POLITYKA OCHRONY DANYCH OSOBOWYCH
w przedsiębiorstwie "VILLA FALSZTYN" Paweł Tarapata
z dnia 25 maja 2018 roku

Uwzględniając obowiązki wynikające z art. 25 oraz art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1), celem zapewnienia, że dane osobowe przetwarzane przez Administratora **są przetwarzane i zabezpieczone zgodnie z postanowieniami prawa poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, oraz w celu nadania przetwarzaniu danych niezbędnych zabezpieczeń,** Administrator zapewnia, że przetwarzane były i są wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Niniejszy dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym. Zestawienia uzupełniające treść niniejszego dokumentu zebrano w postaci załączników. Polityka stanowi jeden ze środków organizacyjnych mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO. Polityka wchodzi w życie z dniem 25 maja 2018 roku.

1. POSTANOWIENIA WSTĘPNE

a) Polityka określa zasady przetwarzania oraz zabezpieczania Danych osobowych przez Administratora celem zapewnienia zbieżności przetwarzania z wymaganiami RODO oraz przepisami bezwzględnie obowiązującego prawa polskiego w zakresie przetwarzania danych osobowych. Polityka stanowi podstawę wdrażanych przez Administratora wymogów, procedur oraz zasad ochrony danych osobowych.

Polityka zawiera:
- opis zasad ochrony danych obowiązujących u Administratora;
- zbiór procedur, instrukcji i regulacji szczegółowych dotyczących przetwarzania Danych osobowych u Administratora, dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych.

b) Polityka obowiązuje wszystkich pracowników oraz współpracowników Administratora. Za przestrzeganie i utrzymanie postanowień Polityki odpowiedzialni są:
- Administrator oraz komórki organizacyjne Administratora, w których przetwarzane są Dane osobowe;
- Pracownicy Administratora, ewentualnie – osoby upoważnione przez Administratora do przetwarzania danych.

c) Dla skutecznej realizacji Polityki, uwzględniając zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia Administrator zapewnia:

- wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność przetwarzania Danych osobowych z wymogami prawa oraz niezbędne zabezpieczenie przetwarzanych danych osobowych;
- stałe monitorowanie zgodności przetwarzania Danych osobowych z wymogami prawa oraz poddawanie środków (o których mowa powyżej) przeglądom oraz uaktualnianiu;
- kontrolę i nadzór nad przetwarzaniem Danych osobowych.

d) Nadzór nad przestrzeganiem postanowień Polityki zapewnia podmiot upoważniony do reprezentacji Administratora Nadzór, o którym mowa w zdaniu poprzedzającym zmierza w szczególności, ale nie wyłącznie do zapewnienia, że czynności związane z przetwarzaniem Danych osobowych u Administratora są zgodne z wymogami prawa oraz postanowieniami Polityki.

e) Administrator zapewnia zgodność postępowania kontrahentów Administratora, w tym w szczególności Podmiotów Przetwarzających, z postanowieniami Polityki, w odpowiednim zakresie, we wszystkich sytuacjach, w których dochodzi do przekazania tym podmiotom Danych osobowych do przetwarzania, w tym przechowywania.

f) Polityka jest przechowywana i udostępniana w wersji papierowej oraz elektronicznej w siedzibie Administratora.

g) Politykę udostępnia się:
   - obligatoryjnie wszystkim osobom upoważnionym do przetwarzania danych osobowych u Administratora, celem zapewnienia osobom upoważnionym należytej wiedzy oraz informacji na temat zasad i wymogów dotyczących przetwarzania Danych Osobowych u Administratora;
   - osobom zainteresowanym, w szczególności osobom fizycznym, których dane dotyczą – na ich wniosek.

ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

Odpowiedzialność za bezpieczeństwo informacji ponoszą wszystkie osoby przetwarzające dane osobowe zgodnie z posiadanymi zakresami obowiązków. Każdy osoba obowiązana jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi w tym m.in.:

a) stosować zasady opisane w Polityce Ochrony Danych oraz innych dokumentach wewnętrznych;
b) chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;
c) chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
d) chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione;
e) utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia;
f) powiadomić Administratora o:
   - ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym;
   - nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian;
   - zniszczeniu lub możliwości zniszczenia informacji chronionych;
   - zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych.

Obowiązki Administratora:

a) wprowadza, zarządza i sprawuje nadzór nad działaniami Polityki Ochrony Danych Osobowych;
b) określa rodzaje zasobów podlegających ochronie;

c) decyduje o celach i środkach przetwarzania danych;
d) zatwierdza Politykę Ochrony Danych Osobowych;
e) prowadzi komunikację z podmiotem danych i przekazuje mu informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny;
f) ułatwia podmiotom danych wykonywanie ich praw;
g) nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie;
h) weryfikuje tożsamość osób wnoszących żądania udzielenia informacji;
i) potwierdza czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli ma to miejsce, udziela wskazanych rozporządzeniem informacji;
j) ułatwia osobie, której dane dotyczą wykonywanie jej praw z art 15–22 RODO;
k) informuje osobę, której dane dotyczą, o działaniach jakie podjął, w związku z jej żądaniami opartymi o art 15-22 RODO;
l) uzasadnienia odrzucenie żądania osoby, której dane dotyczą i poucza ją o prawie skargi;
m) umożliwia dostęp do jej danych osobie, której one dotyczą;
n) dokonuje sprostowania i uzupełniane danych;
o) usuwa dane;
p) powiadamia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu ich przetwarzania; dokonuje przenoszenia danych.

2. DEFINICJE

Ilekroć w niniejszej Polityce zostaną wykorzystane poniższe definicje lub zwroty, należy nadawać im następujące znaczenie:

- **Polityka** – oznacza niniejszą Politykę wraz ze wszystkimi Załącznikami;
- **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, takie 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; o których mowa w art. 4 pkt 1 RODO;
- **RODO** – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1);
- **Administrator danych (ADO)** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Ilekroć w niniejszym dokumencie jest mowa o Administratorze należy przez to rozumieć Pawła Tarapatę prowadzącego działalność gospodarczą pod firmą VILLA FALSZTYN Paweł Tarapata, Falsztyn 116, 34-435 Frydman, wpisanego do Centralnej Ewidencji i Informacji o Działalności Gospodarczej NIP 9441537886, REGON 357025242.
- Martę Tarapatę prowadzącą działalność gospodarczą pod firmą ECO CARBO Marta Tarapata, adres: Kraków (30-383), ul. Lubostroń 7B, wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej NIP 6762208624, REGON 121498489;
- **Osoba upoważniona** – oznacza osobę upoważnioną przez Administratora do przetwarzania Danych osobowych w danym zakresie;
- **Przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie,

wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, o których mowa w art. 4 pkt 2 RODO;

