Videofonika spółka z ograniczoną odpowiedzialnością spółka komandytowa

Polityka Ochrony Danych Osobowych

dokument poufny

Kancelaria Pałucki & Szkutnik
2019-04-30

Spis treści

Preambuła

Niniejszą Politykę Ochrony Danych Osobowych w firmie Videofonika sp. z o.o. sp.k. opracowano w oparciu o przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, na podstawie przeprowadzonego audytu i w oparciu o analizę ryzyka.

Polityka Ochrony Danych Osobowych jest zbiorem dokumentów określających zasady dotyczące zapewnienia bezpieczeństwa w zakresie ochrony danych osobowych przetwarzanych metodą tradycyjną oraz informatyczną.

Najważniejszymi filarami ochrony danych osobowych w Firmie są:

***Legalność** − Firma dba o ochronę prywatności i przetwarza dane zgodnie z prawem.*

***Bezpieczeństwo** − Firma zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.*

***Prawa Jednostki** − Firma umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.*

***Rozliczalność** − Firma dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.*

Firma przetwarza dane osobowe z poszanowaniem następujących zasad:

a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

b) rzetelnie i uczciwie (rzetelność);

c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

d) w konkretnych celach i nie „na zapas" (minimalizacja);

e) nie więcej niż potrzeba (adekwatność);

f) z dbałością o prawidłowość danych (prawidłowość);

g) nie dłużej niż potrzeba (czasowość);

h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

Poszanowanie określonych w niniejszej Polityce Ochrony Danych Osobowych zasad stanowi podstawę należytego przetwarzania danych.

CZĘŚĆ I POLITYKI OCHRONY DANYCH OSOBOWYCH

Rozdział I Postanowienia ogólne

Przedmiot regulacji

§ 1.

1. Polityka ochrony danych określa zasady dotyczące przetwarzania i zabezpieczenia danych osobowych w **Videofonika sp. z o.o. sp.k.** zgodnie z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. Niniejszy dokument stanowi wykonanie obowiązku, o którym mowa w art. 24 ust. 2 RODO.
3. Polityka znajduje zastosowanie do wszystkich procesów przetwarzania danych osobowych w Firmie.
4. Polityka znajduje zastosowanie do wszelkich czynności stanowiących przetwarzanie danych osobowych, bez względu na źródło pochodzenia danych, ich zakres, cel zebrania, sposób przetwarzania i okres przetwarzania.
5. Polityka znajduje zastosowanie do danych powierzonych Administratorowi do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz do danych osobowych, które zostały Administratorowi udostępnione.
6. Obowiązek ochrony danych osobowych przetwarzanych w Firmie, a tym samym obowiązek przestrzegania niniejszej Polityki, odnosi się do wszystkich osób, które mają do nich dostęp bez względu na zajmowane stanowisko, miejsce wykonywania pracy, jak również prawną formę świadczenia pracy. Powyższe oznacza, iż Polityka znajduje zastosowanie do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w Firmie na podstawie umowy o pracę oraz świadczących na jej rzecz usługi w oparciu o umowę cywilnoprawną czy też na innej podstawie prawnej (w szczególności osób odbywających staż, wolontariuszy, praktykantów).
7. Każda osoba, która w ramach wykonywanych obowiązków służbowych przetwarza dane osobowe, może je przetwarzać wyłącznie na podstawie otrzymanego upoważnienia.

8. Każda osoba przetwarzająca dane osobowe w Firmie zobowiązana jest do zapoznania się z Polityką i innymi powiązanymi z nią dokumentami oraz do stosowania zawartych w nich regulacji. Osoba, która zapoznała się z Polityką, winna złożyć swój podpis opatrzony datą pod oświadczeniami stanowiącymi **Załącznik nr 1** do Polityki.

9. Polityka winna być interpretowana w zgodzie z aktualnie obowiązującymi przepisami. Wszelkie wątpliwości interpretacyjne winny być rozstrzygane przy pełnym poszanowaniu zasad ochrony danych osobowych wskazanych w Preambule Polityki.

10. W przypadku gdy nie jest możliwe jednoznaczne ustalenie wymaganego przepisami sposobu postępowania, należy zastosować rozwiązanie zapewniające pełniejszą ochronę przetwarzania danych osobowych.

11. Nadzór nad aktualizacją Polityki sprawuje Inspektor a w razie jego niepowołania bezpośrednio Administrator. Aktualizacja Polityki winna nastąpić w szczególności w przypadku zmiany przepisów, wydania nowych wytycznych organu nadzorczego lub Europejskiej Rady Ochrony Danych bądź gdy okaże się, że aktualne postanowienia Polityki pozostają nieadekwatne do stopnia wymaganego w Organizacji poziomu ryzyka.

12. Firma zatwierdza w drodze uchwały/zarządzenia Politykę i jej aktualizacje.

Definicje

§ 2.

Występujące w niniejszej Polityce zwroty oznaczają:

1) **Administrator Danych Osobowych (ADO, Administrator lub zamiennie Firma, Organizacja) –** Videofonika spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Trzebini, ul. 32-540, wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod nr KRS: 0000545410, posiadająca NIP: 6282263617.

2) **Administrator Systemu Informatycznego (ASI) –** osoba wyznaczona przez Administratora do opieki nad systemem informatycznym, administracji i zarządzania środowiskiem IT w Organizacji.

3) **Dane osobowe –** wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników

określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

4) **Dane osobowe wrażliwe –** szczególne kategorie danych określone w art. 9 RODO, w tym: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby; jak również dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa, o których mowa w art. 10 RODO.

5) **Hasło –** ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

6) **Identyfikator –** ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

7) **Inspektor ochrony danych (Inspektor, IOD) –** osoba wyznaczona przez Administratora danych na podstawie art. 37 RODO, która realizuje zadania monitorowania przestrzegania przepisów o ochronie danych osobowych w Firmie, określone w art. 39 RODO.

8) **Integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmodyfikowane, usunięte, dodane czy zniszczone w sposób nieautoryzowany.

9) **Komórka organizacyjna (KO) –** Departament, Dział, Zespół, samodzielne stanowisko – wynikające z przyjętej w Firmie struktury organizacyjnej.

10) **Naruszenie ochrony danych osobowych –** naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

11) **Obszar przetwarzania danych osobowych –** pomieszczenia lub części pomieszczeń we wszystkich lokalizacjach Firmy, w których są przetwarzane dane osobowe, zarówno w formie papierowej, jak i w systemie informatycznym.

12) **Odbiorca danych –** podmiot, któremu udostępniane są dane osobowe.

13) **Osoba upoważniona –** osoba upoważniona do przetwarzania danych osobowych przez Administratora lub osobę przez niego upoważnioną, mająca bezpośredni dostęp do danych, przetwarzanych w systemie informatycznym lub w dokumentacji papierowej.

14) **Państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.

15) **Podmiot przetwarzający (Procesor)** – podmiot, któremu Firma powierza czynności przetwarzanie danych osobowych w swoim imieniu.

16) **Polityka ochrony danych osobowych (Polityka)** – niniejszy dokument stanowiący zespół regulacji i procedur obowiązujących w Organizacji, utworzony w celu zapewnienia zgodnego z prawem przetwarzania danych osobowych.

17) **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

18) **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.

19) **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

20) **PUODO (organ nadzorczy)** – Prezes Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie.

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

22) **Rozliczalność** – właściwość zapewniająca, że Administrator jest w stanie wykazać, że stosowane przez niego metody są zgodne z RODO oraz skuteczne.

