POLITYKA OCHRONY DANYCH OSOBOWYCH

Administrator:
Lobo Sp. z o.o. Sp.k. z siedzibą w Gdyni
przy ul. Stefana Batorego 23 lok. 7, 81-365 Gdynia
NIP 9512334022, REGON 142843056

Data ostatniej aktualizacji: 25 maja 2018 r.

Spis treści

1. Informacje wstępne ... 3
   A. Definicje ... 3
   B. Cel utworzenia Polityki Ochrony Danych Osobowych ... 4
   C. Zakres stosowania Polityki Ochrony Danych Osobowych ... 4
2. Zasady przetwarzania danych osobowych ... 4
   A. Podstawowe zasady przetwarzania danych osobowych ... 4
   B. Podstawy przetwarzania danych osobowych ... 5
   C. Stosowanie zasady „privacy by design" ... 6
   D. Stosowanie zasady „privacy by default" ... 6
   E. Rejestrowanie czynności przetwarzania ... 6
   F. Powierzenie przetwarzania danych osobowych ... 7
3. Bezpieczeństwo danych osobowych ... 7
   A. Dostęp do danych osobowych przetwarzanych przez Administratora ... 7
   B. Administrator Systemów Informatycznych ... 8
   C. Naczelne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych ... 9
   D. Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych ... 9
   E. Szczególne dodatkowe środki dotyczące zabezpieczenia danych osobowych na urządzeniach przenośnych i nośnikach danych ... 11
4. Inspektor ochrony danych ... 12
5. Postępowanie w przypadku naruszenia ochrony danych osobowych ... 12
   A. Postępowanie wewnętrzne ... 12
   B. Postępowanie zewnętrzne ... 14
6. Aktualność środków ochrony danych osobowych ... 15
7. Postanowienia końcowe ... 16

1. Informacje wstępne

A. Definicje

1.1. Na użytek Polityki Ochrony Danych Osobowych:

a) „**Administrator**" oznacza Lobo Spółkę z ograniczoną odpowiedzialnością spółkę komandytową z siedzibą w Gdyni, ul. Stefana Batorego 23/7, 81-365 Gdynia, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000379784, NIP: 9512334022, REGON: 142843056,

b) „**Administrator Systemów Informatycznych**" oznacza działającą z upoważnienia Administratora osobę, która zarządza systemem informatycznym Administratora i sprawuje nad nim nadzór,

c) „**hasło**" oznacza ciąg znaków literowych, cyfrowych lub innych, znany wyłącznie Administratorowi Systemów Informatycznych oraz użytkownikowi,

d) „**identyfikator użytkownika**" oznacza ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika w systemie informatycznym Administratora,

e) „**organ nadzorczy**" oznacza Prezesa Urzędu Ochrony Danych Osobowych,

f) „**Polityka Ochrony Danych Osobowych**" oznacza niniejszy dokument,

g) „**RODO**" oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1),

h) „**system informatyczny**" oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

i) „**uwierzytelnianie**" oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

j) „**użytkownik**" oznacza osobę uprawnioną do pracy w systemie informatycznym Administratora.

1.2. Na użytek Polityki Ochrony Danych Osobowych stosuje się ponadto definicje określone w RODO, o ile nie są one sprzeczne z definicjami zawartymi w punkcie 1.1 powyżej.

B. Cel utworzenia Polityki Ochrony Danych Osobowych

1.3. Polityka Ochrony Danych Osobowych jest środkiem wdrożonym przez Administratora zgodnie z art. 24 ust. 1 i 2 RODO, którego celem jest wprowadzenie w przedsiębiorstwie prowadzonym przez Administratora procedury postępowania z danymi osobowymi, w oparciu o którą ich przetwarzanie będzie się odbywać zgodnie z RODO i która pozwoli to wykazać.

