarzania danych osobowych:

a) Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby upoważnione przez Administratora w rozumieniu art. 29 RODO. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

- przed rozpoczęciem przetwarzania należy złożyć oświadczenie o zapoznaniu się z dokumentacją ochrony danych osobowych
- dane osobowe można przetwarzać wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych, zawartym w upoważnieniu i tylko w celu wykonywania obowiązków służbowych,
- przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia lub

świadczenia pracy, przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres świadczenia pracy, a także po jego zakończeniu,

- stosowanie określonych przez Administratora procedur oraz wytycznych mających na celu przetwarzanie danych zgodnie z obowiązującym prawem,
- zabezpieczenie danych osobowych przed udostępnieniem osobom nieupoważnionym,
- W przypadku naruszenia przez użytkownika przepisów lub zasad postępowania może podlegać on odpowiedzialności statutowej i karnej,

6. Zbieranie danych osobowych:
   a) Dane osobowe przetwarzane w **Spółce** są pozyskiwane bezpośrednio od osób, których te dane dotyczą (radni, petenci, osoby uczestniczące w sesjach, pracownicy, strony umów cywilno-prawnych). W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy zapewnić, że istnieje podstawa prawna przetwarzania danych,
   b) Przetwarzanie i przechowywanie danych osobowych powinno odbywać się w postaci umożliwiającej identyfikację osób, których dotyczą.
   c) Przetwarzanie i przechowywanie danych osobowych powinno odbywać się nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.
   d) Dane osobowe, które są zbierane powinny być merytorycznie poprawne.
   e) Zakres danych osobowych, które są zbierane, powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.
   f) Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy uprzednio zostaną poddane procesowi anonimizacji, czyli procesowi, który ma na celu uniemożliwienie identyfikacji osób, których dotyczą dane.
   g) Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy odpowiedni przepis prawa wymaga ich archiwizacji przez określony czas.
   h) Przetwarzanie danych osobowych kandydata do pracy (bez względu na formę zatrudnienia) jest możliwe podczas procesu rekrutacji wyłącznie po uzyskaniu jego pisemnego oświadczenia zawierającego zgodę na przetwarzanie jego danych osobowych w celu przeprowadzenia procesu. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu procesu dokumenty zawierające dane osobowe kandydatów są archiwizowane zgodnie z zapisami tych przepisów.
   i) zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
7. Obowiązek informacyjny:
   a) Administrator zobowiązany jest na etapie gromadzenia danych (niezależnie od tego, czy zbiera je bezpośredniego od osób, których one dotyczą, czy też pozyskania ich od podmiotu trzeciego) powiadomić osoby, których dane gromadzi o przysługujących im prawach oraz przekazać informacje o zasadach i celu przetwarzania danych osobowych (wypełnienie „obowiązków informacyjnych" wskazanych w art. 12, 13, 14, 22 i 25 RODO),
   b) zgodnie z art. 13 ust. 1 i 2 RODO, do niezbędnych elementów informacyjnych zaliczyć należy podanie:
      - nazwy i adresu Administratora oraz adresu poczty elektronicznej i numeru faksu i telefonu

oraz gdy ma to zastosowanie, tożsamości i danych kontaktowych przedstawiciela Administratora,

- celu przetwarzania danych osobowych oraz podstawy prawnej przetwarzania,
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców,
- informacji o zamiarze transferu danych osobowych do państwa trzeciego, ze szczególnym uwzględnieniem:
  - ✓ przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
  - ✓ stwierdzenia lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub - w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO - wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
- informacji 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;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
- informacji o prawie wniesienia skargi do organu nadzorczego;
- informacji 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;
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
- W przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO, informacja powinna być poszerzona o:
  - ✓ kategorie odnośnych danych osobowych;
  - ✓ źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

c) Informacje, o której mowa w pkt b każdorazowo należy skutecznie osobie, której dane dotyczą przed podjęciem działań z jej danymi – zamieszczenie na stronie internetowej - BIP. Klauzula powinna być zrozumiała dla osób, których dane mają być gromadzone i przetwarzane.

d) Informowanie powinno się dokonać bez prośby zainteresowanego. Powinno być ono wykonane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy uwzględniać także to, że informowana osoba musi mieć możliwość wniesienia sprzeciwu wobec przetwarzania jej danych i należy stworzyć jej warunki do wyrażenia tego sprzeciwu.

e) Wykonanie obowiązku informacyjnego jest zadaniem osoby realizującej procesy (np. catering, zatrudnienie, zawieranie umów itp.).

8. Informowanie o przetwarzanych danych osobowych:

   a) Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w **Spółce**, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.

   b) Na wniosek osoby, której dane dotyczą, Administrator Danych jest zobowiązany do udzielania informacji zgodnie z pkt. a Informacja powinna być udzielona formie pisemnej oraz powszechnie zrozumiałej.

   c) W razie wniesienia żądania oraz wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych osobowych, bez zbędnej zwłoki, dokonać uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.

   d) Osoba, której dane dotyczą, ma prawo wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach przetwarzania niezbędnego do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnego dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

9. Powierzanie przetwarzania danych osobowych:

   a) Administrator:

      - udostępnia dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego, w szczególności do: **Urządu skarbowego, ZUS itp**.

      - powierza przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej w na piśmie, która określa zasady przetwarzania i zabezpieczenia danych osobowych np. **obsługa podatkowa, informatyczna**.

   b) Umowa powierzenia danych osobowych do przetwarzania musi być zawarta w formie pisemnej w dwóch jednobrzmiących egzemplarzach dla obu stron.

   c) W przypadku zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem trzecim, AD jednocześnie zobowiązuje ten podmiot w formie pisemnej do zachowania poufności powierzanych do przetwarzania danych osobowych oraz sposobów ich zabezpieczeń. Zobowiązanie powinno pozostać w mocy również po zakończeniu przetwarzania.

   d) Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

   e) Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie ryzyka dla danych objętych ochroną, a w szczególności powinien stosować techniczne i organizacyjne środki bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

10. Współadministrowanie danymi:

    a) W przypadku wspólnego przetwarzanie danych w zbiorach przez **Spółkę** z innym podmiotem, na mocy zawartej umowy lub porozumienia, ustalają one wspólnie cele i sposoby przetwarzania

danych (są współadministratorami danych). W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów prawa powszechnie obowiązującego oraz aktów prawa wewnętrznego obowiązujących w obu podmiotach, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo powszechnie obowiązujące. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

b) Zgodnie z zasadami wskazanymi powyżej Spółka współadministruje danymi w ramach **Grupy ASTOR** wspólnym systemem sprzedaży i marketingu, zwanego dalej **„wspólnym systemem sprzedaży i marketingu w Grupie ASTOR"**

c) Uzgodnienia, o których mowa w pkt a, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a osobami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana osobom, których dane dotyczą.

d) Niezależnie od uzgodnień, o których mowa w pkt a, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z przepisów prawa powszechnego wobec każdego z Administratorów.

11. Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej:

a) Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

b) W razie braku decyzji, o której mowa w pkt 1 Administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowane prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.

c) W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w pkt 1 oraz braku odpowiednich zabezpieczeń, o których mowa w pkt 2, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:

- osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,
- przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przed umownych podejmowanych na żądanie osoby, której dane dotyczą,
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną,
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
- przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do

wyrażenia zgody lub przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

- Szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej określone zostały w RODO. O wyrażenie zgody do organu nadzorczego na przekazanie danych występuje Administrator danych, wskazując cel i zakres przekazywanych danych. Administrator zobowiązany jest bezwzględnie przestrzegać postanowień RODO przy przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.

12. Ciągłość działania

Strategia zachowania ciągłości działania jest opracowywana na podstawie zebranych podczas analizy ryzyka i wpływu na działanie wymagań dotyczących parametrów odtworzenia z uwzględnieniem celów i dostępnych zasobów.

Wprowadzenie i utrzymanie systemu ciągłości działania

Efektywność systemu ciągłości działania realizuje się poprzez następujące działania:
testowanie – cykliczne sprawdzanie skuteczności planu ciągłości działania. Testy są także efektywną metodą szkolenia i budowania świadomości na wszystkich szczeblach organizacji.
aktualizację – regularne sprawdzanie i dostosowanie do zmieniających się warunków wewnętrznych i zewnętrznych, umożliwia utrzymanie efektywnego planu działania na wypadek sytuacji kryzysowej.
Odpowiedzialny: Administrator Systemu Informatycznego
audyt – pozwala na stwierdzenie czy spełnia on wymogi zgodności z przyjętą polityką ochrony danych – instrukcją ciągłości działania, przepisami prawa oraz normami i rekomendacjami regulatorów.
Odpowiedzialni: Koordynator Ochrony Danych, Administratora Systemu Informatycznego
Szkolenia i akcje informacyjne – system powinien realizować zadania szkoleniowe: ogólne dla wszystkich radnych oraz specjalistyczne dla osób odpowiedzialnych za bezpieczeństwo informacji w Spółce. Szkolenia ogólne powinny być wspierane okresowymi akcjami informacyjnymi, których głównym celem jest budowanie świadomości pracowników.
Odpowiedzialni: Koordynator ochrony danych, Administrator Systemu Informatycznego, Pracownik wskazany przez AD odpowiedzialny za sprawy organizacyjno-administracyjne.

Dla Spółki przewidziano konieczność zabezpieczenia możliwości ciągłości działania dla następujących elementów:

1. z wykorzystaniem systemów informatycznych,
2. bez udziału systemów informatycznych

Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych z udziałem systemów

Informatycznych:

A Zapewnienie ciągłości pracy systemów informatycznych

1. Wprowadza się poniższą procedurę zgłaszania awarii systemów informatycznych wykorzystywanych do przetwarzania danych osobowych w Spółce.
2. Każdy z użytkowników systemu informatycznego, w sytuacji wystąpienia awarii tego systemu, ma obowiązek niezwłocznego zgłoszenia awarii tego systemu Administratorowi. Zgłoszeń należy dokonywać na adres mailowy Administratora lub numer telefonu.
3. Administrator zawiadamia niezwłocznie o wystąpieniu awarii osobę obsługującą Spółkę pod względem informatycznym.
4. Czas reakcji i czas naprawy określają uzgodnienia pomiędzy **Spółką,** a podmiotem wykonującym naprawy, z zastrzeżeniem, że podjęcie czynności naprawczych nie powinno zostać podjęte później niż 2 godziny od zgłoszenia awarii.
5. Do czasu usunięcia awarii systemu informatycznego, **Spółka** wykorzystuje dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.
6. Wzór dokumentacji papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia danych osobowych do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.
7. Po usunięciu awarii ASI weryfikuje prawidłowość bazy danych, która jest uzupełniana o informacje wytworzone za pomocą zastępczej dokumentacji papierowej.
8. W przypadku uszkodzenia bazy danych należy wykorzystać kopię zapasową w celu przywrócenia poprawności systemu informatycznego.
9. Z czynności mających na celu przywrócenie pracy systemu Administrator sporządza stosowną notatkę.

B Zapewnienie ciągłości pracy sprzętu, na którym przetwarzane są dane osobowe

1. Wprowadza się poniższą procedurę zgłaszania awarii urządzeń wykorzystywanych do przetwarzania danych osobowych w **Spółce**.
2. Każdy z użytkowników, w sytuacji wystąpienia awarii sprzętu służącego do przetwarzania danych osobowych ma obowiązek niezwłocznego zgłoszenia awarii tego sprzętu ASI. Zgłoszeń należy dokonywać na adres mailowy lub numer telefonu Administratora.
3. Podjęcie diagnostyki w celu eliminacji awarii powinno nastąpić nie później niż w ciągu 2 godzin od zgłoszenia awarii, a sama awaria powinna zostać usunięta w ciągu 24 godzin od daty jej wystąpienia.
4. Do czasu usunięcia awarii, **Spółka** wykorzystuje dokumentację papierową, która po usunięciu awarii jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu lub wykorzystywany jest inny sprzęt **Spółki**.
5. Jeżeli awarii nie da się usunąć w ciągu 24 godzin, Administrator danych zapewnia zapasowe urządzenie spełniające wymogi przepisów prawa i umożliwiające realizowanie zadań **Spółki**.