- **Zbiór danych** – oznacza każdy uporządkowany zestaw Danych osobowych, dostępny według określonych kryteriów;
- **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora [np. usługodawca IT, zewnętrzna księgowość];
- **Rejestr** - oznacza Rejestr Czynności Przetwarzania Danych Osobowych Administratora;
- **Uwierzytelnienie** – oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika;
- **Pracownicy Administratora** – oznacza zarówno osoby zatrudnione przez Administratora na podstawie stosunku pracy, jak również osoby fizyczne współpracujące z Administratorem na podstawie Umowy cywilnoprawnej;
- **System** – oznacza System ochrony danych osobowych u Administratora, o którym mowa w 0 Polityce;
- **Dane wrażliwe** – oznaczają Dane Osobowe, o których mowa w art. 9 RODO.
- **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- **Zgoda osoby, której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
- **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
- **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
- **Pseudonimizacja** oznacza 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;
- **Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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 Unii lub prawem państwa członkowskiego, 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;

- **Strona trzecia** oznacza 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;
- **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;
- **Naruszenie ochrony danych** osobowych oznacza 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;
- **Dane genetyczne** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- **Dane biometryczne** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
- **Dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
- **Przedsiębiorca** oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
- **Grupa przedsiębiorstw** oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
- **Organ nadzorczy** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO, w Polsce organem nadzorczym jest Urząd Ochrony Danych Osobowych;
- **Organizacja międzynarodowa** oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

3. DANE OSOBOWE

1. Administrator przetwarza Dane osobowe gromadzone w zbiorach danych. Uaktualnienie lub poszerzenie listy Zbiorów danych następuje po uprzednim przeprowadzeniu analizy skutków oraz ryzyk przetwarzania danych osobowych dla praw i wolności osób fizycznych objętych zbiorem.
2. Administrator nie podejmuje czynności Przetwarzania, które mogłyby wiązać się z istotnym ryzykiem naruszenia praw i wolności osób, których Dane osobowe dotyczą. W przypadku planowania podjęcia czynności, o których mowa w zdaniu poprzedzającym Administrator obligatoryjnie przeprowadza uprzednią ocenę skutków przetwarzania, o których mowa w art. 35 RODO.

3. Dane osobowe domyślnie przetwarzane są na obszarze na terenie obejmującym pomieszczenia biurowe Administratora zlokalizowane w jego siedzibie. Dodatkowy obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

4. PODSTAWY OCHRONY DANYCH OSOBOWYCH

1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się Dane osobowe przetwarzane u Administratora zobowiązane są do Przetwarzania Danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych wewnętrznych aktów prawnych Administratora lub procedur wewnętrznych związanych z przetwarzaniem Danych Osobowych.
3. Przy zatrudnianiu Pracowników oraz w toku zatrudnienia Administrator zapewnia, że:
   a) Pracownicy przez przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad przetwarzania i ochrony Danych Osobowych u Administratora;
   b) każdy z Pracowników zostaje upoważniony na piśmie do Przetwarzania Danych Osobowych w niezbędnym zakresie, zgodnie z wzorem stanowiącym załącznik do Polityki;
   c) każdy z pracowników zostaje zobowiązany do zachowania poufności i integralności Danych osobowych, przy czym Pracownicy zobowiązani są w szczególności:
      - ścisłego przestrzegania zakresu upoważnienia;
      - przestrzegania wymogów prawa oraz postanowień Polityki w zakresie przetwarzania;
      - zachowania w tajemnicy Danych osobowych;
      - zachowania poufności i integralności Danych Osobowych;
      - niezwłocznego zgłaszania Administratorowi wszelkich incydentów związanych z naruszeniem bezpieczeństwa Danych osobowych.
4. Administrator zapewnia, aby Dane Osobowe Przetwarzane u niego były

   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą; Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:
   - osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

5. Przy zapewnieniu Przetwarzania Danych osobowych zgodnie z zasadami wskazanymi 2wyżej Administrator opiera przetwarzanie na następujących podstawach:
   - Legalność – Administrator dba o ochronę prywatności i przetwarza Dane osobowe zgodnie z wymogami prawa;
   - Bezpieczeństwo − Administrator zapewnia odpowiedni poziom bezpieczeństwa Danych osobowych podejmując stale działania w tym zakresie;
   - Prawa Jednostki − Administrator umożliwia osobom, których Dane Osobowe są przetwarzane, wykonywanie swoich praw i prawa te realizuje;
   - Rozliczalność – Administrator zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony danych osobowych.

Administrator nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej.

5. ADMINISTRATOR

1. Administrator danych dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych.
2. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych. Pomieszczenia stanowiące obszar przetwarzania danych są zamykane na klucz.
   Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
   Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Każda osoba przetwarzająca dane osobowe zostaje zapoznana z przepisami w zakresie ochrony danych osobowych poprzez odpowiednie szkolenia.
3. Przetwarzanie szczególnych kategorii danych osobowych

   Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Art. 2. ust. 1 RODO nie ma zastosowania, jeżeli spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą, udzieliła wyraźnej zgody na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą UE lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia;
- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

6. ZAGROŻENIA BEZPIECZEŃSTWA

CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

- **Zagrożenia losowe zewnętrzne** – np. klęski żywiołowe, przerwy w zasilaniu, których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona lecz nie dochodzi do naruszenia poufności danych.

- **Zagrożenia losowe wewnętrzne** – np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania, przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych.

- **Zagrożenia zamierzone, świadome i celowe** – najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

- Przełamane zabezpieczenia tradycyjne – np. zerwane plomby na drzwiach, szafach, segregatorach;
- Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
- Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
- Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
- Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
- Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
- Próba lub modyfikacja danych oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- Niedopuszczalna manipulacja danymi osobowymi w systemie;
- Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu;
- Praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych

osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
- Ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.;
- Podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych;
- Rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

7. INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Niniejsza procedura określa tryb i zasady postępowania przy przetwarzaniu danych osobowych. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

TRYB POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

1. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie, jest Administrator.

2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym Administratora.

3. Administrator po otrzymaniu powiadomienia:
   - podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł);
   - zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia;
   - ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu;
   - niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności;
   - dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia.