1.4. Polityka Ochrony Danych Osobowych określa w szczególności, jakie inne środki techniczne i organizacyjne zostały w tym celu wdrożone przez Administratora przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

C. Zakres stosowania Polityki Ochrony Danych Osobowych

1.5. Polityka Ochrony Danych Osobowych ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

1.6. Politykę Ochrony Danych Osobowych zobowiązana jest stosować każda osoba wchodząca w skład struktury organizacyjnej przedsiębiorstwa Administratora, niezależnie od rodzaju stosunku prawnego łączącego ją z Administratorem. W szczególności dotyczy to członków organów Administratora, pracowników, osób zatrudnionych na podstawie umowy cywilnoprawnej, stażystów i praktykantów.

2. Zasady przetwarzania danych osobowych

A. Podstawowe zasady przetwarzania danych osobowych

2.1. Administrator dochowuje wszelkich starań, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO, innymi powszechnie obowiązującymi przepisami prawa oraz dobrymi praktykami. W związku z tym dane osobowe bezwzględnie powinny być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,

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,

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.

2.2. Administrator nie dokonuje przetwarzania, które z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Rozpoczęcie takiego przetwarzania wymaga uprzedniego dokonania przez Administratora oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO.

B. Podstawy przetwarzania danych osobowych

2.3. Przetwarzanie danych osobowych przez Administratora może mieć miejsce wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,

b) 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,

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,

f) 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.

2.4. Podstawa przetwarzania, o którym mowa w punkcie 2.3 lit. c) i e) powyżej, musi być określona w prawie Unii lub prawie polskim. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w punkcie 2.3 lit. e) powyżej – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

C. Stosowanie zasady „privacy by design"

2.5. Administrator zapewnia stosowanie takich procedur wdrażania zmian, projektów lub inwestycji, które już w fazie projektowania zapewniają ocenę wpływu wdrażanego rozwiązania na ochronę danych osobowych.

2.6. Zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, Administrator wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

2.7. Wdrażając odpowiednie środki techniczne i organizacyjne, Administrator uwzględnia 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 wynikające z przetwarzania.

D. Stosowanie zasady „privacy by default"

2.8. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

E. Rejestrowanie czynności przetwarzania

2.9. Administrator prowadzi w formie elektronicznej rejestr czynności przetwarzania danych osobowych zgodny z wymogami art. 30 ust. 1 RODO.

2.10. Rejestr czynności przetwarzania danych osobowych jest narzędziem umożliwiającym Administratorowi realizację zasady rozliczalności i podlega udostępnieniu na żądanie organu nadzorczego.

F. Powierzenie przetwarzania danych osobowych

2.11. Administrator może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu wyłącznie na zasadach zgodnych z wymogami art. 28 RODO.

2.12. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach podmiotu przetwarzającego w zakresie zabezpieczania danych osobowych.

3. Bezpieczeństwo danych osobowych

A. Dostęp do danych osobowych przetwarzanych przez Administratora

3.1. Do przetwarzania danych osobowych dopuszcza się wyłącznie osoby posiadające wydane przez Administratora upoważnienie do przetwarzania danych osobowych zgodne ze wzorem stanowiącym załącznik **Błąd! Nie można odnaleźć źródła odwołania.** do Polityki Ochrony Danych Osobowych.

3.2. W upoważnieniu do przetwarzania danych osobowych Administrator precyzyjnie wskazuje czasowy i przedmiotowy zakres upoważnienia. Upoważnienie powinno zostać sporządzone w taki sposób, aby jego zakres nie nastręczał wątpliwości interpretacyjnych. W szczególności:

a) przedmiotowy zakres upoważnienia powinien jasno odwoływać się do czynności przetwarzania zamieszczonych i opisanych w rejestrze czynności przetwarzania danych osobowych, o którym mowa w punkcie 2.9 powyżej,

b) przedmiotowy zakres upoważnienia powinien zawierać wyjaśnienie, czy upoważnienie obejmuje przetwarzanie danych osobowych w systemie informatycznym, poza nim, czy obie te możliwości łącznie.

3.3. Każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie Administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

3.4. Przed przystąpieniem do przetwarzania danych osobowych każda osoba działająca z upoważnienia Administratora musi zostać zapoznana z Polityką Ochrony Danych

Osobowych i zobowiązać się do jej przestrzegania według wzoru stanowiącego załącznik **Błąd! Nie można odnaleźć źródła odwołania.** do Polityki Ochrony Danych Osobowych.