C Zapewnienie ciągłości pracy w przypadku braku zasilania elektrycznego w sieci energetycznej

1. Każdy użytkownik systemu ma obowiązek niezwłocznego zgłoszenia braku zasilania sieci energetycznej po jej wystąpieniu. Zgłoszeń należy dokonywać na adres mailowy, telefoniczny Administratora lub Koordynatora.
2. Komputery, na których przetwarzane są dane osobowe są komputerami przenośnymi i stacjonarnymi.
3. Użytkownik komputera przenośnego, o którym mowa w punkcie wyżej jest zobowiązany do takiej organizacji pracy, aby zapewnić przez cały jej okres maksymalny poziom naładowania baterii, która umożliwi jego pracę bez zasilania, co najmniej przez 2 godziny.
4. Jeżeli użytkownik podejrzewa, że naprawa dostawy prądu może wydłużyć się ponad czas naładowania baterii jest zobowiązany do bezpiecznego przerwania pracy i wyłączenia sprzętu komputerowego.
5. Jeżeli do przetwarzania danych osobowych użytkowane są komputery stacjonarne wyposażone są one w urządzenia UPS.
6. W przypadku braku zasilania użytkownik komputera stacjonarnego ma niezwłoczny obowiązek bezpiecznego zakończenia pracy i wyłączenia stacji roboczej.
7. W przypadku wystąpienia braku zasilania, jeśli serwer bazy danych nie ma takiej opcji, Administrator systemu lub upoważniony przez niego pracownik wyłącza serwer bazy danych.
   Strategia zachowania ciągłości działania jest opracowywana na podstawie zebranych podczas analizy ryzyka i wpływu na działanie wymagań dotyczących parametrów odtworzenia z uwzględnieniem celów i dostępnych zasobów.

13. PROCEDURA REAGOWANIA NA INCYDENTY W OBSZARZE DANYCH OSOBOWYCH

1. Celem Instrukcji jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania. Integralną częścią Instrukcji są procedury:
   Procedura wewnętrzna zgłaszania naruszeń ochrony danych osobowych
   Klasyfikacja naruszeń danych osobowych
   Procedura wewnętrznego rejestru naruszeń ochrony danych
   Procedura na wypadek wystąpienia wysokiego ryzyka naruszenia praw i wolności osób
   Procedura zgłaszania naruszeń ochrony danych do organu nadzorczego
   Procedura odtwarzania systemu po awarii oraz ich testowania

A) PROCEDURA WEWNĘTRZNA ZGŁASZANIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH.

1. **Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować przełożonego, Koordynatora Ochrony Danych (KOD), ASI lub AD.**
2. Do typowych incydentów w obszarze bezpieczeństwa danych osobowych należy:
   a. Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

b. Niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
c. Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
d. Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
e. Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
f. Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

3. **Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:**
   a. Stwierdzono złamanie zabezpieczenia systemu ochrony danych osobowych;
   b. Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.
4. W przypadku stwierdzenia incydentu (naruszenia), KOD prowadzi postępowanie wyjaśniające w toku, którego:
   a. Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
   b. Zabezpiecza ewentualne dowody;
   c. Ustala osoby odpowiedzialne za naruszenie;
   d. Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
   e. Inicjuje działania dyscyplinarne;
   f. Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości, dokumentuje prowadzone postępowanie.
5. **Osoba, która stwierdziła lub uzyskała informację wskazującą na naruszenie ochrony tego zbioru/ bazy danych zobowiązana jest do niezwłocznego:**
   a. Zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu;
   b. Jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania;
   c. Powiadomienia o tym fakcie ASI.
6. **ASI jest zobowiązany do niezwłocznego:**
   a. Przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.;
   b. Podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in. :

- fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
- wylogowania użytkownika podejrzanego o naruszenie ochrony danych;
- zmianę hasła na koncie administratora i użytkownika, poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.

c. Szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.

d. Przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy/ zbioru danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

7. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości:
   a. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
   b. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
   c. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne.

B) KLASYFIKACJA NARUSZEŃ DANYCH OSOBOWYCH.

1. Uchybienia i zagrożenia **niecelowe** wewnętrzne i zewnętrzne – załącznik nr 1.
   Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych **należą działania użytkowników danych lub osób nie będących pracownikami**, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności.
   W szczególności są to działania takie jak:
   a. Niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
   b. Niewłaściwe zabezpieczenie sprzętu komputerowego;
   c. Dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia;
   d. Pomyłki ASI;
   e. Kradzież danych;
   f. Kradzież sprzętu komputerowego;
   g. Działanie wirusów i innego szkodliwego oprogramowania oraz działania, wskutek którego dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.
2. Uchybienia i zagrożenia **celowe** wewnętrzne i zewnętrzne.
   Do uchybień i zagrożeń celowych wewnętrznych i zewnętrznych należą działania użytkowników danych, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub

naruszenia ich poufności. W szczególności są to działania takie jak:

a. Celowe zniszczenie danych osobowych lub nośników danych;
b. Kradzież danych osobowych;
c. Dopuszczenie do przetwarzania danych osoby nieposiadającej stosownych uprawnień;
d. Kradzież sprzętu informatycznego;
e. Działanie wirusów i innego szkodliwego oprogramowania oraz działania, wskutek którego dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

3. Zagrożenia losowe.

Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to sytuacje takie jak:

a. Klęski żywiołowe;
b. Przerwy w zasilaniu;
c. Awaria serwera, komputera;
d. Pożar;
e. Zalanie wodą.

C) PROCEDURA WEWNĘTRZNEGO REJESTRU NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

4. Administrator Danych poprzez KOD / ASI w przypadku stwierdzenia naruszenia:
   a. Odnotowuje każde uchybienie - DZIENNIK EWIDENCJI NARUSZENIA DANYCH OSOBOWYCH – wzór PB „Wzory dokumentów wykonawczych".
   b. Sporządza PROTOKÓŁ Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH - wzór PB „Wzory dokumentów wykonawczych".
   c. Wprowadza procedury uniemożliwiające ponowne powstanie incydentu.
5. AD/ KOD/ASI w przypadku stwierdzenia zagrożenia:
   a. Zabezpiecza dowody, powiadamia policję (w przypadku włamania);
   b. Zabezpiecza dane osobowe oraz nośniki danych;
   c. Odnotowuje każde uchybienie - DZIENNIK EWIDENCJI NARUSZENIA DANYCH OSOBOWYCH - wzór PB „Wzory dokumentów wykonawczych".
   d. Sporządza PROTOKÓŁ Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH - wzór PB „Wzory dokumentów wykonawczych".
   e. Wprowadza procedury uniemożliwiające ponowne powstanie zagrożenia;
   f. Podejmuje próbę przywrócenia stanu sprzed zaistnienia zagrożenia.

Załącznik nr 1

Poglądowy rejestr uchybień i zagrożeń oraz postępowanie osób funkcyjnych.

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1.	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić KOD. KOD sporządza protokół uchybienia.
2.	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić KOD. KOD sporządza protokół uchybienia.
3.	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić KOD, który sprawdza za pośrednictwem ASI system uwierzytelniania oraz sprawdza, czy nie doszło do kradzieży lub zniszczenia danych. KOD sporządza protokół uchybienia.
4.	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	KOD za pośrednictwem ASI zabezpiecza nośnik danych. KOD sporządza protokół zagrożenia. Należy powiadomić Policję.
5.	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić KOD. KOD lub osoba które otrzymała o powyższym informacje zabezpiecza dane. KOD sporządza protokół zagrożenia. Należy powiadomić Policję.
6.	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić KOD. KOD sporządza protokół uchybienia.
7.	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić KOD. Osoba odpowiedzialna zabezpiecza pomieszczenie. KOD sporządza protokół uchybienia.
8.	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić KOD. KOD lub osoba upoważniona sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. KOD sporządza protokół zagrożenia. Należy powiadomić Policję.
9.	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. KOD za pośrednictwem ASI ocenia, czy nie doszło do utraty danych osobowych i sporządza protokół uchybienia lub zagrożenia.
10.	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ASI. ASI aktualizuje lub nabywa oprogramowanie antywirusowe. KOD sporządza protokół uchybienia.
11.	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić KOD. KOD lub osoba upoważniona sprawdza stan uszkodzeń, zabezpiecza dowody. KOD sporządza protokół zagrożenia.
12.	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ASI. ASI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia KOD. KOD sporządza protokół zagrożenia.
13.	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ASI. ASI ocenia w wyniku czego doszło do zniszczenia i przywraca dane z kopii zapasowej. ASI powiadamia IOD, który sporządza protokół zagrożenia.
14.	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI. KOD sporządza protokół uchybienia.

15.	Zdarzenia losowe.	Należy oszacować powstałe starty i sporządzić protokół zagrożenia lub uchybienia.

6. Administrator Systemu Informatycznego w obszarze swojej odpowiedzialności przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie nieprzekraczającym **48 godzin** od daty jego zaistnienia i przekazuje go KOD, który sporządza protokół oraz kolejno wdraża procedury:
   a. Procedura działań korygujących i zapobiegawczych;
   b. Procedura bieżącego szacowania ryzyka i wdrożenie wypracowanych wniosków;
   c. Zawiadomienie UODO oraz osoby, której dane dotyczą.

D) PROCEDURA NA WYPADEK WYSTĄPIENIA NARUSZEŃ MOGĄCYCH POWODOWAĆ WYSOKIE RYZYKO NARUSZENIA PRAW I WOLNOŚCI OSÓB.

1. AD wraz z osobami funkcyjnymi (KOD/ASI) dokonuje analizy i oceny wpływu incydentu na prawa i wolności osób, których dane dotyczą – wzór PB „Wzory dokumentów wykonawczych".
2. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie musi być przekazane, jasnym i prostym językiem i opisywać charakter naruszenia ochrony danych osobowych.
3. Zawiadomienie, nie jest wymagane, w następujących przypadkach:
   a. Administrator 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;
   b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   c. 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.
4. **Jeżeli naruszenie dotyczy danych osobowych szczególnej kategorii należy uznać, że zachodzi wysokie prawdopodobieństwo naruszenia praw i wolności osoby fizycznej.**

E) PROCEDURA ZGŁASZANIA NARUSZEŃ OCHRONY DANYCH DO ORGANU NADZORCZEGO.

1. Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych.
2. zgłoszenia można dokonać na 4 sposoby:
   a. Elektronicznie poprzez wypełnienie **dedykowanego formularza elektronicznego** dostępnego bezpośrednio na platformie biznes.gov.pl będącego odwzorowaniem formularza dostępnego w załączniku.
   b. Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: **/UODO/SkrytkaESP**

c. Elektronicznie poprzez wysłanie wypełnionego formularza (dostępnego w załączniku) za pomocą **pisma ogólnego dostępnego na platformie biznes.gov.pl.**
d. Tradycyjną pocztą wysyłając wypełniony formularz na adres Urzędu.

3. Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest Prezes UODO, czy też może inny europejski organ nadzorczy.
   Zgłoszenia dokonuje AD w oparciu o informacje zebrane w wyniku dochodzenia przeprowadzonego przez KOD oraz ASI.

F) PROCEDURA ODTWARZANIA SYSTEMU PO AWARII ORAZ ICH TESTOWANIA.