23) **Sieć telekomunikacyjna** - sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne.

24) **Stacja robocza –** stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom dostęp do danych osobowych znajdujących się w systemie.

25) **Teletransmisja –** przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

26) **UODO –** ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018, poz. 1000).

27) **Uwierzytelnianie –** działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

28) **Użytkownik –** osoba upoważniona do przetwarzania danych osobowych w systemach informatycznych, której nadano identyfikator i przyznano hasło.

29) **Zasób danych osobowych –** wszystkie dane osobowe, niezależnie od sposobu ich utrwalenia, zarówno w formie elektronicznej – w systemie informatycznym oraz na nośnikach (płyty CD/DVD/BD, pamięci flash i inne), jak i papierowej, przetwarzane przez KO/Firmę w celu realizacji jej zadań.

30) **Zbiór danych osobowych –** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rozdział II Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem

Osoby odpowiedzialne za przetwarzanie danych

§ 3.

1. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z przepisami RODO, UODO, przepisami ustaw sektorowych oraz Polityki, odpowiadają:

   a) Administrator,

   b) Inspektor ochrony danych,

   c) Administrator systemu informatycznego,

   d) kierownicy komórek organizacyjnych,

   e) osoby upoważnione do przetwarzania danych osobowych.

2. Jeżeli w Organizacji nie wyznaczono Inspektora, to postanowienia odnoszące się do Inspektora stosuje się odpowiednio do osoby, której przydzielono obowiązki z zakresu ochrony danych osobowych.

3. Jeżeli w Organizacji nie wyznaczono Administratora systemu informatycznego, to postanowienia odnoszące się do ASI stosuje się odpowiednio do osoby, której przydzielono obowiązki związane z opieką nad systemem informatycznym, jego administracją i zarządzaniem środowiskiem IT w Organizacji.

4. Jeżeli w Organizacji nie wyznaczono osoby, o której mowa w ust. 2 lub 3 powyżej, to zadania i obowiązki w tym zakresie realizuje Administrator.

Obowiązki Administratora

§ 4.

1. Administrator w procesie przetwarzania danych osobowych jest odpowiedzialny za:

   1) zapewnienie odpowiednich środków organizacyjnych i technicznych celem przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,

   2) wdrożenie odpowiednich procedur ochrony danych osobowych,

   3) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako elementu dla stwierdzenia przestrzegania przez Firmę ciążących na nim obowiązków, w przypadku gdy uzna to za konieczne,

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

   5) prowadzenie rejestru czynności przetwarzania danych osobowych,

   6) prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,

   7) współpracę z organem nadzorczym,

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

   9) zawiadomienie o naruszeniu ochrony danych osobowych właściwego organu nadzorczego, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, zgłoszenie osobie, której dane dotyczą,

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

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

12) nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

13) zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,

14) zapewnienie, że Inspektor jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych oraz wspieranie IOD w wypełnianiu jego zadań poprzez zapewnienie niezbędnych zasobów do wykonywania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania,

15) zagwarantowanie by Inspektor nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań, a także publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

2. Do obowiązków Administratora należy w szczególności:

1) zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:

a) została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych,

b) został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą,

c) dane były przetwarzane zgodnie z obowiązującymi przepisami prawa, dobrymi praktykami oraz normami społecznymi,

d) dane zbierane były w oznaczonym, zgodnym z prawem celu,

e) dane były merytorycznie poprawne oraz zakres danych był adekwatny do celu zbierania,

f) dane były przetwarzane z ograniczeniem czasowym.

2) prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych.

3) dopuszczanie do przetwarzania danych wyłącznie osoby posiadającej upoważnienie lub/i przeszkolonej z zakresu ochrony danych osobowych, wydawanie i zarządzanie upoważnieniami, którego wzór stanowi **Załącznik nr 2** do Polityki, oraz prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania danych osobowych, stanowiącej **Załącznik nr 3a** do Polityki, jak również prowadzenie i aktualizacja ewidencji przydziału kluczy do poszczególnych pomieszczeń stanowiącej **Załącznik nr 3b** do Polityki.

4) nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

5) respektowanie prawa osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:

a) Administratorze i jego danych kontaktowych,

b) danych kontaktowych Inspektora,

c) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania,

d) prawnie uzasadnionych interesach realizowanych przez Administratora lub przez osoby trzecie,

e) odbiorcach danych osobowych lub o kategoriach odbiorców,

f) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,

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

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

i) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

j) prawie wniesienia skargi do organu nadzorczego,

k) tym, 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 konsekwencje niepodania danych,

l) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,

m) innym celu przetwarzania danych, jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane,

n) źródle pochodzenia danych osobowych.

6) respektowanie praw osób, których dane dotyczą w zakresie:

a) uprawnienia do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące,

b) uzyskania dostępu do danych osobowych oraz informacji,

c) prawa do uzyskania kopii,

d) prawa do sprostowania i uzupełnienia danych,

e) prawa do usunięcia danych,

f) prawa do ograniczenia przetwarzania,

g) prawa do przenoszenia danych,

h) prawa do wniesienia sprzeciwu wobec przetwarzania dotyczących ich danych osobowych,

i) prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

7) przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych.

8) zapewnienie prawidłowej eksploatacji systemu, zgodnej z celami przetwarzania danych osobowych.

9) szkolenie użytkowników systemu informatycznego w zakresie procedur i instrukcji zapewniających ochronę danych osobowych.

10) wyjaśnianie wszystkich zgłoszonych nieprawidłowości i incydentów.

11) wykonywanie przeglądu, konserwacji oraz uaktualnienia systemów służących do przetwarzania danych.

12) zapewnienie bezpieczeństwa w sieci komputerowej.

13) nadawanie, zmiany lub pozbawianie uprawnień dostępu do systemu informatycznego użytkowników.

14) nadzorowanie ochrony antywirusowej.

15) wykonywanie kopii bezpieczeństwa.

3. Administrator wyznacza Inspektora, o ile obowiązek jego wyznaczenia wynika z powszechnie obowiązujących przepisów lub gdy uzna to za konieczne z innych przyczyn, przy uwzględnieniu zasad ochrony danych osobowych oraz z poszanowaniem zapewnienia adekwatnego stopnia ochrony danych osobowych w Organizacji.

4. Administrator wyznacza Administratora systemu informatycznego, o ile uzna to za konieczne.

5. Administrator nadzoruje działania Inspektora ochrony danych oraz Administratora systemu informatycznego.

6. Administrator każdorazowo dokonuje ostatecznej akceptacji najważniejszych z perspektywy organizacji działań Inspektora ochrony danych oraz Administratora systemu informatycznego, w które zaangażowane są podmioty trzecie, przy zachowaniu i poszanowaniu pełnej niezależności Inspektora.

Weryfikacja obowiązku wyznaczenia Inspektora

§ 5.

1. Administrator zobowiązany jest do wyznaczenia Inspektora zawsze w sytuacji, gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości, przy czym rekomendowane jest powołanie Inspektora również w sytuacji, gdy prywatne jednostki realizują zadania w interesie publicznym lub sprawując władzę publiczną;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych

osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

2. Na dzień sporządzenia Polityki Administrator nie jest zobowiązany do wyznaczenia Inspektora w związku z brakiem aktualizacji przesłanek wskazanych w ust. 1 powyżej. Szczegółowy raport weryfikujący istnienie obowiązku wyznaczenia Inspektora stanowi **Załącznik nr 4**.