3.5. Administrator Systemów Informatycznych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik **Błąd! Nie można odnaleźć źródła odwołania.** do Polityki Ochrony Danych Osobowych. Podstawą wpisu do ewidencji może być wyłącznie dokument sporządzony przez Administratora.

B. Administrator Systemów Informatycznych

3.6. Administrator wyznacza Administratora Systemów Informatycznych zgodnie ze wzorem stanowiącym załącznik **Błąd! Nie można odnaleźć źródła odwołania.** do Polityki Ochrony Danych Osobowych.

3.7. Administrator zapewnia, że każda osoba zobowiązana do stosowania Polityki Ochrony Danych Osobowych posiada wiedzę o tym, kto pełni funkcję Administratora Systemów Informatycznych.

3.8. Do zadań Administratora Systemów Informatycznych należy zarządzanie systemem informatycznym Administratora i sprawowanie nad nim nadzoru, w tym:

a) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego,

b) przydzielanie identyfikatorów użytkowników i haseł do systemu informatycznego,

c) zapewnianie zgodności uprawnień użytkowników systemu informatycznego z ewidencją osób upoważnionych do przetwarzania danych osobowych,

d) nadzorowanie działania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

e) sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,

f) podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej transmisji danych za pośrednictwem sieci telekomunikacyjnej,

g) zapewnianie stosowania środków technicznych i organizacyjnych przewidzianych Polityką Ochrony Danych Osobowych oraz ocena ich odpowiedniości dla zapewniania bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

3.9. Administrator Systemów Informatycznych zobowiązany jest ponadto do wykonywania innych obowiązków określonych w Polityce Ochrony Danych Osobowych oraz poleceń Administratora.

C. Naczelne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

3.10. Każda osoba mająca dostęp do danych osobowych jest odpowiedzialna za ich bezpieczeństwo, w tym w szczególności przetwarzanie ich w sposób zgodny z Polityką Ochrony Danych Osobowych.

3.11. Osoby mające dostęp do danych osobowych nie mogą ich ujawniać lub wykorzystywać ani w miejscu pracy, ani poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych w ramach upoważnienia do przetwarzania danych osobowych udzielonego przez Administratora. Zakaz ten obowiązuje także po ustaniu stosunku prawnego łączącego osobę mającą dostęp do danych osobowych z Administratorem.

3.12. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza wyznaczone miejsce ich przetwarzania bez wyraźnego uprzedniego polecenia Administratora.

D. Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych

3.13. Dane osobowe przetwarzane są w wyznaczonych do tego celu pomieszczeniach. Pomieszczenia te zabezpieczone są zamykanymi na klucz drzwiami i systemem alarmowym przeciwwłamaniowym, a okna w tych pomieszczeniach zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej. Pomieszczenia te są ponadto zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

3.14. Przebywanie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz pod warunkiem, że sposób zabezpieczenia tych danych wyklucza przypadkowe ich ujawnienie osobie postronnej.

3.15. Budynki lub pomieszczenia, w których przetwarza się dane osobowe, muszą pozostawać zamknięte na klucz pod nieobecność osób upoważnionych przez Administratora do przetwarzania danych osobowych. Osoby posiadające klucze do tych budynków lub pomieszczeń obowiązane są do ich należytego zabezpieczenia.

3.16. Dostęp do budynków i pomieszczeń, w których przetwarzane są dane osobowe, jest pod nieobecność osób upoważnionych do przetwarzania danych osobowych nadzorowany przez służbę ochrony.

3.17. W miejscu przetwarzania danych osobowych w formie papierowej obowiązuje tzw. zasada „czystego biurka". Zasada ta oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym.

3.18. Zbiory danych osobowych w formie papierowej przechowywane są w zamykanych na klucz szafach.

3.19. Niszczenie wszelkich materiałów zawierających dane osobowe odbywa się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

3.20. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych danych osobowych oraz programów służących do przetwarzania danych. Kopie zapasowe przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco, i usuwane niezwłocznie po ustaniu ich użyteczności.