1. Test bezpieczeństwa systemu teleinformatycznego przetwarzającego dane osobowe.
   a) Za przygotowanie i opracowanie planu testów bezpieczeństwa odpowiada ASI. W realizacji omawianego przedsięwzięcia może uczestniczyć KOD.
   b) Testy bezpieczeństwa powinny zostać przeprowadzone raz w roku, ASI zobowiązany jest sporządzić stosowny raport i przedstawić go AD oraz KOD.
   c) W ramach testu bezpieczeństwa systemu teleinformatycznego przeprowadzona zostanie analiza procedur zawartych w „Polityce Bezpieczeństwa", założenia i prowadzenia wymaganej dokumentacji, rejestrów, oświadczeń.
   d) Ponadto kontroli będą podlegać zdarzenia generowane przez logi systemowe, analiza i raportowanie dzienników zdarzeń. Jednocześnie skontrolowana zostanie wiedza użytkowników systemu teleinformatycznego przetwarzającego dane osobowe.
   e) Zakres testowanych zabezpieczeń systemu teleinformatycznego będzie obejmował wybrane zagadnienia ujęte w kwestionariuszu audytu wewnętrznego.
   f) Raport z przeprowadzonego testu bezpieczeństwa opracowuje ASI i przedstawia do zapoznania KOD i AD.
   g) Test bezpieczeństwa systemu teleinformatycznego może być prowadzony okresowo lub doraźnie na polecenie AD.
2. **Przywracanie systemu do pierwotnej funkcjonalności odbywa się zgodnie z procedurą – PLAN CIĄGŁOŚCI DZIAŁANIA.**

14. Regulamin korzystania z komputerów służbowych

a) Celem wdrożenia regulaminu jest zachowanie równowagi pomiędzy uzasadnionym interesem pracownika do ochrony jego prywatności, a prawem do ochrony informacji prawnie chronionych przetwarzanych przez **Spółkę**, a w szczególności:
   1. Poprawa jakości i zgodności z procedurami obowiązującymi w Spółce, wykonywania pracy przez pracowników;
   2. Zabezpieczenie uzasadnionych interesów (Administratora danych;
   3. Zabezpieczenie danych oraz mienia **Spółki**.

b) Zabronione jest wykorzystywanie przez pracownika komputera służbowego do celów prywatnych. W szczególności zabronione jest instalowanie i wykorzystywanie jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności w **Spółce**.
c) Zabronione jest pobierania określonych danych z Internetu polegające odciążeniu sieci informatycznej poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnej treści oraz kontroli antywirusowej nie wymagają zgody pracownika.
d) Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych jest dopuszczalne na mocy art. 22.2 Kodeksu pracy. Celem monitorowania (w tym poczty służbowej) jest zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy
e) Pracownik zabezpiecza dostęp do służbowej poczty elektronicznej (służbowego adresu e-mail) poprzez nadanie jej indywidualnego hasła ochronnego.
    1. Pierwsze hasło jest nadawane pracownikowi przez ASI. Pracownik jest zobowiązany do zmiany hasła podczas pierwszego logowania się do służbowej poczty elektronicznej.
    2. Pracownik ma obowiązek chronić hasło przed dostępem osób trzecich. W każdym przypadku, gdy hasło zostało ujawnione innej osobie, pracownik jest zobowiązany do jego zmiany.
f) Pracownik może wykorzystywać służbową pocztę elektroniczną (służbowy adres email) wyłącznie do czynności związanych z wykonywaną pracą.
    1. Nie jest dopuszczalne wykorzystywanie służbowej poczty elektronicznej (służbowego adresu e-mail) do celów prywatnych.
    2. Zabronione jest wykorzystywanie prywatnej poczty elektronicznej (prywatnego adresu email) do celów służbowych.
g) Drukarki nie mogą być pozostawione bez kontroli, jeśli są lub wkrótce będą drukowane na nich dane osobowe lub informacje z systemu informatycznego **Spółki**, o ile dostęp osób postronnych do tych drukarek nie jest odpowiednio ograniczony. Za przechowywanie wydruku zawierającego dane osobowe lub informacje z systemu informatycznego **Spółki** odpowiada wykonawca danego wydruku.
h) Przemieszczanie nośników lub sprzętu mobilnego zawierających dane osobowe poza pomieszczenia, w których są one przetwarzane, wymaga stosowania środków ochrony gwarantujących ich zabezpieczenie przed nieuprawnionym dostępem i ich ujawnianiem.
i) Na użytkowniku nośnika lub sprzętu mobilnego użytkowanego poza obszarem przetwarzania **Spółki** spoczywa obowiązek jego ochrony. W szczególności zabrania się pozostawiania bez opieki sprzętu mobilnego i nośników w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.
j) Za utratę lub zniszczenie nośnika lub sprzętu mobilnego powierzonego do pracy odpowiada dany użytkownik, któremu sprzęt został powierzony. Zaistnienie takiego zdarzenia użytkownik zgłasza do bezpośredniego przełożonego.
k) W przypadku, gdy na sprzęcie mobilnym lub nośniku przetwarzane są dane osobowe należy dodatkowo poinformować AD. W zawiadomieniu użytkownik, poza informacjami ogólnymi, podaje okoliczności utraty sprzętu mobilnego lub nośnika oraz zakres utraconych danych osobowych lub informacji wraz z podaniem ich znaczenia dla **Spółki.**

l) Sprzęt mobilny podlega szczególnej ochronie. Jego używanie poza obszarem przetwarzania **Spółki** musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.

m) Zgodę na użytkowanie sprzętu mobilnego poza siedzibą **Spółki** wydaje AD na wniosek pracownika (radnego) użytkującego sprzęt mobilny (jeśli istnieje taka potrzeba określona zadaniami służbowymi), ASI ma wówczas obowiązek zabezpieczenia urządzenie mobilne w tym m.in. szyfruje dysk.

n) Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza siedzibą Spółki, obowiązany jest za zapewnienie poufności i integralności przetwarzanych informacji. Do środków tych zalicza się w szczególności ochronę antywirusową.

o) Używanie sprzętu komputerowego poza siedzibą **Spółki** obliguje użytkownika do stosowania odpowiednich zabezpieczeń, takich jak np. zamykanie szafki, polityka czystego biurka i ekranu, zabezpieczenia dostępu do komputera.

15. Podstawowe zasady pracy na dokumentach zawierających dane osobowe

Zasada prywatności kont w systemach

W przypadku danych przetwarzanych z użyciem systemów informatycznych, użytkownik systemu jest zobowiązany do pracy jedynie na przypisanych mu kontach, które jednoznacznie go identyfikują i wyróżniają. Stosowanie się do tej reguły pozwala uniknąć anonimowości oraz wątpliwości w zakresie: kto i kiedy ingerował w treść danych lub z ich użyciem pracował.

Zasada poufności haseł i kodów dostępu

Każdy użytkownik zobowiązany jest zachowywać poufność oraz nie przekazywać innym osobom udostępnionych mu haseł i kodów dostępu. Reguła ta dotyczy w szczególności osobistych haseł dostępu do systemów informatycznych, a także kodów dostępu do pomieszczeń. Indywidualne hasło należy zachować jedynie dla siebie. Nie należy przekazywać ich innym osobom, w tym przełożonemu lub administratorom, a jeśli już do tego doszło to powinno się je niezwłocznie zmienić.

Zasada czystego ekranu

Metoda zabezpieczająca dane w przypadku nieobecności użytkownika. Zgodnie z tą zasadą każdy komputer służący do pracy z danymi musi mieć ustawiony, włączający się automatycznie po zdefiniowanym okresie bezczynności użytkownika, wygaszacz ekranu. W przypadku wznowienia aktywności wygaszacz powinien być wyłączany jedynie po podaniu odpowiedniego hasła. Dodatkowo przed pozostawieniem włączonego komputera bez opieki użytkownicy mogą zablokować go – włączając wygaszacz ekranu lub w przypadku dłuższej nieobecności najlepiej wylogować z systemu.

Zasada czystego biurka

Zasada czystego biurka to podstawowa zasada osób pracujących z wykorzystaniem dokumentów w formie papierowej. Należy unikać pozostawiania dokumentów na biurku bez nadzoru, szczególnie, gdy dokumenty te zawierają istotne z punktu widzenia Administratora

dane – w tym dane osobowe. Po zakończeniu pracy wszystkie dokumenty, muszą być przechowywane w zamknięciu i nie powinny być eksponowane w miejscu łatwo dostępnym.

Zasada czystych drukarek

Drukując dokumenty z użyciem ogólnodostępnej użytkownik jest zobowiązany do zabierania wydrukowanych dokumentów z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru.

Zasada czystego kosza

W przypadku pracy na dokumentach w formie papierowej, należy pamiętać, że dokumenty papierowe i miękkie nośniki danych z wyjątkiem materiałów jawnych, promocyjnych, marketingowych oraz informacyjnych muszą być niszczone w sposób uniemożliwiający ich ponowne odczytanie np. w niszczarce, umieszczane w specjalnie przeznaczonych do tego celu pojemnikach, etc.

16. Polityka antywirusowa

Osobą prowadzącą działania profilaktyczne mające na celu ochronę zasobów sieci komputerowej Spółka przed atakami wirusów komputerowych jest ASI

1. ASI wykorzystuje następujące funkcje systemowe:
   a) rejestracja i śledzenie informacji o dostępach lub próbach dostępu do zasobów i usług danego systemu.
   b) rejestracja i śledzenie komunikatów o błędach w pracy systemu.
   c) szyfrowanie i uwierzytelnianie informacji przesyłanych w sieci.
   d) wykrywanie obecności fałszywego oprogramowania w danych wpływających do systemu z sieci Internet.
   e) kontrola integralności oprogramowania zainstalowanego w systemie.

2. Ochrona antywirusowa zasobów informatycznych jest realizowana przez system antywirusowy posiadający następujące funkcje:
   a) zabezpieczenie zasobów informatycznych przed wirusami komputerowymi za pomocą modułu rezydentnego, skanującego na bieżąco wszystkie zasoby komputera,
   b) aktualizację baz sygnatur wirusów na bieżąco,
   c) możliwość automatycznego podejmowania działań w przypadku pojawienia się nowych, nieznanych wirusów (np.: zablokowanie komunikacji z zawirusowanym komputerem).

3. Aktualizacja baz sygnatur wirusów
   a) Bazy sygnatur wirusów dla serwerów są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
   b) Bazy sygnatur wirusów dla stanowisk roboczych są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
   c) Aktualizacja baz sygnatur wirusów odbywa się nie rzadziej niż jeden raz każdego dnia roboczego.

4. Kontrola antywirusowa.
   a) Zasoby informatyczne są skanowane na bieżąco za pomocą modułu rezydentnego. Kontroli podlegają wszystkie pliki (odczytywane i zapisywane) w tym poczta elektroniczna;

b) System antywirusowy jest zaprogramowany do wykonywania okresowych kontroli antywirusowych całego systemu plików. Kontrole te są wykonywane przez program automatycznie nie rzadziej niż jeden raz w tygodniu;
c) Zabrania się korzystania ze stanowiska bez aktywnego programu antywirusowego.

Zalecenia dla użytkowników stacji roboczych.

1. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (czytniki DVD, porty USB itp.) nośników rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi itp.
2. Zabrania się bez zgody przełożonego (ASI) używania na stanowisku pracy urządzeń do gromadzenia i przenoszenia danych, takich jak pamięci .flash'' dołączane przez porty USB, karty radiowe, dyski wymienne, modemy nie będących własnością **Spółki**.
3. Z uwagi na próby ataków na systemy użytkowników poprzez zainfekowanie poczty elektronicznej zaleca się zachowanie szczególnej ostrożności przy otwieraniu otrzymanych tą drogą załączników. W przypadku otrzymania nieoczekiwanej przesyłki pocztowej, która zawiera załącznik lub odsyła do treści bezpośrednio do strony www zaleca się aby nie otwierać załącznika ani nie korzystać bezpośrednio z przesłanych odnośników.
4. Każdy nośnik danych, używany do przenoszenia danych pomiędzy stanowiskami komputerowymi, przed odczytaniem danych należy sprawdzić programem antywirusowym.
5. Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy należy niezwłocznie zgłosić ten fakt ASI lub przełożonemu.