3. W wypadku gdy weryfikacja obowiązku wyznaczenia Inspektora prowadzi do negatywnych wniosków powyższe nie stoi na przeszkodzie fakultatywnego wyznaczenia Inspektora.

4. W wypadku gdy weryfikacja obowiązku wyznaczenia Inspektora nie prowadzi do jednoznacznych wniosków Administrator winien wyznaczyć Inspektora.

5. Administrator zobowiązany jest do przeprowadzenia czynności weryfikujących istnienie obowiązku wyznaczenia Inspektora co 12 miesięcy, z zastrzeżeniem dokonania weryfikacji w czasie krótszym, w szczególności w przypadku wydania nowych wytycznych przez organ nadzorczy lub Europejską Radę Ochrony Danych.

6. Administrator zobowiązany jest do opublikowania danych kontaktowych Inspektora (adres e-mail lub/i numer telefonu) na stronie internetowej Firmy oraz podania ich do wiadomości pracowników/współpracowników (imię, nazwisko, adres e-mail, numer telefonu).

Obowiązki Inspektora

§ 6.

1. Inspektor ochrony danych jest wyznaczany przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania swoich zadań.

2. Administrator może wyznaczyć zastępców Inspektora oraz inne osoby, które wchodzą w skład Zespołu Inspektora i wspomagają wykonywanie zadań monitorowania ochrony danych w Firmie.

3. Do podstawowych zadań Inspektora ochrony danych należy:

   a) informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,

   b) monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,

c) monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,

d) doradztwo w zakresie podziału obowiązków, przykładowo pomiędzy Administratorem a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora,

e) działania zwiększające świadomość pracowników Administratora w zakresie obowiązków wynikających z RODO lub przyjętych procedur,

f) szkolenia dla pracowników Administratora uczestniczących w operacjach przetwarzania danych,

g) przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,

h) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,

i) współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,

j) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO,

k) monitorowanie zmian przepisów z zakresu ochrony danych osobowych, wydania nowych lub modyfikacji dotychczasowych wytycznych organu nadzorczego lub Europejskiej Rady Ochrony Danych.

Obowiązki Administratora systemu

§ 7.

1. Funkcję Administratora systemu pełni osoba wyznaczona przez Administratora.
2. Administrator systemu informatycznego w szczególności:

   a) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji Administratora;

   b) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

c) na wniosek właściwej osoby oraz po zaakceptowaniu przez Administratora, przydziela każdemu użytkownikowi identyfikator i hasło do systemu informatycznego oraz na polecenie Administratora dokonuje ewentualnych modyfikacji uprawnień;

d) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

e) podejmuje działania w zakresie ustalenia i kontroli identyfikatorów dostępu do systemu informatycznego;

f) wyrejestrowuje użytkowników na polecenie Administratora;

g) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora oraz Inspektora o naruszeniu i współpracuje z nim przy usuwaniu skutków naruszenia;

h) nadzoruje wykonywanie napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe, sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;

i) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;

j) identyfikuje i analizuje zagrożenia oraz ocenia ryzyka, na które może być narażone przetwarzanie danych osobowych w systemie informatycznym;

k) inicjuje i nadzoruje wdrażanie nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemem informatycznym, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,

l) dokonuje cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemie informatycznym,

m) współpracuje z Inspektorem ochrony danych w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemie informatycznym,

n) uwzględnia zasady ochrony danych w fazie projektowania („privacy by design") oraz domyślnej ochrony danych („privacy by default") przy planowaniu realizacji nowych procesów związanych z

przetwarzaniem danych osobowych, w tym w szczególności nowych systemów informatycznych służących do przetwarzania danych osobowych.

Obowiązki kierowników komórek organizacyjnych

§ 8.

1. Kierownicy komórek organizacyjnych są odpowiedzialni za zarządzanie procesami przetwarzania danych osobowych w swoich komórkach. Do obowiązków kierowników należy:

   a) zarządzanie czynnościami przetwarzania danych osobowych w ramach zadań, realizowanych przez swoje KO;

   b) występowanie z wnioskami do Administratora lub ASI o nadanie, zmianę lub cofnięcie uprawnień pracownikom do określonych zasobów danych osobowych przetwarzanych w systemie informatycznym, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych;

   c) zapoznanie podległych pracowników i innych osób (np. współpracowników) z zasadami przetwarzania i ochrony danych w podległej KO;

   d) wypełnianie obowiązków dotyczących zabezpieczenia obszaru przetwarzanych danych osobowych w podległej KO;

   e) zgłaszanie do Inspektora zamiaru rozpoczęcia nowego procesu przetwarzania danych osobowych lub zmiany w czynnościach przetwarzania danych realizowanych w KO;

   f) w przypadku zbierania danych osobowych, konsultowanie z Inspektorem podstaw prawnych przetwarzania danych osobowych, w tym zbierania i archiwizowanie zgód osób na przetwarzanie ich danych osobowych w wymaganych przypadkach;

   g) ustalanie w porozumieniu z ASI zasad tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w podległej KO.

Osoby upoważnione

§ 9.

1. Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do

niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, rozwiązanie innej umowy łączącej tę osobę z Firmą, powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

2. Osoby upoważnione pisemnie oświadczają, że zobowiązują się do zachowania tajemnicy danych osobowych oraz do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa i przestrzegania procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia w Firmie, cały okres obowiązywania innej umowy łączącej użytkownika z Firmą, a także po ustaniu stosunku pracy, rozwiązaniu innej umowy łączącej osobę upoważnioną z Firmą.

3. Naruszenie przez osoby upoważnione lub osoby nieposiadające upoważnienia, będące pracownikami Firmy, procedur bezpiecznego przetwarzania tych danych, w szczególności świadome udostępnienie danych osobie niepowołanej, lub przetwarzania danych wobec braku podstaw, jest ciężkim naruszeniem obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy bez wypowiedzenia.

4. Osoby upoważnione zobowiązują się do:

   a) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami Polityki służącymi do przetwarzania danych osobowych;

   b) stosowania określonych przez Administratora procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

   c) odpowiedniego zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym;

   d) informowania Administratora niezwłocznie od powzięcia wiedzy o wszelkich podejrzeniach naruszenia lub stwierdzonych naruszeniach oraz wadach systemu przetwarzającego dane osobowe – informacja winna zostać przekazana na adres poczty elektronicznej Administratora.

5. Specjalista do spraw kadrowych jest odpowiedzialny za:

   a) przygotowanie upoważnienia do przetwarzania danych osobowych wraz z umową o pracę/zlecenia/dzieło;

   b) przechowywanie nadanych upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu tajemnicy danych

osobowych i sposobów ich zabezpieczania wraz z aktami osobowymi pracowników lub umowami cywilnoprawnymi;

c) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych.

Rozdział III Podstawowe zasady, które powinny przestrzegać osoby upoważnione do przetwarzania danych osobowych

§ 10.

1. Wykaz podstawowych obowiązków osoby upoważnionej do przetwarzania danych osobowych w Firmie stanowi **Załącznik nr 5** do niniejszej Polityki.
2. Każda osoba upoważniona zobowiązana jest do bezwzględnego przestrzegania obowiązków, o których mowa w ust. 1, również po ich aktualizacji.

Rozdział IV Analiza ryzyka

Dobór odpowiednich środków technicznych i organizacyjnych

§ 11.