4. Administrator sporządza szczegółowy raport zawierający: datę i godzinę wystąpienia incydentu, imię i nazwisko osoby powiadamiającej o zaistniałym zagrożeniu, lokalizację zdarzenia, rodzaj naruszenia bezpieczeństwa wraz z towarzyszącymi okolicznościami, przyczyny wystąpienia naruszenia, podjęte działania, środki zaradcze oraz datę i podpis osoby sporządzającej raport. Administrator podejmuje niezbędne działania w celu zapobiegania naruszeniom zabezpieczeń systemu w przyszłości.

5. Jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, Administrator ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych.

TRYB POSTĘPOWANIA W PRZYPADKU PODEJRZENIA NARUSZENIA ZABEZPIECZEŃ DANYCH OSOBOWYCH

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązana jest niezwłocznie powiadomić o tym Administratora.
2. Administrator po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):
   - ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
   - inicjuje ewentualne działania dyscyplinujące;
   - działa na rzecz przywrócenia działań przedsiębiorstwa po wystąpieniu incydentu;
   - rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych Administrator:
   - podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia;
   - zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia;
   - dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia;
   - sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

4. Administrator sporządza szczegółowy raport wg załącznika, zawierający: datę i godzinę wystąpienia incydentu, imię i nazwisko osoby powiadamiającej o zaistniałym zagrożeniu, lokalizację zdarzenia, rodzaj naruszenia bezpieczeństwa wraz z towarzyszącymi okolicznościami, przyczyny wystąpienia naruszenia, podjęte działania, środki zaradcze oraz datę i podpis osoby sporządzającej raport. Administrator podejmuje niezbędne działania w celu zapobiegania naruszeniom zabezpieczeń systemu w przyszłości.

Tabela opisująca przykładowe zagrożenia oraz sposoby postępowania w przypadku naruszeń bezpieczeństwa danych osobowych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić wg procedury. Sporządzić raport z opisem, jaka

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	informacja została ujawniona.
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Powiadomić wg procedury. Sporządzić raport
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Powiadomić wg procedury. Sporządzić raport.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Powiadomić wg procedury. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Powiadomić wg procedury. Sporządzić raport.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Powiadomić wg procedury. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Powiadomić wg procedury. Sporządzić raport.
Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Powiadomić wg procedury. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Powiadomić wg procedury. Sporządzić raport.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Powiadomić wg procedury. Sporządzić raport.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić wg procedury. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić wg procedury. Sporządzić raport.

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Powiadomić wg procedury. Jeżeli ujawnione zostały ważne dane - sporządzić raport
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Zaprzestać kopiowanie. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić wg procedury. Sporządzić raport.
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić wg procedury. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie. Powiadomić wg procedury. Sporządzić raport.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić wg procedury. Sporządzić raport.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić wg procedury. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić wg procedury. Sporządzić raport.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić wg procedury. Sporządzić raport.

Tabela zjawisk świadczących o możliwości naruszenia ochrony danych osobowych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie administratora bezpieczeństwa informacji oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Powiadomić wg procedury. Sporządzić raport.
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Powiadomić wg procedury. Sporządzić raport.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	
Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić wg procedury. Sporządzić raport.

Tabela naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić wg procedury. Sporządzić raport.
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	

NOTYFIKACJA NARUSZEŃ

W przypadku naruszenia ochrony danych osobowych Administrator zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych. **Nie ma obowiązku zgłoszenia, jeżeli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**.

Administrator dokonuje samodzielnej oceny, czy zaistniałą sytuację objął obowiązek zgłoszenia. Następne bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, o ile naruszenie skutkuje ryzykiem naruszenia prawa lub wolności osób fizycznych. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
To, czy zawiadomienia dokonano bez zbędnej zwłoki, ustala się z uwzględnieniem:

- charakteru i wagi naruszenia ochrony danych osobowych;
- jego konsekwencji;

oraz
- niekorzystnych skutków dla osoby, której dane dotyczą.

Zgłoszenie naruszenia ochrony danych osobowych musi co najmniej:
- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać:
  - kategorie i przybliżoną liczbę osób, których dane dotyczą;
  - kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Administrator zawsze dokumentuje naruszenia ochrony danych osobowych.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych to administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

8. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH I UPRZEDNIE KONSULTACJE

Jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Administrator weryfikuje:
a) obowiązek przeprowadzenia oceny skutków dla ochrony danych, metodologii przeprowadzenia oceny skutków dla ochrony danych;
b) obowiązek przeprowadzenia wewnętrznej oceny lub zlecenia jej podmiotowi zewnętrznemu;
c) skuteczność zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
d) prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie, oraz jakie zabezpieczenia należy zastosować).

W sytuacji, gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator powinien dokonać przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych. Jeżeli ocena ta wykaże, że przetwarzanie może powodować wysokie ryzyko przy braku zastosowania przez administratora środków dla zminimalizowania tego ryzyka, to zgodnie z art. 36 RODO administrator konsultuje się w tej sprawie z organem nadzorczym.

9. MONITORING WIZYJNY

W celu realizacji celów określonych w art. 22^1 § 1 kodeksu pracy, Administrator w swoim przedsiębiorstwie stosuje system nadzoru nad swoim przedsiębiorstwem oraz terenem wokół niego w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Monitoringiem nie obejmuje się szatni, pomieszczeń sanitarnych, palarni czy stołówek.

Administrator oznacza teren i pomieszczenia objęte monitoringiem w sposób czytelny i widoczny, nie później niż jeden dzień przed objęciem danego terenu bądź pomieszczenia monitoringiem. Jednocześnie Administrator informuje swoich pracowników o wprowadzeniu monitoringu na zasadach określonych w kodeksie pracy.

Nagrania obrazu Administrator przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres maksymalnie 3 miesięcy od dnia nagrania. W przypadku gdy nagrania te stanowią dowód w postępowaniu prowadzonym na podstawie przepisów prawa, bądź Administrator powziął wiadomość, iż mogą one stanowić dowód w takim postępowaniu, Administrator jest uprawniony do przechowania takiego nagrania do czasu prawomocnego zakończenia takiego postępowania.

Po upływie okresów przechowywania nagrania z monitoringu ulegają zniszczeniu, chyba że przepisy prawa bezwzględnie obowiązującego stanowią inaczej.

10. SYSTEM OCHRONY DANYCH OSOBOWYCH

Administrator zapewnia zgodność Przetwarzania Danych Osobowych z wymogami prawa również poprzez zaprojektowanie, wprowadzenie i utrzymywanie Systemu. Na System składają się środki organizacyjne oraz środki techniczne ochrony, adekwatne do poziomu ryzyka zidentyfikowanego dla poszczególnych Zbiorów danych oraz kategorii danych.