17. Realizacji praw przysługujących osobie, której dane dotyczą

Podstawowe prawa osób do danych osoby, której dane dotyczą

Prawo dostępu do danych

1. Każdej osobie fizycznej przysługuje prawo dostępu do swoich danych przetwarzanych przez Administratora. Każdej osobie przysługuje prawo do uzyskania wyczerpujących informacji od Administratora, w postaci potwierdzenia, czy dane są faktycznie przetwarzane.
2. Osoba wnioskująca otrzymuje dostęp do swoich danych osobowych poprzez uzyskanie kopii przetwarzanych danych osobowych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
3. Umożliwienie wglądu do danych konkretnej osobie fizycznej nie może powodować naruszenia praw innych osób lub też tajemnic prawnie chronionych. Uzyskując wgląd do swoich danych osobowych fizycznych nie może mieć nieuzasadnionego dostępu do danych innych osób fizycznych.
4. W przypadku, gdy przetwarzana jest duża ilość informacji o osobie, która chce skorzystać z prawa dostępu do swoich danych, Administrator kieruje do tej osoby żądanie sprecyzowania do jakich konkretnie danych lub też informacji o czynnościach przetwarzania jej danych chciałaby ona uzyskać dostęp.

Terminy na udzielenie odpowiedzi na żądanie:

1. Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie miesiąca od otrzymania tego żądania.
2. Jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może

wydłużyć udzielenia odpowiedzi o kolejne 2 miesiące, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

3. W przypadku, gdy administrator nie zamierza udzielić odpowiedzi oraz podjąć działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Prawo do sprostowania danych

Każdej osobie fizycznej przysługuje jednakowe prawo do niezwłocznego sprostowania/uzupełnienia dotyczących go danych osobowych, które są nieprawidłowe lub nieaktualne. Uwzględniając cele przetwarzania, osoba, której dane dotyczą ma prawo do żądania od AD uzupełnienia niekompletnych danych osobowych poprzez przedstawienie odpowiedniego oświadczenia AD.

Jeżeli osoba fizyczna zażąda uzupełnienia katalogu dotyczących go danych osobowych o te, które nie są niezbędne AD do działania, to taki wniosek nie musi zostać pozytywnie rozpatrzony przez AD dla osoby, której dane dotyczą.

Procedura

Komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i dostępnej formie.

Osoba składająca wniosek o sprostowanie/uzupełnienie danych osobowych oświadcza, że jest osobą możliwą do zidentyfikowania, na podstawie dobrowolnie podanych danych osobowych, umożliwiających jej jednoznaczną identyfikację.

W przypadku gdy AD nie jest w stanie zidentyfikować osoby składającej wniosek o sprostowanie/uzupełnienie danych osobowych, ma prawo na podstawie obowiązujących przepisów prawa odmówić rozpatrzenia żądania, uprzednio podejmując wszelkie możliwe środki w celu zidentyfikowania osoby, która z nim wystąpiła.

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) AD przysługują dwa uprawnienia:

1. pobranie rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań (według stawek obowiązujących u AD),
2. odmowa podejmowania działań,

Administrator, w przypadku podjęcia decyzji, o nieuzasadnionym lub nadmiernym charakterze żądania ma obowiązek wykazania takich cech żądania (wniosku) w ewentualnym postępowaniu przed organem nadzorczym.

Administrator jest zobowiązany po dokonaniu sprostowania/uzupełnienia danych osobowych poinformować wszystkich odbiorców którym ujawniono dane podlegające uzupełnieniu/sprostowaniu o fakcie ich uzupełnienia/sprostowania.

W przypadku braku możliwości wykonania powyższego, lub gdy działanie takie wymagałoby niewspółmiernie dużo wysiłku ze strony Administratora, może on podjąć decyzję o nieudzieleniu stosownej informacji odbiorcom, jednakże ma obowiązek wykazania braku możliwości lub niewspółmiernie dużego wysiłku w ewentualnym postępowaniu przed organem nadzorczym.

Terminy rozpatrywania żądań o sprostowanie/uzupełnienie danych osobowych:

1. Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie miesiąca od otrzymania tego żądania.
2. Jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć udzielenia odpowiedzi o kolejne 2 miesiące, jednakże w takim wypadku jest

zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

W przypadku, gdy Administrator nie zamierza udzielić odpowiedzi i działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Prawo do sprostowania danych realizowane jest z uwzględnieniem art. 16 RODO.

Prawo do usunięcia danych (prawo do bycia zapomnianym)
Każdej osobie fizycznej przysługuje prawo żądania usunięcia jej danych osobowych przetwarzanych przez Administratora. Prawo to składa się z następujących uprawnień:

1. możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez AD
2. możliwość żądania, aby AD poinformował innych Administratorów, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci Administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, czy replikacje.

Obowiązek poinformowania innych Administratorów może być ograniczony poprzez: dostępną technologię, koszty, konieczność ograniczenia się Administratora do „rozsądnych działań"
Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych Administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

Każdej osobie fizycznej przysługuje prawo do „bycia zapomnianym". Prawo to można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

1. dane osobowe nie są już niezbywalne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2. osoby, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;
3. osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych;
4. dane osobowe były przetwarzane w sposób „niezgodny z prawem"
5. dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator";
6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W przypadku wykonania prawa do bycia zapomnianym, Administrator zaprzestaje przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowne oświadczenie/wniosek, chyba że zachodzą szczególne przypadku ograniczające prawo do bycia zapomnianym:

1. istnieje przepis prawa, który nakazuje przetwarzanie danych osobowych;
2. istnieje sytuacja, w której przetwarzanie jest niezbędne do ustalenia dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania danych osobowych
Każdej osobie przysługuje prawo żądania ograniczenia przetwarzania danych osobowych. Żądanie ograniczenia przetwarzania danych wynika z art. 19 RODO powinno być złożone w formie wyraźnego

oświadczenia wskazującego przedmiotowy zakres żądania.
Ograniczenie przetwarzania danych Administrator może realizować w szczególności poprzez ich pseudonimizację.
Administrator może przechowywać dane osobowe, co do których zostało zgłoszone żądanie ograniczenia przetwarzania.
Realizacja żądania ograniczenia przetwarzania danych nie powoduje zaprzestania przetwarzania, które jest niezbędne do wykonania obowiązków wynikających z przepisów prawa, zaleceń lub rekomendacji Organu nadzorczego.

Prawo do przenoszenia danych
Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy osoba której dane dotyczą uprzednio dostarczyła Administratorowi dane jej dotyczące, lub wyraziła zgodę na pozyskanie przez Administratora tych danych, w inny sposób, określony uprzednio odpowiednim oświadczeniem.

Prawo do przenoszenia danych to, w szczególności prawo do:
1. otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła Administratorowi;
2. prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła Administratorowi, innemu Administratorowi, bez przeszkód ze strony Administratora danych, o ile jest to technicznie możliwe.

Prawo do przeniesienia danych może zostać wykonane , gdy:
1. przetwarzanie danych odbywa się na podstawie zgody osoby, lub w celu wykonania umowy;
2. przetwarzanie danych odbywa się w sposób zautomatyzowany – prawo do przenoszenia danych obejmuje tylko te dane osobowe, które są przetwarzane przy użyciu systemów informatycznych i nie obejmuje ono tradycyjnych, manualnych papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła Administratorowi. Wykonywanie tego prawa nie może niekorzystnie wpływać na prawa i wolności innych osób. Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Prawo sprzeciwu
Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw
wobec przetwarzania jej danych osobowych, wskazując jednocześnie, wobec jakiego
konkretnego celu przetwarzania składa sprzeciw i wykazać, na czym polega szczególny
charakter jej sytuacji (art. 21 RODO), tj. sytuacji, w której:
1. przetwarzanie jest niezbędne do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej Administratorowi;
2. przetwarzanie jest niezbędne do celów, wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, do złożenia sprzeciwu wobec powyższego przetwarzania jej danych osobowych, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów

statystycznych na mocy art. 89 ust. 1, osoba której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
Prawo do sprzeciwu musi zostać przez Administratora wyraźnie podane do wiadomości osobie, której dane dotyczą, jak również musi być przedstawione jasno i oddzielnie od wszelkich innych informacji.
Administrator ma prawo odmowy uwzględnienia sprzeciwu po dokonaniu analizy, czy szczególna sytuacja osoby, której dane dotyczą, ma charakter nadrzędny wobec prawnie uzasadnionych podstaw do przetwarzania. Jednocześnie Administrator wyjaśni przyczyny, dla których uważa, że interesy, prawa i wolności tej osoby, nie mają charakteru nadrzędnego.
Administrator może odmówić uwzględnienia sprzeciwu, w przypadku gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, w jasny i przystępny sposób wyjaśniając przyczyny odmowy. Odmowa jest poprzedzona analizą szczególnej sytuacji tej osoby.
Administrator, po wniesieniu sprzeciwu przez osobę, której dane przetwarzał, powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji.
Wykazanie zaistnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, prawa i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, jest obowiązkiem leżącym po stronie Administratora, i ma on obowiązek wykazania powyższego, w ewentualnym postępowaniu przed organem nadzorczym.
Wykorzystanie prawa do sprzeciwu nie prowadzi do automatycznego usunięcia wszystkich danych osobowych przez Administratora. Oznacza ono, że Administrator, z chwilą otrzymania sprzeciwu wobec przetwarzania danych osobowych, zaprzestaje z nich korzystać.

Zautomatyzowane przetwarzanie w tym profilowanie
Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
Powyższe nie ma zastosowania, jeżeli ta decyzja:
1. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
2. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
3. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być szczególny przepis prawa. W przypadku gdy zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.
Odwołanie zgody wywołuje wyłącznie skutki na przyszłość – oznacza to, że od chwili otrzymania oświadczenia o odwołania zgody, nie można już opierać się na zgodzie przetwarzania danych.