1. Dobór środków technicznych i organizacyjnych dotyczących przetwarzania i zabezpieczania danych osobowych w Firmie realizowany jest w oparciu o szacowanie ryzyka naruszenia praw i wolności osób, których dane dotyczą.
2. Przy doborze zabezpieczeń należy oceniać ryzyko zarówno w kontekście skutków dla osoby, której dane dotyczą w tym np. dyskryminacja, pozbawienie przysługujących praw, szkody majątkowe i niemajątkowe, jak również ryzyko w kontekście skutków dla Firmy w przypadku niepodjęcia działań związanych z zapewnieniem przetwarzania danych osobowych zgodnie z RODO.

Podstawowa analiza ryzyka

§ 12.

1. Administrator, wdrażając odpowiednie środki techniczne i organizacyjne, uwzględnia stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia po to, aby przetwarzanie odbywało się zgodnie z RODO i aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2. Analizę ryzyka należy dokonywać:

   a) cyklicznie,

   b) w razie zmiany charakteru, zakresu, kontekstu lub celu przetwarzania,

   c) w razie przetwarzania danych w nowym celu.

3. W przypadku gdy analiza ryzyka wykaże umiarkowane, wysokie lub bardzo wysokie ryzyko naruszenia praw lub wolności osób fizycznych konieczne jest niezwłoczne podjęcie adekwatnych środków minimalizujących ryzyko.

4. Procedura analizy ryzyka stanowi **Załącznik nr 6a i 6b** do Polityki.

Ocena skutków dla ochrony danych (DPIA)

§ 13.

1. W przypadku realizacji procesów przetwarzania danych osobowych w Firmie, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO.

2. Niezależnie od zaistnienia sytuacji, o której mowa w ust. 1, przeprowadzenie oceny skutków dla ochrony danych osobowych jest konieczne w przypadkach określonych w art. 35 ust. 3 i 4 RODO.

3. Inspektor w prowadzonym rejestrze czynności przetwarzania danych osobowych wskazuje procesy, dla których należy przeprowadzać ocenę skutków oraz odnotowuje jej przeprowadzenie.

4. Jeżeli dokonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby nie zostały zastosowane środki w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania należy skonsultować się z organem nadzorczym.

5. W przypadku konieczności przeprowadzenia konsultacji z organem nadzorczym Inspektor przygotowuje odpowiedni wniosek o konsultacje zgodnie z art. 36 RODO i kontaktuje się w tej sprawie z organem nadzorczym.

6. Ocenę skutków dla ochrony danych przeprowadza się według procedury stanowiącej **Załącznik nr 7** do Polityki.

Zabezpieczenie danych osobowych

§ 14.

1. Administrator stosuje zabezpieczenia danych osobowych dostosowane do aktualnego stopnia ryzyka.
2. Wykaz obszarów przetwarzania danych wraz ze wskazaniem ich fizycznych zabezpieczeń znajduje się w **Załączniku nr 8** do Polityki. Załącznik nr 8 ma charakter poufny i może być ujawniany jedynie organowi nadzorczemu lub w innych przypadkach na podstawie przepisów prawa.

Rozdział V Prowadzenie rejestrów przetwarzania danych osobowych

Rejestr czynności przetwarzania

§ 15.

1. Firma prowadzi rejestr czynności przetwarzania danych osobowych zgodnie z wymaganiami art. 30 ust. 1 RODO, w stosunku do danych których Firma jest Administratorem.
2. Rejestr czynności stanowi **Załącznik nr 9** do niniejszej Polityki.
3. Za prowadzenie rejestru czynności odpowiedzialny jest Inspektor.

Procesy przetwarzania

§ 16.

1. Inspektor inwentaryzuje procesy przetwarzania danych osobowych w Firmie, przypisując do nich określone czynności przetwarzania danych, ściśle współpracując z Administratorem.
2. Inspektor okresowo dokonuje przeglądów procesów przetwarzania danych w celach aktualizacji prowadzonych rejestrów.
3. Kierownicy komórek organizacyjnych mają obowiązek na bieżąco informować Inspektora o procesach przetwarzania danych osobowych realizowanych w swoich komórkach organizacyjnych oraz o wszelkich zmianach w tych procesach, w szczególności dotyczących:
   a) celów przetwarzania danych, w tym realizowanych czynności;
   b) kategorii osób, których dane są przetwarzane;
   c) zakresów przetwarzanych danych;
   d) podmiotów przetwarzających, którym dane są powierzane;
   e) odbiorców danych, którym dane są udostępniane.

Rejestr kategorii czynności przetwarzania

§ 17.

1. Firma prowadzi rejestr kategorii czynności przetwarzania zgodnie z wymaganiami art. 30 ust. 2 RODO, w stosunku do danych których Firma jest podmiotem przetwarzającym.
2. Rejestr kategorii czynności stanowi **Załącznik nr 10** do niniejszej Polityki.

Rozdział VI Realizacja obowiązków przy przetwarzaniu danych osobowych

Przetwarzanie danych na podstawie zgody

§ 18.

1. Osoby odpowiedzialne w Firmie za procesy, w których zbierane są dane osobowe, mają obowiązek zachowania szczególnej staranności przy ich zbieraniu, w tym:
   a) sprawdzać czy są spełnione podstawy prawne na pozyskiwanie danych osobowych, zgodnie z art. 6 RODO oraz art. 9 – 10 RODO;
   b) zbierać dane osobowe dla określonych, zgodnych z prawem celów realizowanych w Firmie;
   c) zbierać dane w zakresie adekwatnym do celów, w jakich dane będą przetwarzane w Firmie.
2. W przypadku konieczności odbierania zgody na przetwarzanie danych osobowych, należy zapewnić dobrowolność jej pozyskania oraz powiadamiać o prawie do odwołania takiej zgody.
3. Za stosowanie właściwych oświadczeń zgody przy zbieraniu danych osobowych odpowiada kierownik komórki organizacyjnej odpowiedzialnej za proces zbierania danych.
4. Oświadczenia dotyczące odbierania zgody na przetwarzanie danych osobowych muszą być konsultowane z Inspektorem.
5. Inspektor może ustalić obowiązujące wzory oświadczeń zgody dla poszczególnych procesów przetwarzania danych realizowanych w Firmie.

Przetwarzanie danych na podstawie uzasadnionego interesu

§ 19.

1. Administrator uprawniony jest do przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, z wyjątkiem sytuacji, w których nadrzędny charakter wobec interesów Administratora lub strony trzeciej

mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.

2. Procedura testu równowagi interesów stanowi **Załącznik nr 11** do niniejszej Polityki.

3. Administrator uznaje, iż przetwarzanie danych osobowych na podstawie uzasadnionego interesu w zakresie wskazanym w Rejestrze czynności jest dopuszczalne i akceptowalne, bez istotnego negatywnego wpływu dla danych osób, których przetwarzanie dotyczy.

Realizacja obowiązku informacyjnego

§ 20.

1. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych, są odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO.

2. Za stosowanie właściwych klauzul informacyjnych przy zbieraniu danych osobowych odpowiada kierownik komórki organizacyjnej odpowiedzialnej za proces zbierania danych.

3. Klauzule informacyjne muszą być konsultowane z Inspektorem.

4. Inspektor może ustalić obowiązujące wzory klauzul informacyjnych dla poszczególnych procesów przetwarzania danych realizowanych w Firmie.

Rozdział VII Czasowe ograniczenie przetwarzania danych

Retencja danych

§ 21.

1. Dane osobowe zbierane w ramach procesów realizowanych w Firmie są przetwarzane przez czas określony przez właściwe przepisy prawa lub ustalony przez Administratora przy zachowaniu zasad ochrony danych osobowych. Aktualne okresy retencji zawiera **Załącznik nr 12** do niniejszej Polityki.