3.21. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd do wyświetlanych na nich treści osobom postronnym.

3.22. Osobom mającym dostęp do danych osobowych zapewnia się szkolenia, instrukcje i wyjaśnienia niezbędne do zagwarantowania bezpiecznego przetwarzania danych osobowych.

3.23. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. Do każdego użytkownika systemu informatycznego przypisany jest identyfikator użytkownika, a dostęp do danych osobowych możliwy jest wyłącznie po wprowadzeniu tego identyfikatora i dokonaniu uwierzytelnienia za pomocą hasła składającego się co najmniej z 8 znaków i zawierającego małe i wielkie litery oraz cyfry lub znaki specjalne. Zmiana hasła następuje nie rzadziej niż co 30 dni.

3.24. Identyfikator użytkownika, który utracił upoważnienie do przetwarzania danych osobowych, nie może być przydzielony innej osobie.

3.25. System informatyczny służący do przetwarzania danych osobowych podlega zabezpieczeniu, w szczególności przed:

a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,

c) zagrożeniami pochodzącymi z sieci publicznej.

3.26. Osobą wyłącznie uprawnioną do instalowania nowego oprogramowania oraz wprowadzania zmian w oprogramowaniu już zainstalowanym na komputerach Administratora jest Administrator Systemów Informatycznych.

E. Szczególne dodatkowe środki dotyczące zabezpieczenia danych osobowych na urządzeniach przenośnych i nośnikach danych

3.27. Osoba użytkująca urządzenia przenośne lub nośniki danych zawierające dane osobowe zachowuje szczególną ostrożność podczas ich transportu, przechowywania i użytkowania, w tym zabezpiecza je hasłem oraz stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

3.28. Urządzenia przenośne i nośniki danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych, hotelach, samochodach i innych miejscach, do których dostęp mogą uzyskać osoby postronne.

3.29. Urządzenia przenośne i nośniki danych należy przewozić w przeznaczonych do tego pokrowcach, o ile są one dostępne.

3.30. Urządzenia przenośne i nośniki danych należy chronić przed uszkodzeniami, w szczególności przestrzegając zaleceń producentów dotyczących ochrony sprzętu.

3.31. Użytkowanie urządzeń przenośnych i nośników danych w miejscach publicznych jest dozwolone wyłącznie pod warunkiem wykluczenia ryzyka przypadkowego ujawnienia danych osobowych osobie postronnej.

3.32. Urządzenia przenośne i nośniki danych mogą być użytkowane wyłącznie przez osoby wskazane przez Administratora.

3.33. Osoba użytkująca urządzenia przenośne lub nośniki danych jest zobowiązana do wykonywania kopii zapasowych danych osobowych oraz programów służących do przetwarzania danych według instrukcji przekazanych jej przez Administratora lub Administratora Systemów Informatycznych.

3.34. Osoba użytkująca urządzenia przenośne lub nośniki danych jest zobowiązana do niezwłocznego zawiadomienia Administratora lub Administratora Systemów Informatycznych o ich utracie lub uszkodzeniu.

4. Inspektor ochrony danych

4.1. U Administratora nie wyznaczono inspektora ochrony danych w rozumieniu RODO.

4.2. Administrator wyznaczy inspektora ochrony danych w przypadku, gdy będzie to wymagane przez powszechnie obowiązujące przepisy prawa albo gdy uzna to za środek niezbędny do zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

5. Postępowanie w przypadku naruszenia ochrony danych osobowych

A. Postępowanie wewnętrzne

5.1. Każdy, kto poweźmie wiadomość o przypadku naruszenia ochrony danych osobowych, zobowiązany jest do niezwłocznego zawiadomienia o tym fakcie Administratora Systemów Informatycznych.

5.2. Jeżeli jest to możliwe i uzasadnione okolicznościami, osoba dokonująca zawiadomienia powinna:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków naruszenia,

b) ustalić przyczyny i sprawców naruszenia,

c) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,

d) udokumentować wstępnie zaistniałe naruszenie,

e) nie opuszczać miejsca incydentu prowadzącego do naruszenia do czasu przybycia Administratora Systemów Informatycznych, jeżeli ten uzna to za konieczne.