16. Procedura haseł

1. Cele wprowadzenia zasad postępowania z wszystkimi środkami kontroli haseł dostępu do danych:
    a. RODO nakazuje, aby dane osobowe były dostępne wyłącznie dla osób upoważnionych w strukturze Spółki oraz aby samo przetwarzanie odbywało się na polecenie Administratora. Zarządzanie hasłami służy kontroli dostępu do danych składowanych i przetwarzanych w systemach informatycznych Spółki, w postaci cyfrowej.
    b. Procedura ma za zadanie zredukować ryzyko nieautoryzowanego dostępu do przetwarzanych danych przez osoby nieupoważnione oraz umożliwić poufne przetwarzanie dokumentacji w systemach informatycznych Spółki.
    c. Procedura ma również redukować ryzyko kradzieży danych osobowych zawartych w systemach teleinformatycznych organizacji.
    d. Niniejsza Procedura służy ustaleniu standardu postępowania z hasłami do systemów informatycznych Spółki.
    e. Niniejsza Procedura ma zastosowanie do każdego systemu i zasobu informatycznego służącego do przetwarzania danych osobowych w Spółce.
2. Tworzenie haseł tymczasowych i zmiana haseł:
    a. Dostęp do danych osobowych przetwarzanych w systemach informatycznych Spółki musi być zabezpieczony hasłem.
    b. ASI zobowiązany jest zgłaszać zastrzeżenia do niniejszej polityki ze szczególnym uwzględnieniem sugerowanej w nich złożoności haseł, z chwilą powzięcia informacji o niedostateczności lub innych wadach standardów wdrażanych na jej podstawie.
    c. ASI odpowiedzialny jest za utworzenie konta użytkownika w każdym systemie i narzędziu służącym do przetwarzania danych osobowych oraz za wygenerowanie nowym użytkownikom tymczasowych pierwszych haseł.
    d. Nowo wygenerowane hasło jest hasłem tymczasowym i wymagana jest jego niezwłoczna zmiana na hasło docelowe, spełniające warunki opisane poniżej.
    e. ASI ma możliwość zresetowania hasła dostępu na wniosek oraz po zweryfikowaniu tożsamości użytkownika.
3. Minimalny poziom złożoności hasła:
    a. Każdy użytkownik zobowiązany jest do niezwłocznej zmiany tymczasowego hasła dostępu utworzonego przez ASI.
    b. Nowe hasło powinno składać się z co najmniej 8 znaków będących przypadkową kombinacją cyfr, małych i wielkich liter oraz symboli specjalnych.
    c. Nowe hasło nie może być identyczne z hasłami używanymi w systemach prywatnych, w szczególności z hasłami używanymi do dostępu do platform dla graczy, for internetowych, social media, komunikatorów internetowych itp..
    d. Każdy użytkownik komputera odpowiada za stworzenie bezpiecznego hasła zgodnego z wyżej wspomnianymi standardami.
    e. ASI tak konfiguruje obsługiwane systemy, aby wymuszały one stosowanie się do wytycznych dot. złożoności haseł.
    f. Jeśli zaistnieje sytuacja, w której określony system lub narzędzie nie pozwala na wymuszenie stosowania haseł o określonej złożoności.

i. Brak możliwości wymuszenia stosowania haseł zgodnych z niniejszą polityką rozpatrywać należy jako źródło ryzyka i uwzględnić w toku procesu analizy ryzyka naruszenia praw lub wolności osób, których dane dotyczą z wykorzystaniem danego systemu lub narzędzia.

4. Zasady przechowywania haseł:
    a. Nie dozwolone jest zapisywanie haseł w przeglądarkach internetowych.
        i. Zaleca się korzystanie z menedżera haseł;
        ii. ASI odpowiedzialny jest za wskazanie oprogramowania do przechowywania haseł.
    b. Hasła stanowią informacje poufne i mogą być znane wyłącznie ich dysponentom (nie wolno ich podawać nikomu, nawet przełożonemu lub ASI (komórka IT).
    c. Zabrania się zapisywania haseł w notatnikach, na stickerach, w kalendarzach itp.
    d. W związku z potrzebą zapewnienia ciągłości działania, zachodzi potrzeba przechowywania haseł pozwalających na zakładania kont administratorów (na zasadach opisanych poniżej). W siedzibie Spółki znajduje się szafa / sejf do dyspozycji Zarządu Spółki, w której przechowuje się hasła do kont superadministratora (ROOT)
5. Konta superadministratorów (ROOT) i zapewnienie ciągłości działania:
    a. W celu zapewnienia ciągłości działania systemu informatycznego Spółki tworzy się konta super-administratora (ROOT – o ile zachodzi taka potrzeba) dla każdego systemu i narzędzia służącego do przetwarzania danych osobowych.
    b. Konta te służą do zakładania kont i blokowania kont Administratorów. Hasła do tych kont znajdują się w wyłącznej dyspozycji Zarządu Spółki.
    c. Hasło super-administratora (ROOT) powinno składać się z co najmniej 14 znaków będących przypadkową kombinacją cyfr, małych i wielkich liter oraz symboli specjalnych.
    d. Hasło super-administratora (ROOT) składuje się w szafie w zapieczętowanej kopercie, do której dostęp ma wyłącznie Zarząd Spółki.
    e. Z chwilą zniknięcia konieczności stosowania uprawnień superadministratora (ROOT), hasło do tego konta należy zmienić na nowe hasło spełniające w/w wymagania.
    f. Nowe hasło należy zapisać, zamknąć w zaklejonej kopercie i przenieść do składowania do szafy, o której mowa powyżej.

17. Procedura inicjacji i realizacji fazy planowania i okresu przetwarzania danych osobowych

1. Cele procedury jest uwzględnienie przepisów i zasad przetwarzania danych osobowych na etapach::
    a. **Zasada privacy by design** oznacza, że administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.
    b. **Zasada privacy by default** oznacza wdrożenie odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi

się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. w szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób fizycznych bez interwencji osoby, której te dane dotyczą.

c. Procedury maje zapewnić, aby każda zmiana w procesach przetwarzania była poprzedzona działaniami analitycznymi i predykcyjnymi w celu redukcji ryzyka naruszenia praw i wolności osób, których dane są w danym procesie przetwarzane.
d. Drugim celem realizacji fazy planowania jest utrzymanie aktualności dokumentacji, a w szczególności Rejestru Czynności Przetwarzania, Rejestru Kategorii Czynności Przetwarzania oraz Analizy Ryzyka.

2. Inicjacja fazy planowania:
   a. Fazę planowania inicjuje osoba wskazana jako odpowiedzialna za dany proces przetwarzania w Rejestrze Czynności Przetwarzania dla czynności przetwarzania, w których Spółka jest Administratorem w której ma nastąpić zmiana, dla czynności przetwarzania, dla których Spółce powierzono przetwarzanie, ewidencjonowanych w RKCP.
   b. Fazę planowania należy zainicjować w przypadku planowania zmian w procesie w zakresie:
      - Rozszerzenia kategorii przetwarzań czyli włączenia do obecnego procesu nowej czynności - np. udostępnienia danych, upublicznienia danych, przechowywania (zapisywania do późniejszego wykorzystania) danych, które wcześniej były poddawane analizie wyłącznie na bieżąco itd.
      - Zmiany celu przetwarzania
      - Rozszerzenia typów przetwarzanych informacji, a więc zwiększenia ilości kategorii danych osobowych stanowiących przedmiot przetwarzania w zakresie danych powierzonych do przetwarzania zmiana zakresu danych pociąga za sobą wyłącznie konieczność dokonania ponownej analizy w zakresie poufności danych.
      - Zmiany w brzmieniu przepisów stanowiących podstawę prawną przetwarzania.
      - Zmiany wykonawcy lub podwykonawcy
      - Braku możliwości utrzymania ciągłości funkcjonalności wskazanych jako zabezpieczenia w Analizie Ryzyka lub powzięciu przekonania o niedostateczności tych zabezpieczeń (np. w wyniku wystąpienia naruszenia podlegającego zgłoszeniu pomimo stosowania tych zabezpieczeń).
      - Wprowadzeniu do procesu przetwarzania transgranicznego lub zmiany państwa docelowego albo organizacji międzynarodowej przy przetwarzaniu transgranicznym.
      - Powzięciu informacji o wygaśnięciu certyfikacji podmiotu współpracującego.
      - Zmianie typów procesów przetwarzania, dla których Prezes Urzędu Ochrony Danych Osobowych przewiduje obowiązek prowadzenia oceny skutków dla ochrony danych.
   c. Inicjując fazę planowania należy:
      - Ustalić nieprzekraczalny termin realizacji danej zmiany (np. moment rozpoczęcia stosowania nowego prawa, moment zakończenia umowy z wykonawcą / podwykonawcą, termin planowanego wdrożenia nowego rozwiązania).
      - Zawiadomić o tym fakcie KOD.

- Zgromadzić informacje o zmianie (np. treść nowelizacji przepisów prawa, ofertę od nowego podwykonawcy, opis planowanej technologii itd.).
- Zgromadzić bieżące informacje o procesie (zebrać procedury w nim realizowane, zapoznać się z treścią RCP / RKCP i Analizy Ryzyka).
- Doprowadzić do spotkania z osobami, których kompetencje lub decyzyjność okażą się niezbędne do przeprowadzenia analizy danego procesu (na spotkaniu zawsze niezbędna jest osoba lub zespół realizujący dany proces w jego obecnym kształcie oraz IOD, w dalszej kolejności potrzebni mogą okazać się: prawnik - zwłaszcza przy zmianie przepisów stanowiących podstawę prawną przetwarzania oraz w kontekście przetwarzania transgranicznego; administrator systemu - jeżeli zmiana ma dotyczyć funkcjonalności systemowych; dostawca nowej technologii / przedstawiciel firmy, z którą rozważa się rozpoczęcie współpracy; przedstawiciel klienta; IOD klienta).

3. Prowadzenie fazy planowania składa się z następujących czynności:
    a. Dokonanie ponownej analizy ryzyka (sugeruje się przeprowadzenie pełnej analizy, zgodnie z przyjętą metodologią jednak dla drobnych zmian dopuszczalne jest wyłącznie skorygowanie obszarów powiązanych).
    b. W przypadku braku możliwości redukcji ryzyka z WYSOKIEGO w dowolnym obszarze lub w przypadku faktu spełnienia kryteriów, o których mowa w art. 35 (Ocena skutków dla ochrony danych), jak również w przypadku zmiany typów procesów przetwarzania, dla których Prezes Urzędu Ochrony Danych Osobowych przewiduje obowiązek prowadzenia oceny skutków dla ochrony danych, przeprowadzenie oceny skutków dla ochrony danych (DPIA).
    c. Opracowanie nowych procedur postępowania lub modyfikacji obecnych procedur, zgodnie z zapotrzebowaniem.
    d. Uzyskaniu akceptacji Zarządu Spółki - Administratora na modyfikację procesu w świetle przedstawionych wyników fazy planowania.
    e. W przypadku akceptacji Zarządu Spółki - Administratora dla procesów, w których powierzono przetwarzanie danych osobowych, przedstawienie propozycji modyfikacji klientowi / kontrahentowi oraz opracowanie aneksu do umowy powierzenia przetwarzania danych osobowych.
    f. W przypadku akceptacji Zarządu Spółki- Administratora, przeszkolenie personelu zaangażowanego z nowych lub znowelizowanych procedur.
    g. W przypadku akceptacji Zarządu Spółki - Administratora, dokonanie uaktualnienia RCP / RKCP i Analizy Ryzyka.

18. Procedura zarządzania uprawnieniami

1. Cele zarządzania uprawnieniami:
    a. RODO nakazuje, aby dane osobowe były dostępne wyłącznie dla osób upoważnionych (zarówno w strukturze Spółki, jak i po stronie podmiotów powiązanych, którym powierza się przetwarzanie) oraz, aby samo przetwarzanie odbywało się na polecenie Administratora. Zarządzanie uprawnieniami służy kontroli dostępu do danych zarówno w znaczeniu materialnym (a więc kto ma dostęp do jakiego typu danych oraz czy wyłącznie je widzi, czy

też może je edytować), jak i w znaczeniu celowym i czasowym (a więc kiedy danej osobie wolno wykonać określone operacje na danych osobowych).

b. Zarządzanie uprawnieniami służy również do uzyskania zdolności wykazania, kto dokonał jakich operacji, dla celów rozliczalności i dowodowych.
c. Zarządzanie uprawnieniami ma także za zadanie zredukować ryzyko wystąpienia błędu ludzkiego, które jest wysokie, jeżeli istnieje możliwość przetwarzania danych przez osoby nieznające procedur i zasad postępowania lub procesu, w którym dane te są wykorzystywane.
d. Ostatecznie, zarządzanie uprawnieniami służy ułatwieniu blokady możliwości uzyskania dostępu do danych w przypadku zakończenia stosunku pracy lub współpracy.