Na System składają się w szczególności następujące środki:

a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe, jedynie do Osób upoważnionych oraz zapewnienie, że inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do Przetwarzania Danych osobowych wyłącznie w towarzystwie Osoby upoważnionej;
b) zamykanie pomieszczeń tworzących obszar, w którym gromadzone i przechowywane są dane osobowe, w sposób uniemożliwiający dostęp do nich osobom trzecim;
c) zapewnienie zabezpieczenia obszaru, w którym gromadzone i przechowywane są dane osobowe, przed czynnikami losowymi, takimi jak pożar lub powódź;
d) wykorzystywanie zamykanych szafek, szuflad lub innych środków technicznych uniemożliwiających osobom niepowołanym dostęp do przechowywanych w nich Danych osobowych;
e) wdrożenie Polityki czystego biurka,
f) wdrożenie Procedury otwierania i zamykania budynków oraz pomieszczeń biurowych,
g) zapewnienie skutecznego usuwania lub niszczenia dokumentów zawierających Dane osobowe, w sposób uniemożliwiający ich późniejsze odtworzenie;
h) zapewnienie bezpieczeństwa sprzętowego i informatycznego, obejmującego:
i) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz,
j) zapewnienie aktualności stosowanego oprogramowania,
k) zabezpieczenie sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem,
l) zapewnienie stałego i częstotliwego sporządzania kopii zapasowych danych przechowywanych na komputerach, serwerze oraz w sieci wewnętrznej Administratora,
m) ograniczenie dostępu do sprzętu komputerowego, serwera oraz sieci lokalnej poprzez stosowanie reguł Uwierzytelniania;
n) przeprowadzanie okresowej analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

o) realizację standardów weryfikacji i doboru Podmiotów przetwarzających, jak również warunków powierzenia Przetwarzania danych na rzecz poszczególnych Podmiotów przetwarzających;

p) monitorowanie zmian w zakresie procesów Przetwarzania Danych osobowych u Administratora oraz na bieżąco zarządza zmianami mającymi wpływ na ochronę Danych osobowych u Administratora.

11. REJESTR

1. Rejestr obejmuje kategorie czynności przetwarzania Danych Osobowych u Administratora. Za pośrednictwem Rejestru Administrator dokumentuje czynności przetwarzania Danych Osobowych oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje Dane osobowe.
2. Za pośrednictwem Rejestru, w szczególności poprzez wskazanie w Rejestrze ogólnych środków ochrony Danych Osobowych objętych wyodrębnioną czynnością przetwarzania, Administrator dąży również do wykazania zgodności Przetwarzania Danych Osobowych z wymogami prawa.
3. W Rejestrze, odrębnie dla każdej zidentyfikowanej kategorii czynności przetwarzania Danych osobowych, odnotowuje się co najmniej:
    - nazwę czynności;
    - cel przetwarzania;
    - opis kategorii osób, których Dane osobowe przetwarzane są w ramach danej czynności;
    - opis kategorii Danych osobowych przetwarzanych w ramach danej czynności;
    - podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą przetwarzania jest uzasadniony interes;
    - opis kategorii odbiorców danych, w tym Podmiotów przetwarzających,
    - informację o ewentualnym przekazaniu Danych osobowych poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
    - ogólny opis technicznych i organizacyjnych środków ochrony Danych osobowych, znajdujących zastosowanie do danej czynności.
4. W przypadku uaktualnienia lub poszerzenia kategorii czynności przetwarzania Danych Osobowych, Administrator dokonuje niezwłocznego uaktualnienia Rejestru celem zapewnienia zgodności Rejestru ze stanem faktycznym oraz zakresem operacji przetwarzania Danych osobowych u Administratora.
5. Postanowienia ust. 3wyżej nie wyłączają możliwości ujęcia w Rejestrze w miarę potrzeby informacji dodatkowych, zwiększających szczegółowość lub czytelność Rejestru lub ułatwiających zarządzanie zgodnością ochrony Danych osobowych z wymogami prawa, oraz realizację zasady rozliczalności.
6. Administrator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania poprzez wskazanie ogólnej podstawy prawnej przetwarzania, takiej jak: zgoda, umowa, obowiązek prawny nałożony na Administratora, uzasadniony cel Administratora.

12. REALIZACJA OBOWIĄZKÓW WOBEC OSÓB, KTÓRYCH DANE OSOBOWE DOTYCZĄ

1. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.

2. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których Dane osobowe przetwarza.
3. Administrator pozostawia do wglądu w swojej siedzibie :
    - Politykę;
    - Informację o prawach osób, których dane dotyczą;
    - Informację o zakresie przetwarzanych danych osobowych w poszczególnych celach;
    - Metodach kontaktu z Administratorem w zakresie danych osobowych;
4. W celu realizacji praw osoby, której Dane osobowe dotyczą, Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
5. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, informując osobę, której dane dotyczą:
    - o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby;
    - o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;
    - o planowanej zmianie celu przetwarzania danych;
    - o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe);
    - prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
6. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
7. Niezależnie od postanowień 5wyżej, Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
8. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.
9. Administrator wydaje osobie, której Dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.
10. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której Dane osobowe dotyczą. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
11. Administrator uzupełnia i aktualizuje dane na żądanie osoby, której Dane osobowe dotyczą. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
12. Z uwzględnieniem regulacji, o jakich mowa 13niżej, na żądanie osoby, Administrator usuwa dane, gdy:
    - dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
    - zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

- osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
- dane były przetwarzane niezgodnie z prawem,
- konieczność usunięcia wynika z obowiązku prawnego,
- żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

13. Administrator przy usuwaniu danych osobowych uwzględnia, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.
14. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, podejmuje on rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
15. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
    - osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
    - przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
    - Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
    - osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
16. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.
17. Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Kancelarii, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.
18. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, o którym mowa w art. 21 RODO, a dane przetwarzane są przez Administratora w oparciu o jego uzasadniony interes lub o powierzone mu zadanie w interesie publicznym, Administrator zobowiązuje się uwzględnić sprzeciw, o ile nie zachodzą po jego stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
19. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego, Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

13. MINIMALIZACJA DANYCH

1. Administrator wdraża procedury służące realizacji zasady minimalizacji przetwarzanych Danych Osobowej pod względem:
    - **adekwatności** Danych osobowych **do celów** przetwarzania, obejmujących ograniczenie ilości przetwarzanych Danych Osobowych oraz zakresu przetwarzania do celu Przetwarzania;
    - **ograniczenia dostępu** do Danych osobowych wyłącznie do Osób upoważnionych, dla których wykorzystanie Danych osobowych w określonym zakresie jest niezbędne dla prawidłowej realizacji obowiązków;
    - **ograniczenia czasu przechowywania** Danych osobowych do okresu, dla którego przechowywanie Danych osobowych jest niezbędne ze względu na realizację celu Przetwarzania lub obowiązków nałożonych na Administratora.

2. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

3. Administrator stosuje ograniczenia dostępu do Danych Osobowych poprzez wdrożenie:
    - zobowiązań Pracowników do zachowania poufności, w tym w zakresie Danych Osobowych;
    - weryfikację kręgu wewnętrznych odbiorców Danych Osobowych poprzez nadawanie poszczególnym Pracownikom szczegółowych upoważnień co do Przetwarzania Danych Osobowych;
    - wdrożenie logicznych środków technicznych ochrony Danych osobowych poprzez ograniczenie dostępu do systemów, oprogramowania oraz zasobów sieciowych wykorzystywanych w procesie Przetwarzania Danych Osobowych;
    - wdrożenie fizycznych środków technicznych ochrony Danych osobowychd).
4. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
5. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Administratora.
6. Administrator przetwarza dane osobowe z uwzględnieniem kryteriów wskazanych w Rejestrze. Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
7. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Administratora, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Administratora. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

14. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia Administrator wdraża środki techniczne i

organizacyjne zapewniające należyty stopień ochrony Danych osobowych, odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administratora.

2. Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
    - Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
    - Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Ponadto analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;
3. Administrator wdraża środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

15. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych Osobowych uważa się w szczególności:
    - Naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są Dane osobowe;
    - udostępnienie Danych osobowych osobom nieupoważnionym;
    - przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich Przetwarzania;
    - nieuprawnione lub przypadkowe uszkodzenie, utratę, zniszczenie lub zmianę Danych osobowych.

2. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych oraz szacuje skalę ryzyka.

3. W przypadku naruszenia ochrony Danych Osobowych, Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

4. Jeżeli ryzyko naruszenia praw i wolności osoby, której Dane osobowe dotyczą jest wysokie, Administrator zawiadamia o incydencie także osobę, której danej dotyczą, chyba że:
    - Administrator wdroży odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
    - Administrator zastosuje następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą lub
    - wymagałoby to 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.

5. Niezależnie od obowiązków wskazanych wyżej, Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

16. POWIERZENIE PRZETWARZANIA

1. Administrator może powierzyć Przetwarzanie Danych osobowych Podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi w art. 28 ust. 3 RODO.
2. Administrator korzysta wyłącznie z usług takich Podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. W celu weryfikacji spełnienia obowiązku, o którym mowa w zdaniu poprzedzającym, Administrator przed powierzeniem przetwarzania potencjalnemu Podmiotowi przetwarzającemu w miarę możliwości uzyskuje informacje o zasadach ochrony Danych osobowych stosowanych przez potencjalny Podmiot przetwarzający oraz o praktykach tego podmiotu dotyczących zabezpieczenia Danych osobowych.

   Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych**. Jest on obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

   Administrator danych nadaje upoważnienia osobom przetwarzającym dane osobowe. Prowadzi on wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie**.**

   Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

PODMIOT PRZETWARZAJĄCY

a) Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
b) Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
c) Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora.

To **umowa lub inny instrument prawny** stanowią w szczególności, że podmiot przetwarzający:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
- biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
- uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
- po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
- udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji i przyczynia się do nich.
- udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W związku z obowiązkiem wskazanym w art. 28 ust. 3 lit. h) RODO podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

d) Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między Administratorem a podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

e) Wystarczające gwarancje, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 RODO lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO.

f) Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, mogą się opierać w całości lub w części na standardowych klauzulach umownych, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43 RODO.

g) Bez uszczerbku dla art. 82, 83 i 84 RODO, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za Administratora w odniesieniu do tego przetwarzania.

W celu dochowania szczególnej staranności przy wyborze procesora Administrator ocenia, czy podmiot mający w jego imieniu przetwarzać dane, spełnia wymogi, na przykład poprzez skontrolowanie stosowanych przez niego sposobów zabezpieczenia danych.

17. PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO. ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA. PROCEDURA ANALIZY RYZYKA/OCENA SKUTKÓW

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
Administrator dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem informacji. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami.

Powyższe cele realizowane są dzięki:

- podziałowi odpowiedzialności i obowiązków, umożliwiając pracownikom dopilnowanie, wczesne wykrycie i zminimalizowanie zagrożeń mogących mieć wpływ na ciągłość działania;
- wdrożeniu planów ciągłości działania.

O konieczności tworzenia planu ciągłości działania dla systemu informatycznego decyduje Administrator na podstawie analizy ryzyka.

ZAGADNIENIA OGÓLNE DOTYCZĄCE ANALIZY RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.
Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
W przypadku konieczności przeprowadzenia oceny skutków (art. 35 RODO), wymagane jest wykonanie następujących czynności:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania;
- ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

- ocena ryzyka – środki planowane w celu zaradzenia ryzyku, przedstawione w postaci planu postępowania z ryzykiem.

DEFINICJE

a) **aktywa** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych;
b) **naruszenie (incydent) ochrony danych osobowych** – to 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;
c) **zagrożenie** – potencjalne naruszenie (potencjalny incydent);
d) **skutki** – rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia);
e) **ryzyko** – prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

POTENCJALNE AKTYWA PODLEGAJĄCE ANALIZIE RYZYKA ORAZ OCENIE SKUTKÓW

a) analizie ryzyka poddawane są zbiory danych osobowych, procesy przetwarzania, środki zabezpieczeń, np. zbiór pracowników, zbiór klientów, proces wysyłania informacji handlowej z bazy marketingowej banku, zasady rozliczalności, integralności, poufności, itp.;
b) do analizy wymagane jest zidentyfikowanie aktywów;

WYZNACZENIE ZAGROŻEŃ

a) Administrator jest odpowiedzialny za określenie listy możliwych zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze lub w procesie przetwarzania;
b) zagrożenia powinny być identyfikowane w odniesieniu do aktywów.

WYLICZENIE RYZYKA DLA ZAGROŻEŃ

a) Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania
b) Administrator określa przykładowe skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji
c) Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

PORÓWNANIE WYLICZONYCH RYZYK ZE SKALĄ I OKREŚLENIE DALSZEGO POSTĘPOWANIA Z RYZYKIEM - Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem;

REAKCJA NA WARTOŚĆ RYZYKA

- akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń;
- działania obniżające ryzyko, które może zastosować Administrator:
    a) przekazanie – przerzucenie ryzyka (outsourcing, ubezpieczenie);
    b) unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji);
    c) redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrive'ów z danymi wynoszonych poza firmę).