2. Za określenie odpowiednich czasów retencji danych osobowych w procesach przetwarzania danych w Firmie odpowiada Inspektor. Określenie czasów retencji wymaga ściślej współpracy z Administratorem oraz upoważnionymi osobami.

3. Dane osobowe, dla których okres przetwarzania nie wynika z obowiązujących przepisów prawa, są przetwarzane tak długo, jak długo

istnieje jednocześnie podstawa prawna oraz niezbędny cel dla ich przetwarzania.

4. Ustanie celu przetwarzania danych jest równoznaczne z koniecznością zaprzestania przetwarzania danych osobowych.

5. Dane osobowe przetwarzane wyłącznie w oparciu o przesłankę zgody na przetwarzanie danych osobowych są usuwane zawsze niezwłocznie po wycofaniu takiej zgody.

6. W każdej komórce organizacyjnej Firmy odpowiedzialnej za określony proces lub procesy przetwarzania danych osobowych, co najmniej jeden raz w każdym roku kalendarzowym – w pierwszym kwartale danego roku - odbywa się weryfikacja zasobów danych osobowych prowadzonych w formie papierowej jak i elektronicznej, obejmująca:

   a) sprawdzenie, czy dane osobowe, dla których upłynął okres przechowywania wynikający z przepisów prawa lub wewnętrznych przepisów Firmy zostały usunięte;

   b) sprawdzenie, czy w odniesieniu do danych osobowych, których czas przechowywania nie został określony przez właściwe przepisy prawa lub wewnętrzne przepisy Firmy, nadal istnieje podstawa prawna oraz niezbędny cel przetwarzania danych osobowych.

7. W przypadku ustalenia w trakcie weryfikacji, o której mowa w ust. 6, że okres przetwarzania danych osobowych upłynął bądź nie istnieje podstawa prawna lub cel do dalszego przetwarzania danych osobowych, dane osobowe powinny zostać trwale usunięte z nośników papierowych, elektronicznych oraz systemów informatycznych.

Rozdział VIII Zasady udostępniania danych osobowych

Powierzenie danych przez Administratora

§ 22.

1. Administrator może powierzyć innemu podmiotowi przetwarzanie danych osobowych jedynie w drodze umowy lub innego instrumentu prawnego. Podmiot, któremu zostały powierzone dane, może przetwarzać dane wyłącznie w określonym celu i zakresie. Każdy przypadek powierzenia danych osobowych jest rejestrowany w rejestrze powierzeń stanowiącym **Załącznik nr 13** do Polityki.

2. Umowa powierzenia przetwarzania danych osobowych może zostać zawarta jedynie z podmiotem, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by

przetwarzanie spełniało wymogi przepisów RODO i chroniło prawa osób, których dane dotyczą.

3. Za zapewnienie odpowiednich gwarancji, o których mowa w ust. 2, uznaje się w szczególności, choć nie wyłącznie:

   a) zapewnienie Administratorowi w umowie powierzenia przetwarzania danych realnego prawa do prowadzenia audytów i kontroli procesora w zakresie odnoszącym się do przedmiotu umowy, jak również gwarancji współpracy w zakresie realizacji obowiązków wynikających z RODO;

   b) legitymowanie się procesora certyfikatem potwierdzającym wypełnienie wymogów norm ISO z zakresu ochrony danych osobowych, w tym bezpieczeństwa teleinformatycznego;

   c) przestrzeganie przez procesora branżowego kodeksu dobrych praktyk zatwierdzonego przez organ nadzorczy;

   d) legitymowanie się procesora certyfikatem uzyskanym w ramach mechanizmu certyfikacji, o jakim mowa w RODO i UODO.

4. Umowa powierzenia może zostać zawarta również w formie elektronicznej.

5. Kontrola podmiotów przetwarzających, którym zostały powierzone czynności przetwarzania danych osobowych należących do Firmy, jest przeprowadzana przez Inspektora lub inne wyznaczone osoby zgodnie z zapisami zawartymi w umowach powierzenia przetwarzania danych osobowych, w odniesieniu do uprawnienia określonego w art. 28 ust. 3 lit. h RODO.

6. Administrator przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym jest zobowiązany poinformować o tym Inspektora oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych.

Przetwarzanie danych jako podmiot przetwarzający

§ 23.

Administrator w zakresie prowadzonej przez siebie działalności może przetwarzać dane osobowe jako podmiot przetwarzający, z zastrzeżeniem iż takie przetwarzanie nie jest prowadzone na dzień wejścia w życie Polityki.

Przekazanie danych

§ 24.

1. Osoby, które udostępniają w imieniu Firmy dane osobowe do podmiotu zewnętrznego (w formie papierowej lub elektronicznej), przed ich udostępnieniem mają obowiązek sprawdzić czy istnieją podstawy prawne umożliwiające wykonanie tych czynności, w tym:
   a) wymóg prawa dotyczący udostępnienia danych;
   b) zgoda osoby na udostępnienie danych innemu podmiotowi;
   c) zapis w umowie z podmiotem współpracującym, przy spełnieniu warunku, że udostępnienie nie narusza praw i wolności osoby, której dane dotyczą;
   d) wniosek o udostępnienie danych od podmiotu uprawnionego, ze wskazaniem podstawy prawnej do otrzymywania danego rodzaju danych osobowych.
2. W razie powtarzającego się i niestandardowego udostępniania danych należy odnotowywać każde jednostkowe udostępnienie w rejestrze udostępnień zawierającym co najmniej podstawę prawną udostępnienia (zgoda, umowa, uzasadniony interes, przepis prawa), rodzaj udostępnianych danych, wskazanego odbiorcę danych.
3. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO albo na podstawie innych przepisów prawa.

Przekazanie danych do państwa trzeciego

§ 25.

Administrator może przekazywać dane osobowe do podmiotów znajdujących się w państwie trzecim (poza Europejski Obszar Gospodarczy), jednak może to nastąpić wyłącznie przy zachowaniu zgodności z wymogami RODO.

Rozdział IX Realizacja praw osób, których dane dotyczą

Prawa podmiotów danych

§ 26.

1. Każdej osobie, której dane osobowe są przetwarzane przez Firmę przysługują prawa określone w art. 15 – 22 RODO, w tym:

a) prawo dostępu do danych jej dotyczących;

b) prawo do sprostowania danych;

c) prawo do usunięcia danych;

d) prawo do ograniczenia przetwarzania;

e) prawo do przenoszenia danych;

f) prawo do sprzeciwu na przetwarzanie jej danych;

g) prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu.

2. Za rozpatrywanie złożonych do Firmy żądań w zakresie uprawnień, o których mowa w ust. 1, odpowiada Inspektor lub inna osoba wskazana przez Administratora.

3. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą.

4. Procedura realizacji praw osób, których dane dotyczą, stanowi **Załącznik nr 14a** do Polityki. Każdy wniosek winien zostać odnotowany w ewidencji prowadzonej według wzoru stanowiącego **Załącznik nr 14b** do Polityki.

Rozdział X Postępowanie w sytuacji naruszenia ochrony danych

Obowiązek poinformowania o naruszeniu

§ 27.

1. Każda osoba, która powzięła wiedzę, niezależnie od źródła pochodzenia, o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych, zobowiązana jest do niezwłocznego poinformowania o powyższym Administratora oraz Inspektora ochrony danych.

2. Inspektor zobowiązany jest do oszacowania ryzyka i zarekomendowania Administratorowi, przy współpracy ASI, sposobu postępowania w zakresie koniecznych do podjęcia środków bezpieczeństwa, rozważenia zgłoszenia naruszenia organowi nadzorczemu oraz zawiadomienia osób, których dane dotyczą.