2. Generalne zasady dotyczące zarządzania uprawnieniami:
    a. Każda osoba może dysponować prawem do wglądu lub edycji danych osobowych wyłącznie w zakresie, w jakim jest to niezbędne dla realizacji aktualnych obowiązków służbowych.
        - Oznacza to, że w przypadku zastępstwa, uprawnienia dostępowe do zasobów osoby zastępowanej muszą być nadawane czasowo, a nie bezterminowo;
        - oraz że wszelkie zmiany po stronie prowadzonych projektów takie, jak zamknięcie projektu, przeszeregowanie osoby do innego projektu, ograniczenie zakresu działań w danym projekcie i podobne, muszą znajdować odzwierciedlenie w zakresie uprawnień dostępowych.
    b. Zarządzanie uprawnieniami jest więc procesem ciągłym, w którym na bieżąco monitoruje się zakres zadań, zakres obecnie posiadanych uprawnień oraz planowany termin realizacji zadań wymagających określonych uprawnień.
    c. Aby móc zarządzać uprawnieniami w taki sposób, konieczne jest prowadzenie ich ewidencji, aby w każdej chwili była możliwość ustalenia bieżącego ich zakresu.
    d. Ponadto, aby spełnić kryterium konieczności w zakresie przyznawania uprawnień, niezbędne jest, aby w procesie ich nadawania uczestniczyła osoba, która posiada wiedzę fachową co do zakresu zadań danego pracownika lub współpracownika oraz w przedmiocie natury tych zadań, ich charakteru oraz zakresu informacji potrzebnego do ich realizacji.
    e. Z uwagi na potrzebę prowadzenia ewidencji uprawnień, system zarządzania nimi musi bazować na komunikacji w postaci pisemnej (w tym elektronicznej), aby zredukować ryzyko błędu ludzkiego przy aktualizacji ewidencji oraz aby umożliwić wyjaśnianie spraw niezrozumiałych, trudnych lub obarczonych błędem formalnym.
    f. Z racji tego, że samo tylko umożliwienie dostępu do danych osobowych osobie nieuprawnionej stanowi naruszenie prawa, w proces zarządzania uprawnieniami muszą być zawsze zaangażowane minimum dwie osoby chyba, że uprawnienia nadaje Zarząd, który w pierwszej kolejności odpowiada za ewentualne naruszenie zasad ochrony.
    g. Wyłącznymi osobami, które mogą same zatwierdzać wnioski dotyczące ich własnych uprawnień, mogą być osoby, które w pierwszej kolejności ponoszą odpowiedzialność za zabezpieczenie danych osobowych, a więc członkowie Zarządu.
3. Obszar stosowania procedury zarządzania uprawnieniami:
    a. Procedurę stosuje się do następujących zasobów i na następujących zasadach:

b. Poczty elektronicznej w zakresie przekierowania skrzynek pocztowych na okoliczność zastępstw lub w okresie następującym po zakończeniu współpracy z dysponentem danej skrzynki pocztowej.
    - o fakcie przekierowania skrzynki zawiadamiana jest osoba, która jest użytkownikiem tej skrzynki;
    - respondenci zawiadamiani są o fakcie przekierowania skrzynki przez ustawienie na niej autorespondera informującego o okolicznościach oraz okresie nieobecności użytkownika skrzynki;
    - przekierowanie następuje w momencie powzięcia informacji o dłuższej nieobecności użytkownika skrzynki (złożenie wniosku urlopowego lub rozwiązanie albo wygaśnięcie stosunku pracy lub współpracy);
    - użytkownik skrzynki zobowiązany jest zasugerować osobę, do której jego poczta ma zostać przekierowana;
    - przekierowanie poczty akceptuje Zarząd Spółki;
    - przekierowanie poczty realizuje ASI/ firma IT lub osoba bezpośrednio oddelegowana do tego zadania przez Zarząd;
    - osoba, do której przekierowano pocztę, udzielając odpowiedzi, pisze z własnego konta imiennego;
    - zabronione jest wysyłanie jakiejkolwiek korespondencji z konta innego użytkownika;
    - konta pocztowe imienne zakłada ASI/ firma IT każdemu pracownikowi i współpracownikowi, w związku z rozpoczęciem pracy lub współpracy na rzecz lub z Spółką.
c. Poczty elektronicznej w zakresie przekazywania haseł dostępowych do skrzynek celowych (nie imiennych), takich jak rekrutacja@..., faktury@..., biuro@... itp.
    - cała zawartość skrzynki celowej dotyczyć może wyłącznie jednego zadania w rozumieniu procedury postępowania z dokumentami i zasobami (zasada ta nie dotyczy skrzynki biuro@... stanowiącej narzędzie kontaktu w każdej możliwej sprawie);
    - dokonując wysyłki korespondencji ze skrzynki celowej, nadawca ma obowiązek podpisać się imieniem i nazwiskiem w treści wiadomości;
    - konta pocztowe celowe zakłada ASI/ firma ITD na wniosek Zarządu lub osoby upoważnionej, a następnie nadaje uprawnienia dostępowe do nich każdemu wskazanemu we wniosku pracownikowi i współpracownikowi Spółki.
d. Zasobów zawartych w chmurze, w folderach działów lub projektów, jak również zasobów zawartych na dysku sieciowym.
    - dostęp do zasobu zostaje nadany przez ASI/ firma IT na wniosek Zarządu lub osoby upoważnionej każdemu pracownikowi i współpracownikowi Spółki, w zakresie podstawowym, wynikającym z profilu stanowiska, w związku z nawiązaniem stosunku pracy lub współpracy;
    - dostęp do poszczególnych folderów w chmurze oraz na dysku sieciowym przyznawany jest na podstawie wniosku kierowanego przez samego zainteresowanego lub kierownika jego działu;
    - wniosek ten musi uzyskać akceptację Zarządu lub osoby upoważnionej;

- w ramach chmury oraz na dysku sieciowym tworzy się drzewo folderów;
- wszystkie osoby zaangażowane w proces zarządzania uprawnieniami dostępowymi do zasobów chmurowych i zlokalizowanych na dysku sieciowym (wnioskujący, ewentualny zatwierdzający, ASI/ firma IT oraz Zarząd) muszą być dołączeni do każdej korespondencji w przedmiocie tych uprawnień;
- zabronione jest udostępnianie przez zasób chmurowy lub na dysku sieciowym jakichkolwiek dokumentów poza folderami z uwagi na trudność określania retencji danych w nich zawartych;
- w przypadku wystąpienia uchybienia tej zasadzie, wszystkie dokumenty udostępnione, ale nie przeniesione do określonego folderu docelowego, uważa się za dokumenty tymczasowe.

4. Zasady komunikacji:
    a. Komunikacja w przedmiocie uprawnień prowadzona jest pocztą elektroniczną (na przechowywanie tych wiadomości, osoba akceptująca zakłada na poczcie folder "Zarządzanie uprawnieniami"; osoba wnioskująca może potraktować tę korespondencję jako dokumenty tymczasowe);
    b. Wszelkie wady formalne wniosków, błędy przy ich redagowaniu lub niejasność ich treści stanowią zawsze błędy nadawcy wniosku.
5. Zasady ewidencjonowania uprawnień:
    a. W celu wyliczenia stanu zerowego, dokonuje się następujących działań:
        - ASI/ firma IT określa zakres uprawnień dostępowych do zasobów sieciowych dla każdego pracownika i współpracownika;
        - ASI/ firma IT weryfikuje, czy ustawione są jakiekolwiek przekierowania poczty w ramach domeny Spółki;
        - ASI/ firma IT sprawdza, czy w domenie istnieją jakiekolwiek konta pocztowe celowe (nie imienne);
        - Zarząd Spółki dokonuje weryfikacji, czy każda osoba posiadająca jakiekolwiek uprawnienia jest pracownikiem lub współpracownikiem jeżeli nie, niezwłocznie wzywa ASI do blokady tych uprawnień);
        - Zarząd Spółki dokonuje weryfikacji, czy obecny zakres uprawnień dostępowych pracowników odpowiada faktycznemu zakresowi realizowanych przez nich zadań poprzez doprowadzenie do spotkania osób merytorycznie odpowiedzialnych za realizację określonych zadań (kierowników komórek) i administratorów danych systemów informatycznych (w przypadku wyników negatywnych - braku zgodności - Zarząd wzywa ASI do blokady tych uprawnień);
        - Zarząd Spółki lub osoba upoważniona ocenia, czy istniejące przekierowania poczty są w dalszym ciągu uzasadnione (jeżeli nie, niezwłocznie wzywa ASI do wyłączenia przekierowania) oraz czy dla każdego z kont przekierowanych ustawiony jest stosowny autoresponder (jeżeli nie, Zarząd wskazuje osobę odpowiedzialną za opracowanie treści odpowiedzi, a następnie ustawia lub zleca ustawienie autorespondera);
        - Zarząd Spółki lub osoba upoważniona ustala zasadność posiadania aktywnych kont celowych. W przypadku stwierdzenia wygaśnięcia celu ich posiadania, dokonuje

analizy dalszej zasadności przechowywania danych na zasadach określonych w procedurze zarządzania dokumentami i zasobami oraz, o ile zachodzi taka potrzeba, dokonuje usunięcia konta celowego;

- Z chwilą doprowadzenia stanu faktycznego do stanu oczekiwanego, dokonuje się spisania uprawnień w formacie przyjętym przez ASI/ firmę IT i zaakceptowanym przez Zarząd Spółki.

b. Z chwilą założenia ewidencji uprawnień, prowadzi się jej aktualizację poprzez naniesienie informacji o fakcie realizacji każdego skutecznego wniosku o nadanie lub odebranie uprawnień.
c. Wnioski nieskuteczne (które nie uzyskały akceptacji oraz które nie zostały jeszcze zrealizowane) nie są ewidencjonowane.
d. Za aktualność ewidencji odpowiada Dział IT.

6. Odbieranie uprawnień:
   a. Odbieranie uprawnień może nastąpić na podstawie autonomicznej decyzji Zarządu Spółki lub osoby upoważnionej lub na wniosek kierownika komórki (bez podania przyczyny, ale wyłącznie względem jego podwładnych).
   b. Wniosek o odebranie uprawnień kieruje się do tych samych osób i na tych samych zasadach, co wnioski o nadanie uprawnień.
   c. Okolicznościami, w których musi nastąpić odebranie uprawnień, są:
      - wygaśnięcie stosunku pracy lub współpracy, w tym wypowiedzenie umów ze szczególnym uwzględnieniem rozwiązania umów bez zachowania okresu wypowiedzenia;
      - zakończenie współpracy z danym klientem (zakończenie projektu);
      - ograniczenie zakresu prac realizowanych w ramach danego projektu lub zakończenie subprojektu (zakończenie realizacji określonego zadania w ramach projektu lub ustalenie z klientem, że określone zadania nie będą dalej realizowane);
      - zmiana celu przetwarzania zasobu (przeniesienie określonego zasobu do zasobów archiwalnych lub przechowywanych z uwagi na ustalenie, dochodzenie lub obronę roszczeń - domyślnie dane powinny zmienić swoją lokalizację zgodnie z postanowieniami procedury zarządzania dokumentami i zasobami jednak na okres operacyjny dopuszczalne jest ograniczenie dostępu do nich przez zarządzanie uprawnieniami);
      - przeszeregowanie pracownika.
7. Zarząd Spółki może na podstawie stosownego pełnomocnictwa powierzyć kwestie decyzyjne związane z nadawaniem / odbieraniem uprawnień pracownikowi Spółki.

19. Procedura monitoringu

I. Podstawa prawna monitoringu pracowników

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

2) Ustawa o ochronie danych z dnia 10 maja 2018 roku;
3) Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy art. $22^{2,3}$ (Dz.U.2019.0.1040);
   a. art. 22^{2}, który nie tylko wskazuje warunki dopuszczalności stosowania monitoringu wizyjnego w zakładzie pracy, ale również wytyczne dla pracodawców stosujących różne formy monitoringu pracowników w zakresie: formy określenia zakresu, celu i sposobu stosowania monitoringu, okresu przechowywania danych uzyskanych w toku monitoringu, obowiązków informacyjnych wobec pracowników – a w określonych przypadkach również wobec osób trzecich,
   b. art. 22^{3}, który reguluje stosowanie monitoringu poczty elektronicznej pracownika oraz innych form monitoringu.
4) Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego, czerwiec 2018.