5.3. W razie otrzymania zawiadomienia o przypadku naruszenia ochrony danych osobowych Administrator Systemów Informatycznych powinien niezwłocznie podjąć wszelkie działania niezbędne do wyjaśnienia okoliczności związanych z naruszeniem i minimalizacji jego skutków. O podjętych działaniach Administrator Systemów Informatycznych bezzwłocznie zawiadamia Administratora, który może wydać mu wiążące wskazówki co do sposobu postępowania w sprawie naruszenia.

5.4. O ile nie okaże się, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator Systemów Informatycznych zobowiązany jest do niezwłocznego przygotowania projektu zgłoszenia naruszenia ochrony

danych osobowych do organu nadzorczego i przekazania tego projektu Administratorowi. Projekt zgłoszenia powinien co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

b) zawierać imię i nazwisko oraz dane kontaktowe Administratora Systemów Informatycznych jako oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji,

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

d) 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.

5.5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Systemów Informatycznych zobowiązany jest do niezwłocznego przygotowania projektu zawiadomienia osoby, której dane dotyczą, o takim naruszeniu, i przekazania tego projektu Administratorowi. Projekt zawiadomienia powinien jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz powinien co najmniej:

a) zawierać imię i nazwisko oraz dane kontaktowe Administratora Systemów Informatycznych jako oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji,

b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

c) 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.

5.6. Przygotowanie przez Administratora Systemów Informatycznych projektu zawiadomienia, o którym mowa w punkcie 5.5 powyżej, nie jest wymagane w następujących przypadkach:

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

b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c) zawiadomienie osoby, której dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku Administrator Systemów Informatycznych przygotowuje publiczny komunikat lub zastosowanie podobnego środka, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

5.7. Administrator, uwzględniając informacje i dokumenty przekazane przez Administratora Systemów Informatycznych, dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta prowadzona jest w sposób, który pozwala organowi nadzorczemu na weryfikację przestrzegania art. 33 RODO.

B. Postępowanie zewnętrzne

5.8. 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, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenie musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

b) zawierać imię i nazwisko oraz dane kontaktowe Administratora Systemów Informatycznych jako oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji,

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

d) 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.

5.9. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, Administrator może je udzielać organowi nadzorczemu sukcesywnie bez zbędnej zwłoki.

5.10. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz powinno co najmniej:

a) zawierać imię i nazwisko oraz dane kontaktowe Administratora Systemów Informatycznych jako oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji,

b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

c) 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.

5.11. Zawiadomienie, o którym mowa w punkcie 5.10 powyżej, nie jest wymagane w następujących przypadkach:

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

b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

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

6. Aktualność środków ochrony danych osobowych

6.1. Administrator dokonuje stałej oceny ryzyka naruszenia praw lub wolności osób fizycznych w związku z przetwarzaniem danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania.

6.2. Środki techniczne i organizacyjne wdrożone przez Administratora celem zapewnienia, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać, w tym w szczególności Polityka Ochrony Danych Osobowych, są w razie potrzeby poddawane przeglądom i uaktualniane.

6.3. Potrzeba przeglądu środków technicznych i organizacyjnych występuje co najmniej w przypadku, gdy zmieni się charakter, zakres, kontekst lub cel przetwarzania albo prawdopodobieństwo lub poziom ryzyka naruszenia praw lub wolności osób fizycznych.

6.4. Potrzeba uaktualnienia środków technicznych i organizacyjnych występuje co najmniej w przypadku, gdy zmieni się prawdopodobieństwo lub poziom ryzyka naruszenia praw lub wolności osób fizycznych.

7. Postanowienia końcowe

7.1. Przestrzeganie Polityki Ochrony Danych Osobowych stanowi dla pracowników Administratora podstawowy obowiązek pracowniczy w rozumieniu Kodeksu pracy.

7.2. Załączniki do Polityki Ochrony Danych Osobowych stanowią jej integralną część.