Zgłoszenie naruszenia do organu nadzorczego

§ 28.

1. W sytuacji stwierdzenia wystąpienia naruszenia ochrony danych osobowych oraz prawdopodobieństwa zaistnienia ryzyka naruszenia praw lub wolności osób fizycznych, informacja o naruszeniu powinna zostać zgłoszona do PUODO. W sytuacjach wątpliwych lub niejednoznacznych należy dokonać zgłoszenia do PUODO.
2. Zgłoszenie naruszenia przygotowuje Inspektor przy współpracy z Administratorem oraz, gdy jest to wskazane, ASI, i dokonuje w terminie 72 godzin po stwierdzeniu naruszenia, zgodnie z wymaganiami art. 33 RODO.
3. W przypadku gdy naruszenie ochrony danych odnosi się do procesów przetwarzania realizowanych przez Firmę w roli podmiotu przetwarzającego, Organizacja zobowiązana jest do podjęcia adekwatnych środków zaradczych oraz do niezwłocznego poinformowania administratora powierzonych danych.

Zawiadomienie osób, których dane dotyczą

§ 29.

W sytuacji gdy stwierdzone naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o naruszeniu należy zawiadomić wszystkie osoby, których dane dotyczą. Inspektor analizuje czy w odniesieniu do wymogów art. 34 ust. 3 RODO zawiadomienie osób, których dane dotyczą, będzie wymagane. Wysokie ryzyko występuje, jeśli proces szacowania wagi naruszenia, o którym mowa w § 30 ust. 3 Polityki, wykazał wagę inną niż niską i średnią.

Procedury oraz ewidencje naruszeń

§ 30.

1. Szczegółowa procedura regulująca proces naruszeń ochrony danych stanowi **Załącznik nr 15** do Polityki.
2. Każde stwierdzone naruszenie ochrony danych osobowych, niezależnie do tego, czy jest zgłaszane do organu nadzorczego czy też nie, jest dokumentowane przez Inspektora. Wzór ewidencji naruszeń ochrony danych osobowych stanowi **Załącznik nr 16** do Polityki.
3. Weryfikacja konieczności zawiadamiania osób, których dane dotyczą, wymaga przeprowadzenia szacowania wagi naruszenia według schematu opisanego w **Załączniku nr 17** do Polityki.

Rozdział XI Rozliczalność zgodności realizacji obowiązków RODO

Monitorowanie przestrzegania przepisów

§ 31.

1. W celu weryfikacji zastosowanych w Firmie środków technicznych i organizacyjnych, zapewniających przetwarzanie danych osobowych zgodnie z RODO, wykonuje się ich monitorowanie.
2. Monitorowanie ochrony danych osobowych prowadzone jest:
   a) na bieżąco przez kierowników KO, w których przetwarzane są dane osobowe;
   b) poprzez audyty okresowe i doraźne (w sytuacji wystąpienia incydentów naruszenia ochrony danych) wykonywane przez Inspektora;
   c) podczas audytów wewnętrznych przeprowadzanych przez upoważnione podmioty.
3. Inspektor okresowo analizuje zgodność dokumentacji przetwarzania danych osobowych przyjętej w Firmie z przepisami o ochronie danych osobowych, aktualnym orzecznictwem, jak również z wytycznymi krajowego organu nadzorczego lub Europejskiej Rady Ochrony Danych oraz rekomenduje jej aktualizację.

Rozdział XII Skutki naruszenia regulacji ochrony danych osobowych

Odpowiedzialność za naruszenie ochrony danych

§ 32.

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w art. 107 – 108 UODO oraz w art. 130, 266 - 269, 287 Kodeksu karnego. Treść przepisów stanowi **Załącznik nr 18** do Polityki.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością na podstawie przepisów prawa pracy (dotyczy osób zatrudnionych na podstawie umowy o pracę).

Rozdział XIII Postanowienia końcowe

§ 33.

1. Polityka wraz z Załącznikami jest dokumentem wewnętrznym, stanowiącym tajemnicę przedsiębiorstwa, i nie może być udostępniana osobom nieupoważnionym w żadnej formie, chyba że obowiązek jej udostępnienia ma charakter prawny.
2. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO, UODO oraz odpowiednich ustaw sektorowych.
3. Polityka wchodzi w życie z dniem 30.04.2019.
4. Administrator informuje o zmianie Polityki z wyprzedzeniem nie krótszym niż 7 dni przed planowanym wejściem w życie, chyba że względy bezpieczeństwa przemawiają za wprowadzeniem zmian w trybie natychmiastowym.
5. Zmiana Załączników wchodzi w życie z chwilą poinformowania osób upoważnionych, z zastrzeżeniem wejścia w życie Załączników mających charakter niejawny z chwilą ich sporządzenia.
6. **Załącznik nr 8 pozostaje niejawny i może być ujawniony jedynie upoważnionym organom**.

Część II Procedury dotyczące bezpieczeństwa systemów informatycznych

Rozdział I Dostęp do systemów informatycznych

Odnotowywanie udostępnienia danych

§ 1.

1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
   1) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   2) operacje wykonywane na przetwarzanych danych,
   3) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom niebędącym właścicielem ani współwłaścicielem systemu,
   4) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   5) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
2. Każda operacja dokonywana w systemie zostaje opatrzona datą oraz nazwą użytkownika wprowadzającego dane oraz adresem IP komputera.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy

§ 2.

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe dokonując logowania z użyciem identyfikatora i hasła. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabrania się pracy wielu użytkowników na wspólnym koncie.
2. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, zostaje niezwłocznie wyrejestrowany z systemu

informatycznego, w którym są przetwarzane, zaś hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

3. Użytkownik jest zobowiązany do powiadomienia ASI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.

4. W przypadku gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.

5. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerów.

6. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 3 minut system automatycznie powinien aktywować wygaszacz.

7. Po zakończeniu pracy użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy, zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

Zarządzanie uprawnieniami użytkowników

§ 3.

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych.

2. Po nadaniu upoważnienia Administrator przekazuje go ASI celem nadania identyfikatora oraz uprawnień użytkownika w systemach informatycznych i aplikacjach.

3. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login).

4. Osoba upoważniona do przetwarzania danych osobowych pracuje w systemie operacyjnym stacji roboczej z poziomu dostępu użytkownika a nie administratora.

5. Za rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym odpowiada Administrator.

6. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku nieobecności pracownika w

pracy trwającej dłużej niż 21 dni kalendarzowych lub w przypadku uzasadnionego podejrzenia zawinionego naruszenia ochrony danych.

7. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje Administrator systemu na wniosek Administratora danych, z podaniem daty oraz przyczyny odebrania uprawnień.

Rozdział II Metody i środki uwierzytelnienia

Ogólne zasady postępowania z hasłami

§ 4.

1. ASI informuje użytkownika o nadaniu pierwszego hasła do stacji roboczej.
2. Użytkownik zobowiązany jest do niezwłocznej zmiany otrzymanego hasła do stacji roboczej.
3. Hasła nie mogą być powszechnie używanymi słowami, w szczególności nie należy jako haseł wykorzystywać dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów, nazw miesięcy.
4. Niedopuszczalne jest stosowanie identycznych lub podobnych haseł zarówno do urządzeń i aplikacji prywatnych, jak i służbowych.
5. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
6. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
7. Rekomendowane jest przechowywanie haseł przy wykorzystywaniu menadżera haseł, do którego użytkownik ustanowi mocniejsze hasło.
8. Wszelkie hasła przekazywane są pracownikom w formie zabezpieczonej przed dostępem osób trzecich.