II. Cel monitoringu:

Monitoringu TV

Na podstawie art. 22^{3} Kodeks pracy (Dz.U.2019.0.1040) przesłankami do jego zastosowania jest zapewnienie bezpieczeństwa pracowników w tym przestrzegania procedur BHP, ochrony mienia, zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Podmiot na szkodę.

W przypadku monitoringu pracowników oraz klientów (pacjentów) podstawą przetwarzania danych jest art. 6 ust. 1 lit f tzw. ważny interes administratora, którego celem jest zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwe użytkowanie udostępnionych pracownikowi narzędzi pracy.

III. Definicje:

a) Monitoring wizyjny — kamery, okablowanie, rejestrator oraz oprogramowanie wykorzystywane do zbierania oraz przechowywania wizerunku.
b) Dane osobowe — wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli nie wymaga to nadmiernych kosztów, czasu lub działań.
c) Polityka Bezpieczeństwa (PB) — obowiązująca w Podmiocie.
d) Zbiór danych osobowych — każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
e) Administrator Danych (AD) — należy przez to rozumieć – **Improvement Factory Sp. z o.o.**
f) Przetwarzanie danych osobowych — wykonywanie wszelkich operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
g) Zbieranie danych — wejście w posiadanie danych osobowych.
h) Usuwanie danych — fizyczne niszczenie danych lub taka ich modyfikacja, która uniemożliwia ustalenie osoby, której dane dotyczą.
i) Utrwalanie — zapisanie informacji na materialnym nośniku.
j) Udostępnianie — objęcie w posiadanie danych osobowych przez innego Administratora Danych Osobowych lub podmiotu przetwarzającego.
k) Wgląd — fizyczne przeglądanie zawartości zbioru danych osobowych bez wejścia w posiadanie przeglądanego zbioru.
l) Osoba upoważniona — osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu zgodnie z Polityką Bezpieczeństwa.

IV. Monitoring wizyjny

Monitoring wizyjny został wdrożony po dokonaniu planowania i zdefiniowania zagrożeń bezpieczeństwa jako najbardziej adekwatne narzędzie służące osiągnięciu celu, po dokonaniu analizy potrzeb i celowości wraz z prognozą jego skuteczności w kontekście wpływu na zachowanie prywatności osób przebywających na terenie Podmiotu w zakresie obowiązku zapewnienia bezpieczeństwa. Na system monitoringu wizyjnego składają się kamery, urządzenie rejestrujące, monitor umożliwiający wgląd do utrwalonego zapisu oraz okablowanie.
Monitoring prowadzony jest całodobowo i obejmuje obiekt Spółki oraz teren bezpośrednio przyległy.

V. Zabezpieczenia techniczne i organizacyjne (rozmieszczenie kamer).

a) Zabrania się instalowania kamer w toaletach, pomieszczeniach socjalnych czy też poszczególnych pomieszczeniach biurowych – co mogłoby prowadzić do naruszenia prywatności.
b) Osobom mającym dostęp do zapisu rejestratora monitoringu należy wydać **upoważnienia** do przetwarzania danych osobowych i uwzględnić je w **ewidencji.**
c) W przypadku potrzeby powierzenia zapisu monitoringu innym podmiotom należy zawrzeć stosowną umowę powierzenia przetwarzania danych osobowych.
d) Za nadzór nad rejestratorem odpowiedzialny jest AD / ASI.

VI. Zasady monitoringu.

a) Zbieraniu, utrwalaniu oraz przechowywaniu wizerunku jako danej osobowej podlega wyłącznie obraz (wizja) z kamer systemu monitoringu. Funkcjonujący w firmie system **nie rejestruje dźwięku (fonii);**
b) Wykaz obszarów objętych monitoringiem wizyjnym oznakowany jest tablicami informacyjnymi (piktogramami);
c) Miejsca objęte monitoringiem wizyjnym zostały przeanalizowane pod kątem poszanowania prywatności i intymności pracowników oraz innych osób przebywających na terenie Podmiotu;
d) Miejsca objęte monitoringiem są oznakowane poprzez umieszczenie informacji zawierającej piktogram informujący o objęciu obszaru monitoringiem oraz z informacją dotyczącą:
   - Administratora Danych,
   - Celu istnienia monitoringu,
   - Prawa oraz sposobie uzyskania dodatkowych informacji.
e) Wzór oznakowania informującego o objęciu monitoringiem – załącznik do procedury
f) Monitoring funkcjonuje całodobowo;
g) Efekty wprowadzenia monitoringu wizyjnego wraz z ich wpływem na bezpieczeństwo pracowników i osób przebywających na terenie firmy są na bieżąco monitorowane.

VII. Zasady rejestracji monitoringu.

a) Obraz utrwalony na rejestratorze, zlokalizowany w firmie nagrywany jest przez okres 30 dni, po czym jest nadpisywany;
b) Zaleca się, aby z okres nagrywania nie przekraczał 90 dni, po tym czasie może zostać nadpisany;
c) W uzasadnionych przypadkach, w szczególności, gdy system monitoringu wizyjnego zarejestrował wydarzenia niezgodne z prawem zapis może zostać przeniesiony na elektroniczny nośnik pamięci;
d) Nośniki z zachowanym nagraniem przechowuje ASI/ osoba wskazana przez AD;

e) Nośniki zawierające przeniesiony z rejestratora zapis obrazu przechowujemy wyłącznie do momentu zaprzestania jego użyteczności, np. do czasu wyjaśnienia sprawy lub zakończenia odpowiednich postępowań nie dłużej niż jeden rok;
f) Zapisany obraz z monitoringu może zostać udostępniony zgodnie z zasadami określonymi w Polityce Bezpieczeństwa;
g) Nośniki zawierające utrwalony zapis wizyjny polegają obowiązkowi tworzenia kopii zapasowych zgodnie z procedurami określonymi w Polityce Bezpieczeństwa;
h) W momencie zaprzestania użyteczności nagrania zapisanego na zewnętrznym nośniku, jest ono usuwane zgodnie z procedurą określoną w Polityce Bezpieczeństwa;
i) Dostęp do zapisu wizyjnego utrwalonego w rejestratorze oraz zewnętrznych nośników posiada wyłącznie Administrator Danych Osobowych oraz upoważnione przez Niego osoby zgodnie z procedurami określonymi w Polityce Bezpieczeństwa;
j) Rejestrator oraz zewnętrzne nośniki zawierające zapisany obraz zabezpieczony jest przed dostępem osób nieupoważnionych poprzez zastosowanie środków technicznych oraz organizacyjnych określonych w Polityce Bezpieczeństwa.

VIII. <u>Zabezpieczanie i udostępnianie danych objętych monitoringiem.</u>

1. Administrator Danych zabezpiecza dla celów dowodowych zdarzenia zarejestrowane przez monitoring, które zagrażają bezpieczeństwu, życiu i zdrowiu pracowników oraz osób przebywających na terenie obiektów Spółki i terenie bezpośrednio do niej przyległym, a także wskazują na niszczenie i kradzież mienia:
    a. na wniosek osób trzecich;
    b. na wniosek organów prowadzących postępowania, np. policji, prokuratury, sądów;
    c. z inicjatywy osób obsługujących system monitoringu,

   które mogą być następnie dowodem popełnienia czynu zabronionego
2. Zabezpieczenie danych monitoringu polega na ich zarejestrowaniu na nośniku danych, umożliwiającym ich powielanie.
3. Zabezpieczone dane z monitoringu są udostępniane organom prowadzącym postępowanie w sprawie zarejestrowanego zdarzenia, np. policji, prokuraturze, sądom, które działają na podstawie odrębnych przepisów.
4. Zabezpieczone dane mogą być również przekazywane zakładowi ubezpieczeń, z którym Spółka zawarła umowę ubezpieczenia, w ramach prowadzonej likwidacji szkody osobowej lub majątkowej, zgłoszonej przez osoby trzecie.
5. Każdorazowe udostępnienie zabezpieczonych danych w postaci zdarzeń zarejestrowanych przez system monitoringu odbywa się na pisemny wniosek wyżej wskazanych podmiotów.
6. Dane z systemu monitoringu zabezpieczone na wniosek podmiotu uprawnionego są przechowywane przez AD przez okres jednego roku od dnia złożenia wniosku. Po upływie tego terminu zabezpieczone dane są niszczone.
7. Z czynności zniszczenia danych, o której mowa powyżej, sporządza się protokół, który powinien zawierać:
    a. czas i miejsce zarejestrowanego obrazu zdarzeń, podlegającego zniszczeniu;
    b. sposób zniszczenia;
    c. imię, nazwisko, stanowisko służbowe osoby dokonującej zniszczenia;

d. czas i miejsce zniszczenia;
e. podpis osoby dokonującej zniszczenia.

8. Z czynności zniszczenia danych, o której mowa powyżej sporządza się protokół, który powinien zawierać:
   a. czas i miejsce zarejestrowanego obrazu zdarzeń podlegającego zniszczeniu;
   b. sposób zniszczenia;
   c. imię, nazwisko, stanowisko służbowe osoby dokonującej zniszczenia;
   d. czas i miejsce zniszczenia;
   e. podpis osoby dokonującej zniszczenia.
9. Treść klauzuli informacyjnej, dotyczącej monitoringu wizyjnego zawarta jest w Załączniku nr 4 do niniejszego Regulaminu.

Udostępnianie danych objętych monitoringiem.

a) Administrator Danych zabezpiecza zdarzenia zarejestrowane przez monitoring, które zagrażają bezpieczeństwu, życiu i zdrowiu pracowników i osób przebywającym na terenie, niszczeniu i kradzieży mienia dla celów dowodowych:
   - na wniosek osób trzecich;
   - na wniosek organów prowadzących postępowania np. policji, prokuratury, sądów;
   - zaobserwowane przez osoby obsługujące monitoring, które mogą być dowodem na popełnienie czynu niedozwolonego.

b) Zabezpieczenie danych monitoringu polega na ich zarejestrowaniu na nośniku danych, umożliwiającym ich powielanie;
c) Nośniki danych zawierające zarejestrowane dane powinny być zabezpieczone i przechowywane w specjalnie wyznaczonym do tego miejscu;
d) Zabezpieczone dane z monitoringu są udostępniane tylko organom prowadzącym postępowanie w sprawie zarejestrowanego zdarzenia np. policji, prokuraturze, sądom, które działają na podstawie odrębnych przepisów;
e) Zabezpieczone dane mogą być również przekazywane ubezpieczycielowi firmy w ramach prowadzonej likwidacji szkody osobowej lub majątkowej zgłoszonej przez osoby trzecie;
f) Każdorazowe zabezpieczenie zdarzeń zarejestrowanych przez monitoring odbywa się na pisemny wniosek podmiotów w/w wskazanych;
g) Dane z monitoringu zabezpieczone na wniosek podmiotu uprawnionego są przechowywane przez AD przez okres jednego roku od dnia złożenia wniosku. Po upływie tego terminu zabezpieczone dane są niszczone.;
h) Z czynności zniszczenia danych, o której mowa powyżej sporządza się notatkę, która powinna zawierać:

- czas i miejsce zarejestrowanego obrazu zdarzeń podlegającego zniszczeniu;
- sposób zniszczenia;
- imię, nazwisko, stanowisko służbowe osoby dokonującej zniszczenia;
- czas i miejsce zniszczenia;
- podpis osoby dokonującej zniszczenia.

