**POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH**

**ROZDZIAŁ 1**

**POSTANOWIENIA OGÓLNE**

1. Niniejszy dokument zawiera ogólne zasady ochrony danych osobowych w firmie RS STUDIO PROJEKTOWE architekt Roland Stańczyk, Wierzbnowska 66D, 05-510 Konstancin-Jeziorna - („**Administrator**”).
2. Niniejszy dokument, zwany dalej „**Polityką Bezpieczeństwa**”, został wdrożony w celu dostosowania działalności Administratora do przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE) („**RODO**”) oraz przepisów prawa polskiego wydanych na podstawie upoważnień przewidzianych przepisami RODO, tj. ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku o ochronie danych osobowych („**UODO**”).
3. Administrator jest administratorem danych osobowych, o których mowa w wykazie stanowiącym Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa (rejestr czynności przetwarzania).
4. Ilekroć w niniejszym dokumencie jest mowa o:
5. **RODO** – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27.04.2016r. 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 osobowych);
6. **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie 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;
7. **szczególnych kategorii danych** – rozumie się przez to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;
8. **przetwarzaniu** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
9. **pseudonimizacji** – rozumie się przez to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
10. **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
11. **administratorze** - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
12. **podmiocie przetwarzającym** - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
13. **odbiorcy** - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
14. **stronie trzeciej** - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
15. **zgodzie** osoby, której dane dotyczą - rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
16. **naruszeniu ochrony danych osobowych** - rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
17. **organie nadzorczym** - rozumie się przez to niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO i art. 34 UODO;
18. **wytycznych Grupy Roboczej** – wytyczne wydane i opublikowane przez Grupę Roboczą powołaną na podstawie art. 29 dyrektywy nr 95/46/WE;
19. **osobie zatrudnionej** – rozumie się przez to osobę, wykonującą wewnątrz firmy Administratora działania na rzecz Administratora na podstawie zawartej umowy o pracę.
20. Administrator, przy przetwarzaniu danych osobowych, stosuje następujące **zasady**:
	1. zasadę **zgodności z prawem, rzetelności i przejrzystości** – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
	2. zasadę **ograniczenia celu przetwarzania** – dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
	3. zasadę **minimalizacji danych** – dane osobowe musza być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
	4. zasadę **prawidłowości** – dane osobowe muszą być 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;
	5. zasadę **ograniczonego przechowywania** - dane osobowe muszą być 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;
	6. zasadę **integralności i poufności** - dane osobowe muszą być 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;
	7. zasadę **rozliczalności** – Administrator jest odpowiedzialny za przestrzeganie przepisów i wykazanie ich stosowania.
21. Administrator uwzględniania ochronę danych w fazie projektowania przetwarzania danych osobowych oraz stosuje domyślną ochronę danych zgodnie z przepisami RODO i UODO oraz stosując środki techniczne i organizacyjne opisane w niniejszym dokumencie.

**ROZDZIAŁ 2**

**INSPEKTOR OCHRONY DANYCH OSOBOWYCH,
KOORDYNATOR DS. OCHRONY DANYCH**

1. Na dzień przyjmowania niniejszego dokumentu, Administrator nie stwierdził, aby na podstawie art. 37 ust. 1 RODO był obowiązany do powołania Inspektora Ochrony Danych Osobowych.
2. Administrator wyznaczy inspektora ochrony danych osobowych („**Inspektor**”) w przypadku, jeżeli główna działalność Administratora będzie polegać 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 na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO lub Administrator spełni pozostałe wymagania określone powszechnie obowiązującym przepisami (w szczególności w odniesieniu do ilości zatrudnionych).

**ROZDZIAŁ 3**

**WYKAZ DANYCH PRZETWARZANYCH PRZEZ ADMINISTRATORA**

1. Administrator przetwarza dane osobowe w zakresie zgodnym z wykazem – rejestrem przetwarzania danych osobowych stanowiącym Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa.
2. Administrator nie przetwarza szczególnych kategorii danych.
3. Administrator nie przetwarza danych osobowych osób poniżej 18.tego roku życia.
4. Administrator nie przekazuje danych osobowych do krajów trzecich, tj. poza obszar EOG.