Hasła użytkowników do stacji roboczych

§ 5.

1. Hasło do stacji roboczych mają długość przynajmniej 8 znaków – składają się z wielkich i małych liter oraz cyfr lub znaków specjalnych.
2. System stacji roboczej powinien wymuszać zmianę hasła nie rzadziej niż co 90 dni.

Hasła do serwera/sieci

§ 6.

1. Hasło dostępu do serwera/sieci składa się z co najmniej 11 znaków.
2. Hasło składa się z wielkich i małych liter oraz z cyfr.
3. Zmiana hasła odbywa się raz na 90 dni.

Hasła administratora

§ 7.

1. Hasło administratora składa się z co najmniej 10 znaków.
2. Hasło składa się z wielkich i małych liter oraz cyfr lub znaków specjalnych.
3. Hasło powinno być znane tylko administratorowi oraz osobie uprawnionej do reprezentowania Firmy.
4. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
5. W przypadkach awaryjnych hasło może być przekazane decyzją Administratora osobie zastępującej administratora.
6. Po ustaniu sytuacji awaryjnej Administrator jest zobowiązany do zmiany hasła.

Rozdział III Procedura tworzenia kopii zapasowych

Tworzenie kopii bezpieczeństwa dokumentacji serwera

§ 8.

1. Administrator posiada własny serwer zlokalizowany na pierwszym piętrze budynku, w którym znajduje się siedziba Firmy. Serwerownia jest odrębnie zamkniętym pomieszczeniem, do którego dostęp ma ASI oraz inne upoważnione osoby.
2. W serwerze skonfigurowana jest macierz dyskowa (RAID). Serwer zabezpieczony jest dodatkowo zasilaczem UPS.
3. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

Pozostałe kopie bezpieczeństwa

§ 9.

1. Kopia zapasowa danych zapisanych na dyskach lokalnych krytycznych stacji roboczych jest sporządzana automatycznie raz na tydzień i obejmuje takie dane jak dane z poczty firmowej oraz baza danych programu Handlowo-Kadrowo-Płacowego. Kopie danych są wysyłane do zewnętrznego dostawcy usługi chmury po ich uprzednim zaszyfrowaniu. Usunięcie kopii zapasowej może nastąpić po roku od jej stworzenia.

Rozdział IV Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

Zabezpieczenie elektronicznych nośników informacji

§ 10.

1. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Dane osobowe wynoszone poza obszar przetwarzania na przenośnych nośnikach muszą być zaszyfrowane.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe uszkadza się w sposób mechaniczny uniemożliwiając ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
5. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych bez ich uprzedniego zaszyfrowania.
6. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do ich sprawdzenia programem antywirusowym na swoim komputerze.
7. Nośniki magnetyczne z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności – przechowywane w miejscach chronionych przed dostępem nieuprawnionych osób, a po ich

wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

Rozdział V Procedura zabezpieczenia systemu informatycznego

Ochrona antywirusowa

§ 11.

1. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym zapewnienie odpowiedniej ilości licencji dla użytkowników.
2. System antywirusowy zainstalowany jest na stacjach roboczych.
3. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików oraz poczty wychodzącej i przychodzącej.
4. Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.
5. Użytkownicy zapewniają stałą aktywność programu antywirusowego – program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
6. Aktualizacja definicji wirusów odbywa się automatycznie przez system.
7. W przypadku stwierdzenia pojawienia się wirusa lub innego podobnego zagrożenia każdy użytkownik zobowiązany jest do powiadomienia o powyższym ASI.
8. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora (ciągła praca w tle).
9. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.
10. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
11. Jeżeli oprogramowanie antywirusowe pozwala, to należy ustawić harmonogram zadań tak, aby raz w tygodniu lub więcej razy sprawdzał daną jednostkę komputerową pod kątem obecności wirusów.
12. Do obowiązków Administratora systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.

13. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
14. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
15. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
16. Kontrola antywirusowa przeprowadzana jest na wybranym komputerze w przypadku stwierdzenia nieprawidłowości zgłoszonych przez pracownika w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
17. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirus oraz wszystkie posiadane przez użytkownika nośniki.
18. Użytkownik jest obowiązany zawiadomić Administratora systemu o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
19. Użytkownicy mogą podłączać zewnętrzne nośniki danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

§ 12.

1. Sieć bezprzewodową zabezpieczono technologią WPA2.
2. Administrator może wprowadzić mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Mogą one uwzględniać: blokowanie stron internetowych określonego typu, blokowanie określonych stron internetowych, analizę przesłanych informacji pod kątem niebezpiecznego oprogramowania.
3. Administrator stosuje system IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, który po 5 krotnej próbie uzyskania dostępu blokuje adres IP atakującego.

Zabezpieczenie infrastruktury informatycznej i telekomunikacyjnej

§ 13.

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar Organizacji, na których są przetwarzane dane osobowe, są zobowiązani do

przestrzegania zasad bezpieczeństwa opisanych w Regulaminie użytkowania komputerów przenośnych stanowiącego **Załącznik nr 19**.

2. W przypadku dostępu do danych osobowych przez Internet do środków teletransmisji wymagane jest uwierzytelnienie (podanie loginu i hasła).
3. Dostęp do stacji roboczych lub systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użycie systemów informatycznych.

Zabezpieczenie programów i baz przetwarzających dane osobowe

§ 14.

1. Dostęp do danych osobowych w programie lub bazie wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano mechanizm blokady dostępu po 3 próbach nieudanego logowania się.
3. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
4. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.
5. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
6. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
7. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

Aktualizacja oprogramowania

§ 15.

1. ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service packi, łatki).
2. Administrator odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

Rozdział VI Procedura wykonywania napraw i konserwacji

§ 16.

1. ASI odpowiada za bezawaryjną pracę systemu IT, w tym stacji roboczych, aplikacji serwerowych, baz danych.
2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej niż raz w roku.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
5. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
6. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego winny być wykonywane przez osobę upoważnioną.
7. Przed rozpoczęciem czynności konserwacyjnych i naprawczych dane i programy znajdujące się w systemie winny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą.
8. W razie gdy wykonywanie prac konserwacyjnych i naprawczych nie może zostać zrealizowane wewnątrz Organizacji, należy skorzystać z usług podmiotu zewnętrznego. Skorzystanie z usług podmiotu zewnętrznego wymaga uprzedniego zawarcia z nim umowy o zachowaniu poufności zawierającej karę umowną na wypadek jej naruszenia.
9. O ile to możliwe, czynności konserwacyjne i naprawcze wykonywane przez podmioty zewnętrzne powinny być wykonywane na terenie Organizacji pod ścisłym nadzorem osoby upoważnionej.

10. W przypadku zaistnienia konieczności przekazania uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren Organizacji należy: wymontować nośniki z danymi osobowymi, trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania bądź nadzorować proces naprawy przez osobę upoważnioną, gdy nie ma możliwości usunięcia danych z nośnika.

11. Realizacja prac konserwacyjnych i naprawczych przez podmioty zewnętrzne winna być ewidencjonowana w książce zawierającej rodzaj wykonywanych czynności, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących tych czynności z imienia i nazwiska.

Rozdział VII Procedury korzystania z komunikacji elektronicznej

Procedura korzystania z Internetu

§ 17.

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy stacji roboczej oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła.

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo.

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą „https”.