Załącznik nr 1 do Procedury

WNIOSEK
O UDOSTĘPNIENIE DANYCH ZAWARTYCH W ZAPISIE MONITORINGU WIZYJNEGO

…….
Dane wnioskodawcy

Zwracam się z prośbą o umożliwienie wglądu do zapisu monitoringu wizyjnego

1. Data, godzina i miejsce, w którym został dokonany zapis monitoringu wizyjnego:

_____

2. Wskazanie przeznaczenia dla udostępnionego zapisu:

_____

3. Informacje umożliwiające wyszukiwanie nagrania:

_____

_____
podpis

Decyzja Zarządu:
wyrażam zgodę* / nie wyrażam zgody*
Decyzja Zarządu nie wymaga uzasadnienia.

Podpis Przedstawiciela Zarządu……

Załącznik nr 2 do Procedury

WZÓR OZNAKOWANIA INFORMUJĄCEGO O OBJĘCIU MONITORINGIEM

OBIEKT MONITOROWANY CAŁODOBOWO
Administratorem Danych jest
Improvement Factory Sp. z o.o. ul. Kręta 1 80-217 Gdańsk
Monitoring wizyjny prowadzony jest w celu zapewnienia bezpieczeństwa pracowników, ochrony mienia, realizacji zapisów kodeksu pracy.
Dodatkowe informacje można znaleźć na stronie internetowej Spółki

Załącznik nr 3 do Procedury

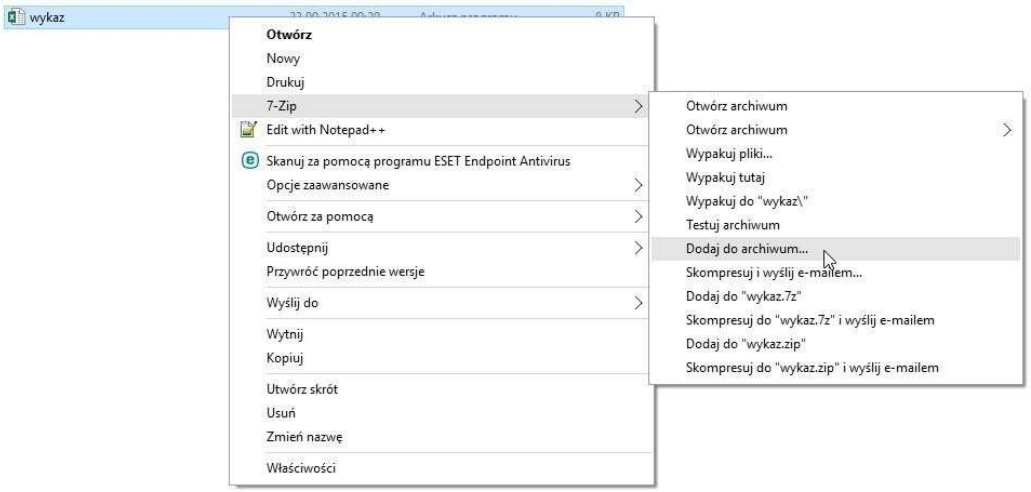
TABELARYCZNY WYKAZ ROZMIESZCZENIA KAMER.

Lp	Typ kamery	Miejsce zamontowania

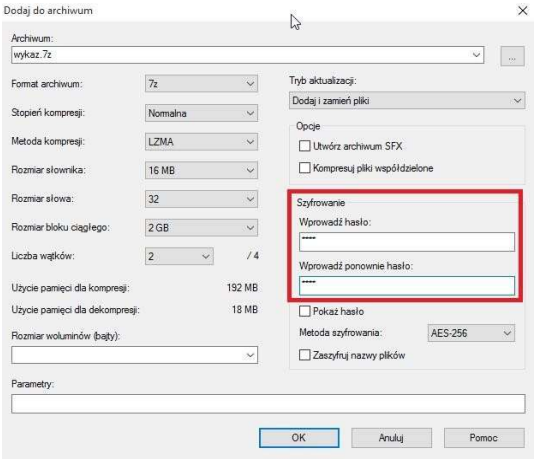
Lp	Typ rejestratora	Lokalizacja	Czas przechowywania nagrania

20. Procedura pseudonimizacji i szyfrowania danych

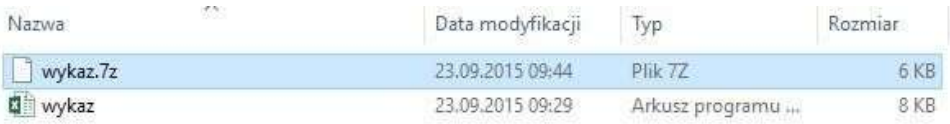
1. Celem procedury jest określenie zasad i sposobów stosowanych w Spółce w zakresie szyfrowania i pseudonimizacji danych osobowych przesyłanych drogą elektroniczną oraz przetwarzanych w formie tradycyjnej.
2. Procedura określa minimalne wymagania jakie AD zobowiązany jest zastosować, aby chronić powierzone mu dane osobowe w zakresie szyfrowania dokumentów oraz ich pseudonimizacji.
3. Pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
4. Do najczęściej stosowany metod należą:
   a. **szyfrowanie kluczem tajnym** - obecność klucza pozwala jednocześnie utajnić zbiór danych i w razie konieczności ponownie go odczytać, przypisując konkretne informacje do konkretnych osób. W domyśle jedynie posiadanie klucza daje możliwość odszyfrowania danych;
   b. **tokenizacja** - jest to technika szyfrowania jednokierunkowego i polega na zastąpieniu fragmentów danych ciągiem losowych liczb, co sprawia, że informacje te stają się bezużyteczne dla osób postronnych;
   c. **skracanie** - czyli skrócenie wybranych wartości, tak aby odczytanie ich faktycznego znaczenia stało się niemożliwe.
5. **Minimalne wymogi stosowane podczas przesyłania danych osobowych drogą elektroniczną:**
   A. Szyfrowanie plików pakietu MS OFFICE.
   a. Pliki przesyłane drogą elektroniczną (np. pliki tekstowe, arkusze kalkulacyjne, inne) powinny zostać zaszyfrowane poprzez nadanie hasła (min 8 znaków, duże i małe litery) w programie WORD, EXCEL, POWER POINT w następujący sposób:
      - <u>W systemie WINDOWS:</u>
        - Przejdź do pliku > informacji > chronić dokument > szyfrowania za pomocą hasła.
        - Wpisz hasło, a następnie wpisz je ponownie, aby je potwierdzić.
        - Zapisz plik, aby upewnić się, że hasło zacznie obowiązywać.
   b. Hasło powinno zostać udostępnione odbiorcy przy użyciu innego środka komunikacji np. sms, inny adres email.
   B. Szyfrowanie plików przy użyciu programów pakujących / rozpakowujących.
   a. Pliki przesyłane drogą elektroniczną (np. pliki tekstowe, arkusze kalkulacyjne, inne) powinny zostać zaszyfrowane poprzez nadanie hasła (min 8 znaków, duże i małe litery) na poziomie programu służącego do archiwizacji np. 7zip.
   b. Instrukcja szyfrowania pliku/katalogu programem 7-zip.
      - Należy kliknąć prawym przyciskiem myszy na plik lub katalog i wybrać opcję 7-zip -> Dodaj do archiwum. Przykład na poniższym rysunku:



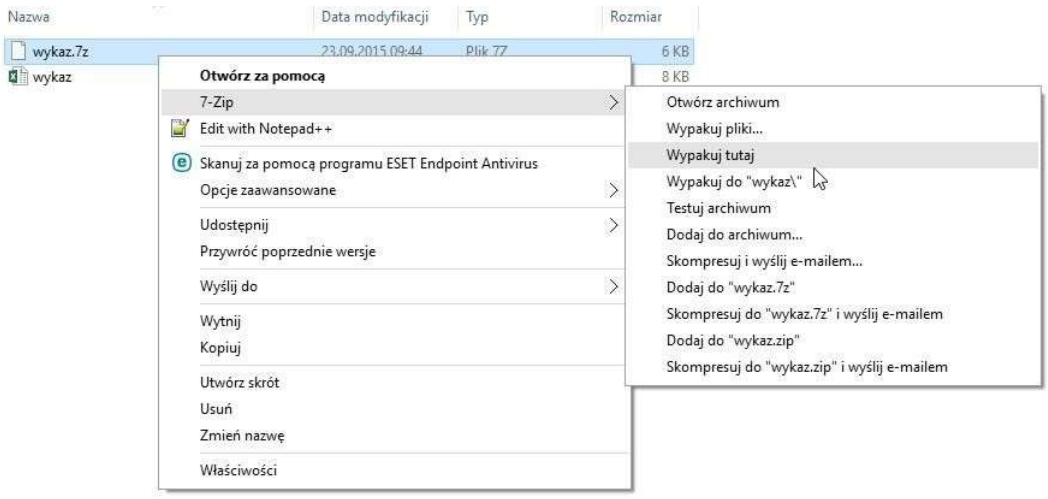
- Następnie w okienku „Dodaj do archiwum” w polu „Wprowadź hasło:” wpisujemy hasło, którym chcemy zaszyfrować plik lub katalog. W polu „Wprowadź ponownie hasło:” ponownie wpisujemy hasło w celu weryfikacji poprawności wpisanego hasła. Przykład na poniższym rysunku:



- W wyniku szyfrowania otrzymujemy plik o rozszerzeniu .7z, który można bezpiecznie przesłać e-mailem jak normalny załącznik.



c. Instrukcja odszyfrowania pliku/katalogu programem 7-zip
   - Zaszyfrowany załącznik w wiadomości e-mail należy zapisać na komputerze.
   - Na zaszyfrowanym pliku należy kliknąć prawym przyciskiem myszy i wybrać opcję 7 zip -> wypakuj tutaj. Przykład na poniższym obrazku:



6. **Pseudonimizacji dokumentów AD wykonuje między innymi w sytuacjach:**
   - udostępniania informacji w ramach przepisów dotyczących informacji publicznej;
   - udostępniania dokumentów związkom zawodowym w obszarze, w którym nie są one uprawnione do ich przetwarzania;
   - innym podmiotom lub instytucjom, którym przysługuje dostęp do danych osobowych, lecz AD posiada ich szerszy zakres niż jest to wymagane w ramach udostępnienia.
7. **Minimalne wymogi stosowane podczas pseudonimizacji dokumentów zawierających dane osobowe:**
   - Dokumenty w wersji tradycyjnej udostępnia się tylko w niezbędnym zakresie uniemożliwiając odczyt danych osobowych, które nie wymagają udostępnienia lub zostałyby udostępnione nadmiarowo poprzez ich zamazanie na kopii dokumentu;
   - Dokumenty w wersji elektronicznej udostępnia się tylko w niezbędnym zakresie uniemożliwiając odczyt danych osobowych, które nie wymagają udostępnienia lub zostałyby udostępnione nadmiarowo poprzez ich zamazanie na kopii dokumentu lub programowe wyszczególnienie tylko tych podlegających udostępnieniu.

21. Obowiązywanie dokumentu

Polityka Bezpieczeństwa wchodzi w życie z dniem zatwierdzenia i wprowadzenia przez Zarząd i obowiązuje wszystkich pracowników bez względu na formę świadczenia pracy we wszystkich obszarach gdzie dochodzi do przetwarzania informacji podlegających ochronie w tym danych osobowych.

22. Wykaz załączników

1. załącznik nr 1 - wzór upoważnień,
2. załącznik nr 2 - wykaz obszarów przetwarzania danych osobowych,
3. załącznik nr 3 - wykaz zbiorów danych osobowych,

4. załącznik nr 4 - wniosek o realizację praw osób których dane dotyczą,
5. załącznik nr 5 - rejestr naruszeń ochrony danych osobowych,
6. załącznik nr 6 - rejestr umów powierzenia danych osobowych,
7. załącznik nr 7 - ewidencja wydanych upoważnień do przetwarzania danych osobowych,
8. załącznik nr 8 - wykaz środków fizycznych, technicznych oraz organizacyjnych stosowanych w celu zabezpieczenia danych oraz informacji,