PLAN POSTĘPOWANIA Z RYZYKIEM

- wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne;
- Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

PONOWNA ANALIZA ZAGROŻEŃ I RYZYKA

Analiza zagrożeń i ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne). W przypadku, gdy analiza ryzyka prowadzona jest w ramach Oceny skutków, wymagana jest do przeprowadzenia przynajmniej raz na 5 lat.

OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH I UPRZEDNIE KONSULTACJE

Jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
Przy ocenie skutków Administrator weryfikuje:

- obowiązek przeprowadzenia oceny skutków dla ochrony danych, metodologii przeprowadzenia oceny skutków dla ochrony danych;
- obowiązek przeprowadzenia wewnętrznej oceny lub zlecenia jej podmiotowi zewnętrznemu;
- skuteczność zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie, oraz jakie zabezpieczenia należy zastosować).

W sytuacji, gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator powinien dokonać przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych. Jeżeli ocena ta wykaże, że przetwarzanie może powodować wysokie ryzyko przy braku zastosowania przez Administratora środków dla zminimalizowania tego ryzyka, to zgodnie z art. 36 RODO Administrator konsultuje się w tej sprawie z organem nadzorczym.

18. PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

OBOWIĄZEK INFORMACYJNY

Osoba, której dane dotyczą, jest informowana o **prowadzeniu operacji przetwarzania i o jego celach**. Ponadto Administrator podaje wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.
Dodatkowo informuje o fakcie **profilowania** oraz o konsekwencjach. W przypadku zbierania danych od osoby, której dane dotyczą, wskazuje, czy ma ona obowiązek je podać oraz o konsekwencjach ich niepodania.

Administrator, w przypadku, gdy zbiera dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO informuje o:

- swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;
- danych kontaktowych inspektora ochrony danych (jeżeli go wyznaczyliśmy);

- celach przetwarzania, do których mają posłużyć dane osobowe;
- podstawie prawnej przetwarzania;
- prawnie uzasadnionym interesie realizowanym przez Administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu Administratora (art. 6 ust. 1 lit. f RODO);
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- transferze danych do państwa trzeciego, w tym o:
- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO;
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także przenoszenia danych;
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych (art. 6 ust. 1 lit. a) RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a RODO);
- prawie do 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 informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

PRAWO DOSTĘPU DO DANYCH

Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

- cele przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- prawo do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- prawo wniesienia skargi do organu nadzorczego;
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczenie i przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą.

PRAWO DO SPROSTOWANIA DANYCH

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Sprostowania danych dokonuje Administrator.

PRAWO DO USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM")

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, o ile zachodzi jedna z przesłanek wskazana w art. 17 RODO.
Usunięcia danych dokonuje Administrator.

PRAWO DO OGRANICZANIA PRZETWARZANIA

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

PRAWO DO PRZENOSZENIA DANYCH

Prawo to zapewnia osobom, których dane dotyczą, możliwość otrzymywania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych, które dostarczyły Administratorowi, oraz możliwość przesłania tych danych osobowych innemu administratorowi bez przeszkód.

Zgodnie z treścią art. 20 ust. 1 lit. a) RODO, prawo do przenoszenia danych znajduje zastosowanie wobec operacji przetwarzania danych na podstawie **zgody** podmiotu danych oraz **umowy**, której podmiot danych jest stroną.

Administrator przekazuje dane za pomocą takich narzędzi jak: „streaming", płyta CD, DVD lub inny fizyczny nośnik bądź przesyła dane bezpośrednio innemu administratorowi (zgodnie z artykułem 20 ust. 2 RODO, gdy jest to technicznie wykonalne).

19. ZABEZPIECZENIE DANYCH – ŚRODKI TECHNICZNE I ORGANIZACYJNE

ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- przetwarzanie danych osobowych administratora może odbywać się **wyłącznie w ramach wykonywania zadań służbowych** (zakres uprawnień wynika z zakresu tych zadań);
- do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie nadane przez Administratora;**
- odwołanie/ unieważnienie upoważnienia następuje na piśmie;
- Administrator prowadzi **ewidencję osób upoważnionych** oraz na jej podstawie przygotowuje upoważnienia. Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją, zrozumieniem wszystkich zasad bezpieczeństwa oraz zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczania;
- Administrator wprowadza **procedurę otwierania i zamykania budynków oraz pomieszczeń biurowych**.
  Do otwierania oraz zamykania budynku uprawnione są osoby wskazane przez Administratora. Po otwarciu budynku osoba uprawniona otwiera pomieszczenie w którym znajdują się i są przechowywane klucze do pozostałych pomieszczeń biurowych. Z pomieszczenia tego pracownicy pobierają klucze do swojego pomieszczenia biurowego, kwitując ich odbiór (na oddzielnej ewidencji bądź w ewidencji czasu pracy).
  W razie niemożności otwarcia bądź zamknięcia pomieszczeń bądź budynku, należy niezwłocznie zawiadomić o tym fakcie osoby zarządzające przedsiębiorstwem lub inne osoby upoważnione. Pomieszczenia biurowe zamykane są na klucz, ewentualnie zabezpieczane są kartą dostępu lub zamkami szyfrowymi. Każdy pracownik odpowiada za swój klucz (ewentualnie kartę lub kod dostępu). W pomieszczeniach biurowych, gdzie przebywa tylko jeden pracownik, jest on zobowiązany do każdorazowego zamknięcia pomieszczenia w przypadku jego opuszczenia, z wyłączeniem pomieszczeń, które łączą się z pomieszczeniami posiadającymi bezpośrednie wyjście na korytarz, pod warunkiem przebywania w pomieszczeniach innych pracowników. Przebywanie pracowników w przedsiębiorstwie po godzinach pracy lub w dni wolne od pracy jest dopuszczalne wyłącznie za zgodą wyrażoną na piśmie lub na podstawie polecenia Administratora.
  Po zakończeniu pracy pracownicy mają obowiązek zamknąć pomieszczenia na klucz, a klucz oddać osobie sprzątającej bądź osobie przebywającej w pomieszczeniu, w którym są przechowywane klucze do pomieszczeń w budynku. Osoba sprzątająca lub inna osoba upoważniona po zakończeniu pracy ma obowiązek sprawdzenia pomieszczeń biurowych,

korytarzy oraz innych pomieszczeń znajdujących się w przedsiębiorstwie celem stwierdzenia możliwości zamknięcia budynku.