Procedura korzystania z poczty elektronicznej

§ 18.

1. W związku z licznymi zagrożeniami wynikającymi z korzystania z poczty elektronicznej, wprowadza się całkowity zakaz korzystania z prywatnej skrzynki pocztowej na komputerach przetwarzających dane osobowe oraz komputerach działających w nich w jednej podsieci.

2. Do działania dopuszcza się wyłącznie skrzynki pocztowe utworzone lub zaakceptowane do wykorzystywania przez Administratora.

3. Skrzynka pocztowa powinna być wykorzystywana wyłącznie na komputerach bezpiecznych i chronionych przed wirusami. W związku z tym sugeruje się wykorzystywanie skrzynki poza Firmą lub na urządzeniach innych niż służbowe tylko w sytuacjach nagłych i niezbędnych.

4. Hasło do skrzynki pocztowej powinno być traktowane z należytą starannością, tak jak inne hasła, zgodnie z ustalonymi politykami jakości hasła.

5. Z uwagi na masowe ataki niebezpiecznego oprogramowania prowadzone z użyciem poczty elektronicznej, uruchamianie załączników przesyłanych tą drogą, niezależnie od formatu pliku, musi być poprzedzone następującymi działaniami:

   a) należy zastanowić się, czy z danym nadawcą wiążą Firmę jakiekolwiek związki wymagające przesyłania plików;

   b) należy zastanowić się, czy dany nadawca ma powód do przesłania takiego pliku;

   c) należy zastanowić się, czy treść wiadomości nie odbiega od zazwyczaj stosowanej, czy nie zawiera błędów stylistycznych i językowych.

6. W przypadku gdy wiadomość elektroniczna zawiera odsyłacze (linki) do wskazanych stron w Internecie, użytkownik przed ich kliknięciem jest zobowiązany przeprowadzić następującą analizę:

   a) należy zastanowić się, czy z danym nadawcą wiążą Firmę jakiekolwiek związki wymagające przesyłania linków do kliknięcia;

   b) należy zastanowić się, czy dany nadawca ma powód do przesłania takiego odsyłacza;

   c) należy zastanowić się, czy treść listu nie odbiega od zazwyczaj stosowanej, czy nie zawiera błędów stylistycznych i językowych;

   d) należy rozważyć, czy nie jest możliwe wejście na wskazany adres poprzez jego wpisanie ręczne w oknie przeglądarki internetowej;

   e) jeżeli po wejściu pod podany adres wymagane jest podanie danych uwierzytelniających należy rozważyć, czy aby na pewno strona nie służy do wyłudzania tych danych.

7. Jeżeli na którymkolwiek etapie powyższych procedur pojawią się wątpliwości, należy natychmiast przerwać korzystanie z poczty i skonsultować wątpliwości z ASI, Administratorem lub Inspektorem.

8. W przypadku wysyłania wiadomości zawierających dane osobowe w małych ilościach (faktury, pojedyncze formularze), skierowanych bezpośrednio do osoby, której dane dotyczą, dopuszczalne jest wysyłanie wiadomości niezaszyfrowanej.

9. W przypadku wysyłania wiadomości zawierających większą ilość danych osobowych lub zawierających dane szczególnej kategorii (dane wrażliwe), należy przeprowadzić proces szyfrowania opisany poniżej.

10. Niezależnie od rodzaju wysyłanej wiadomości, należy upewnić się, że wpisywany adres odbiorcy jest poprawny i nie pojawiło się w nim jakieś przekłamanie, które może spowodować, że dane trafią do zupełnie innego odbiorcy.

11. Jeżeli dane zawarte są w pojedynczych plikach pakietu biurowego MS Office (Word, Excel) lub LibreOffice/OpenOffice (Writer, Calc) można wybrać metodę zapisania pliku z hasłem szyfrującym.

12. Jeżeli dane zawarte są w większej liczbie plików lub są to pliki z programów nieposiadających opcji szyfrowania, należy pliki z danymi zaszyfrować wykorzystując zabezpieczone hasłem archiwum ZIP lub podobne. Można tu wykorzystać darmowy program 7-zip udostępniający tworzenie szyfrowanych archiwów 7z oraz ZIP (dostępny również dla osób nieposiadających programu 7-zip).

13. Hasło szyfrujące należy przekazać odbiorcy w inny sposób niż poprzez e-mail. Można je podać telefonicznie albo via SMS.

14. Hasło szyfrujące należy dobrać zgodnie z zasadami doboru dobrej jakości hasła, a do tego powinno być ono inne niż hasła stosowane przy wysyłce danych do innych odbiorców.

15. Jeżeli wysyłanie danych pomiędzy dwoma odbiorcami odbywa się często i proces szyfrowania i zarządzania hasłami staje się kłopotliwy, ASI wdraża na wniosek pracownika metody szyfrowania asymetrycznego, takie jak GPG czy SMIME, oraz szkoli obie strony z wykorzystania tej metody. W procesie szyfrowania asymetrycznego nie jest już konieczne ustanawianie haseł i przekazywanie ich innym kanałem, gdyż opiera się na zasadzie wykorzystania kluczy prywatnych i publicznych.

16. Dane osobowe wysyłane i odbierane pocztą elektroniczną trafiają do folderów (wysłane, odebrane itp.) w programie pocztowym lub na serwerze obsługującym skrzynkę.

17. Jeżeli system obsługi skrzynki lub program pocztowy nie pozwala na automatyzację czyszczenia zawartości, ADO zobowiązuje pracownika do ręcznego usuwania przynajmniej raz w miesiącu wiadomości przechowywanych dłużej niż wskazane okresy.
18. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy wiadomości.
19. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
20. Nie należy otwierać załączników (plików) w e-mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
21. Użytkownicy nie powinni rozsyłać za pośrednictwem e-maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp.
22. Użytkownicy nie powinni rozsyłać e-maili zawierających załączniki o dużym rozmiarze.
23. Podczas wysyłania e-maili do wielu adresatów jednocześnie należy użyć metody „ukryte wiadomości – UDW".
24. Użytkownik zobowiązany jest do umieszczenia w stopce e-maila informacji o poufnym charakterze wiadomości, konieczności usunięcia otrzymanej wiadomości, w przypadku gdy wiadomość ta dotarła do błędnego odbiorcy.

Załączniki:

1. Oświadczenie o zachowaniu poufności danych wraz z informacją o naruszeniu danych.
2. Upoważnienie do przetwarzania danych.

3a. Ewidencja osób upoważnionych do przetwarzania danych.

3b. Ewidencja przydziału kluczy.

3. Raport weryfikujący obowiązek wyznaczenia inspektora.
4. Obowiązki osób upoważnionych.

6a. Procedura określająca zasady szacowania ryzyka.

6b. Arkusz analizy ryzyka.

7. Ocena skutków dla ochrony danych.
8. Obszary przetwarzania danych wraz z ich fizycznym zabezpieczeniem /załącznik niejawny/.
9. Rejestr czynności przetwarzania.
10. Rejestr kategorii czynności.
11. Procedura testu równowagi na podstawie art. 6 ust. 1 lit. f) RODO.
12. Okresy retencji danych.
13. Rejestr powierzeń.

14a. Procedura rozpatrywania wniosków praw osób, których dane dotyczą.

14b. Ewidencja wniosków praw osób których dane dotyczą.

15. Procedura naruszeń ochrony danych.
16. Ewidencja naruszeń ochrony danych.
17. Algorytm wagi naruszenia.
18. Wyciąg z przepisów.
19. Regulamin korzystania z komputerów przenośnych.