Osoby dysponujące kluczami zobowiązane są do odpowiedniego zabezpieczenia kluczy przed ich zgubieniem bądź kradzieżą. W przypadku zagubienia klucza bądź stwierdzenia jego braku pracownik zgłasza ten fakt Administratorowi bądź osobie przez niego upoważnionej, celem dorobienia bądź wydania kluczy zapasowych.

Zabrania się pracownikom samodzielnego dorabiania kluczy do jakichkolwiek pomieszczeń w przedsiębiorstwie. Zabrania się pozostawiania kluczy w zamkach od drzwi podczas obecności bądź nieobecności pracownika w danym pomieszczeniu. Zabrania się udostępniania kluczy osobom nieupoważnionym.

- W celu zapobiegania nieautoryzowanemu dostępowi do informacji lub kradzieży informacji i środków jej przetwarzania stosuje się **Politykę czystego biurka**. Reguluje ona zasady ochrony danych osobowych przetwarzanych u Administratora w formie papierowej (dokumenty papierowe, dokumentacja listowa, dokumenty przekazywane przez klientów, korespondencję urzędową).

  Pracownicy Administratora zobowiązani są do ograniczenia dostępu osób postronnych do danych osobowych zawartych na nośnikach papierowych wykorzystywanych przy wykonywaniu obowiązków służbowych. W toku pracy pracownicy zobowiązani są do przechowywania na biurku lub przy stanowisku pracy tylko tych dokumentów, które są mu niezbędne do wykonywania bieżących zadań w danym momencie pracy.

  Ważne dokumenty i nośniki zawierające dane osobowe nie powinny pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pokoju. Pokój należy zamknąć w sposób uniemożliwiający dostęp dla osób nieuprawnionych. Ponadto w toku pracy przy stanowisku pracy nie powinny znajdować się płyny lub inne substancje grożące zniszczeniem lub uszkodzeniem dokumentacji papierowej przy ich rozlaniu.

  Po zakończeniu pracy dokumenty i nośniki z danymi osobowymi powinny być przechowywane w szafach, a pokoje powinno się zamykać, celem zabezpieczenia dokumentacji przed dostępem do niej osób postronnych. Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników. Pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenie zleconego zadania. Nie powinny one pozostawać dostępne ani dla obcych osób ani dla pracowników nieposiadających stosownych uprawnień. Jeżeli dany dokument nie będzie już wykorzystywany w przedsiębiorstwie Administratora, dokumenty te powinny zostać niezwłocznie zniszczone w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji (czyli np. z wykorzystaniem niszczarki), chyba że dokumenty te zgodnie z niniejszą Polityką lub innymi przepisami obowiązującymi u Administratora powinny zostać zarchiwizowane.
- **Polityka czystego ekranu** ma na celu zabezpieczenie przed nieautoryzowanym dostępem do systemu informatycznego i zabezpieczeniem przed ujawnieniem informacji chronionych. Każdorazowe odejście od stanowiska pracy powinno być poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu tak, aby niemożliwe było uzyskanie nieautoryzowanego dostępu do systemu. W tym celu każdy komputer powinien mieć wprowadzony system automatycznego uruchamiania się wygaszania ekranu i wylogowania użytkownika. Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wyrejestrować się (wylogować się) z systemu lub też zablokować dostęp do systemu.
- Zabrania się udzielania informacji o danych osobowych w formie telefonicznej bez weryfikacji tożsamości rozmówcy.

ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje stuprocentowego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik mający styczność z przetwarzanymi danymi, świadom odpowiedzialności, postępował zgodnie z przyjętymi w niniejszym dokumencie zasadami i minimalizował zagrożenie wynikające z błędów ludzkich. Ochrona danych osobowych przetwarzanych przez Administratora obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.

Przetwarzać dane osobowe w systemach informatycznych jak i tradycyjnych zbiorach papierowych u Administratora może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.

Zbiory danych u Administratora zabezpiecza się poprzez:

1. ŚRODKI OCHRONY FIZYCZNEJ:

- ☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi)
- ☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min
- ☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C
- ☐ Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej
- ☐ Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy
- ☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu
- ☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych
- ☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony
- ☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez całą dobę jest nadzorowany przez służbę ochrony
- ☐ Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie
- ☐ Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie
- ☐ Zbiór danych osobowych w formie papierowej przechowywany jest w niemetalowej szafie
- ☐ Zbiór danych osobowych w formie papierowej przechowywany jest w metalowej szafie
- ☐ Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej
- ☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie

- ☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie
- ☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej
- ☐ Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach
- ☐ Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego
- ☐ Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy
- ☐ Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów

2. ŚRODKI SPRZĘTOWE, INFRASTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ

- ☐ Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania
- ☐ Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS
- ☐ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora (login) użytkownika oraz hasła
- ☐ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena
- ☐ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej
- ☐ Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych
- ☐ Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł
- ☐ Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych
- ☐ Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji
- ☐ Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia
- ☐ Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu
- ☐ Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej
- ☐ Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity
- ☐ Użyto system Firewall do ochrony dostępu do sieci komputerowej

- ☐ Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej
- ☐ Użyto Program Antywirusowy, który zapewnia ochronę przed wirusami i oprogramowaniem szpiegującym, bez względu na rodzaj systemu operacyjnego
- ☐ Użyto filtr antyspamowy
- ☐ Użyto programu , który szyfruje dane na dyskach

3. ŚRODKI OCHRONY W RAMACH SYSTEMOWYCH NARZĘDZI PROGRAMOWYCH I BAZ DANYCH

- ☐ Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych
- ☐ Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych
- ☐ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła z wyłączeniem aplikacji biurowych (takich jak produkty Microsoft Office, procesory tekstu, arkusze kalkulacyjne, programy pocztowe)
- ☐ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena
- ☐ Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej
- ☐ Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego
- ☐ Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych
- ☐ Zastosowano kryptograficzne środki ochrony danych osobowych
- ☐ Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe
- ☐ Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika
- ☐ Kopie zapasowe tworzone są w obrębie serwera
- ☐ Kopie zapasowe tworzone są na dyskach zewnętrznych

Administrator dokłada szczególnej staranności w celu zapewnienia, że wszystkie podmioty, którym powierza się przetwarzanie danych osobowych gwarantują środki zabezpieczeń co najmniej na poziomie uznanym przez Administratora za obligatoryjny. Administrator dokonuje oceny czy podmiot mający w jego imieniu przetwarzać dane osobowe spełnia wymogi dotyczące środków zabezpieczeń.

PRZEGLĄD SYSTEMU OCHRONY DANYCH

System Ochrony Danych jest monitorowany poprzez podjęcie następujących działań:

- wykonywanie audytów wewnętrznych przez Administatora;
- wykonywanie okresowych przeglądów dokonywanych przez kierownictwo;
- wykonywanie analizy ryzyka.

20. SZKOLENIA OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

Obieg informacji dotyczących nadawania uprawnień w przedsiębiorstwie Administratora przedstawia się następująco: osoba odpowiedzialna za zatrudnienie informuje Administratora o każdej nowozatrudnionej osobie przetwarzającej dane osobowe, celem nadania uprawnień oraz przeszkolenia takiej osoby.

Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna zostać przeszkolona i zapoznana z przepisami z zakresu ochrony danych osobowych, w szczególności regulacjami wewnętrznymi zawartymi w Polityce Ochrony Danych Osobowych oraz przepisami RODO. **Za przeprowadzenie szkolenia odpowiada Administrator**.
Potwierdzeniem zapewnienia zapoznania przepisów stanowić może pozytywnie zdany test. Szkolenia są przeprowadzane cyklicznie co najmniej raz na 2 lata. Potwierdzenie odbycia szkolenia przez uczestników są dokumentowane.
Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy powinni pisemnie potwierdzić znajomość tych zasad.

21. BEZPIECZEŃSTWO DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

POSTANOWIENIA OGÓLNE

1. Za przestrzeganie zapisów dotyczących bezpieczeństwa danych w systemach informatycznych odpowiedzialny jest Administrator.
2. Obszar, w którym są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora.
3. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe, tablety i smartfony. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych **tzw. Polityka czystego ekranu.**

PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.

Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych**.**
Upoważnienia do przetwarzania danych osobowych rejestrowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych.

STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZENIEM I UŻYTKOWANIEM

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem:

- hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów;
- hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
- hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury;
- hasło nie może być jednakowe z identyfikatorem użytkownika;
- hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności. **W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie Administratora.**

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora.
2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
3. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.
4. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych płyty CD, pendrive i inne, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

Kopie zapasowe powinny być kontrolowane przez administratora w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

- działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego: poprzez zainstalowanie programu antywirusowego lub poprzez zainstalowanie firewalla (zapora sieciowa).
- utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie urządzenia chroniącego system informatyczny przed skutkami awarii zasilania typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną.

Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

Kopie zapasowe:

- przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym;
- usuwa się niezwłocznie po ustaniu ich użyteczności.

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są przez Administratora.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności Administratora. W innym przypadku musi być zawarta umowa powierzenia danych osobowych.

Przeglądy techniczne powinny być wykonywane nie rzadziej niż raz na dwa lata.
Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni Administrator.

PROCEDURA W PRZYPADKU WYSTĄPIENIA INCYDENTÓW

W przypadku stwierdzenia uchybień dotyczących przetwarzania danych każda osoba powinna o tym fakcie niezwłocznie powiadomić Administratora. Następnie Administrator wprowadza zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

KONTROLA STANU ZABEZPIECZEŃ

Administrator ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

ZASADY KORZYSTANIA Z INTERNETU

- użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach;

- użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu;
- zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem);
- nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł;
- w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel;
- należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

- przesyłanie danych osobowych z użyciem maila poza przedsiębiorstwo może odbywać się tylko przez osoby do tego upoważnione;
- w przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny);
- użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu;
- zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata;
- **nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy**. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu” infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy;
- bez weryfikacji wiarygodności nadawcy, nie należy „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając” na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy;
- należy zgłaszać informatykowi przypadki podejrzanych maili;
- podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW” lub „Do wiadomości”- w zależności czy adresaci znają swoje adresy mailowe
- przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego;
- użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

22. POSTĘPOWANIE W WYPADKU KLĘSKI ŻYWIOŁOWEJ

Klęską żywiołową jest katastrofa spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

Każda osoba, która będzie świadkiem zbliżania się w/w zagrożeń jest obowiązana powiadomić o tym Administratora w każdy możliwy sposób. Numer telefonu Administratora jest znany pracownikom i współpracownikom. Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez innych obowiązków wskazanych w dokumentacji.

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:

- zamknięcia systemu informatycznego;
- zabezpieczenia danych osobowych przetwarzanych tradycyjnie.

W czasie trwania akcji ratunkowej i po jej zakończeniu administrator oraz obecni użytkownicy powinni w miarę możliwości zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem, o ile nie stoi to w sprzeczności z poleceniami wydanymi przez służby ratunkowe

23. POSTANOWIENIA KOŃCOWE

Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

Każda osoba przetwarzająca dane osobowe zapoznaje się z treścią Polityki Ochrony Danych Osobowych oraz zobowiązuje się do stosowania postanowień w niej zawartych przy przetwarzaniu danych osobowych.
Administrator nie przekazuje Danych osobowych do państwa trzeciego położonego poza terytorium Unii Europejskiej lub Europejskiego Obszaru Gospodarczego, poza sytuacjami, w których następuje to na wniosek osoby, której Dane osobowe dotyczą. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Administrator okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

Polityka wchodzi w życie z dniem ogłoszenia.
W sprawach nieuregulowanych w Polityce odpowiednie zastosowanie znajdują postanowienia RODO oraz powszechnie obowiązujące przepisy prawa polskiego i europejskiego.
Wszelkie zmiany lub uzupełnienia do Polityki wymagają dla swej skuteczności formy pisemnej pod rygorem nieważności. Zmiany lub uzupełnienia do Polityki wchodzą w życie nie wcześniej niż w terminie 7 dni od dnia ich ogłoszenia.

Do Polityki dołączono następujące Załączniki, stanowiące integralną część Polityki:

1. Załącznik nr 1 – Lista Zbiorów danych u Administratora;
2. Załącznik nr 2 – Formularz zgody na potrzeby procesu rekrutacji;
3. Załącznik nr 3 – Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych;
4. Załącznik nr 4 – Ewidencja naruszeń ochrony danych osobowych;
5. Załącznik nr 5 – Upoważnienie do przetwarzania danych osobowych;
6. Załącznik nr 6 – Wzór unieważnienia upoważnienia do przetwarzania danych osobowych;
7. Załącznik nr 7 – Ewidencja osób upoważnionych do przetwarzania danych osobowych;
8. Załącznik nr 8 – Oświadczenie o poufności;
9. Załącznik nr 9 – Karta szkolenia z zakresu ochrony danych osobowych.