**ROZDZIAŁ 4**

**POUFNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH**

1. Przetwarzanie danych osobowych odbywa się wyłącznie z upoważnienia Administratora. Dostęp do danych osobowych mogą mieć osoby, które: a/ są zatrudnione przez Administratora lub b/ zawarły z Administratorem umowę powierzenia przetwarzania danych osobowych lub c/ są upoważnione do przetwarzania danych na podstawie obowiązującego na terytorium Rzeczypospolitej Polskiej aktu prawnego lub d/ są współadministratorami danych osobowych.
2. W przypadku osób zatrudnionych dostęp do przetwarzania danych osobowych mają wyłącznie osoby, które:
3. zostały upoważnienie przez Administratora do przetwarzania danych osobowych oraz
4. zostały poinformowane przez Administratora o zasadach przetwarzania danych osobowych u Administratora, w szczególności poprzez zapoznanie się z dokumentacją wdrożoną u Administratora w zakresie ochrony danych osobowych, w tym z niniejszym dokumentem oraz
5. uczestniczyły w szkoleniu zorganizowanym przez Administratora w zakresie ochrony danych osobowych.
6. W celu utrzymania odpowiedniego poziomu wiedzy osób upoważnionych do przetwarzania danych osobowych Administrator zapewnia:
7. uprzednią informację o zmianach dokumentacji z zakresu przetwarzania danych osobowych,
8. szkolenia z zakresu ochrony danych osobowych.
9. W celu zapewnienia poufności danych osobowych przetwarzanych u Administratora, Administrator pozyskuje oświadczenia o zachowaniu poufności od:
10. osób zatrudnionych,
11. osób, które nie są upoważnione do przetwarzania danych osobowych, jednak z uwagi na dostęp do pomieszczeń Administratora mogą mieć dostęp do danych osobowych (np. dotyczy osób sprzątających).
12. Wykaz osób i zakres powierzonego im przetwarzania danych osobowych zawiera Załącznik nr 1 do Polityki Bezpieczeństwa.
13. Wzór upoważnia dla osób upoważnionych do przetwarzania danych osobowych zawiera Załącznik 2 do Polityki Bezpieczeństwa.

**ROZDZIAŁ 5**

**PODSTAWA PRZETWARZANIA DANYCH OSOBOWYCH**

1. Administrator przetwarza dane osobowe: (a) na podstawie zgody osoby, której dane dotyczą lub (b) w celu wykonania umowy zawartej przez Administratora lub (c) w celu wypełnienia obowiązków prawnych ciążących na Administratorze lub (d) w celu wynikającym z prawnie uzasadnionych interesów realizowanych przez Administratora. Podstawy przetwarzania poszczególnych danych osobowych wskazuje Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa.
2. W przypadku prowadzenia procesów rekrutacyjnych Administrator przetwarzane dane osobowe kandydatów na podstawie zgody kandydata.
3. W przypadku zatrudnienia kandydata, Administrator przetwarza jego dane osobowe na podstawie umowy lub na podstawie zgody.
4. W przypadku przetwarzania danych osobowych na podstawie zgody osoby, zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia.

**ROZDZIAŁ 6**

**CZAS PRZETWARZANIA DANYCH OSOBOWYCH**

Dane osobowe są przetwarzane przez czas wskazany w Załączniku nr 1 do niniejszej Polityki Bezpieczeństwa.

**RODZIAŁ 7**

**OBOWIĄZEK INFORMACYJNY**

1. Administrator, zbierając dane osobowe, przekazuje osobom fizycznym informacje,
o których mowa w art. 13 i 14 RODO z uwzględnieniem przepisów ustawy o ochronie danych osobowych. Administrator podejmuje odpowiednie środki, by w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą wszelkich informacji. Jeżeli osoba, której dane dotyczą tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
2. W przypadku zbierania przez Administratora danych osobowych od osoby, której dane dotyczą, Administrator przekazuje informację, o której mowa w art. 13 RODO podczas pozyskiwania danych, chyba że osoba, której dane dotyczą dysponuje już tymi informacjami.
3. W przypadku pozyskania przez Administratora danych osobowych w sposób inny niż od osoby, której dane dotyczą, Administrator podaje informację:
4. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych,
5. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
6. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
7. Postanowienia powyższe nie mają zastosowania, gdy – i w zakresie, w jakim:
8. osoba, której dane dotyczą, dysponuje już tymi informacjami;
9. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
10. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą lub;
11. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.
12. Wzór informacji stanowi Załącznik nr 3 do Polityki Bezpieczeństwa.
13. Wzór zgody pracownika na przetwarzanie danych stanowi Załącznik 3a do Polityki Bezpieczeństwa.

**ROZDZIAŁ 8**

**ODBIORCY DANYCH OSOBOWYCH**

1. Administrator udostępnia dane osobowe jedynie w zakresie, w jakim jest to niezbędne do realizacji celu przetwarzania danych osobowych:
	1. na podstawie przepisów prawa:
2. podmiotom publicznym, w odniesieni do których cel i sposób przetwarzania danych określają przepisy ustaw,
3. podmiotom prywatnym, w odniesieniu do których cel i sposób przetwarzania powierzonych danych określają przepisy ustaw i które, zgodnie z przepisami prawa są zobowiązane do zachowania w tajemnicy otrzymanych danych osobowych (banki, usługi pocztowe i kurierskie, notariusze);
	1. na podstawie umowy powierzenia przetwarzania danych osobowych: podmiotom prywatnym, z których usług Administrator korzysta (np. usługi księgowe, usługi prawne).
4. W przypadku zawierania umów powierzenia przetwarzania danych osobowych, Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.
5. W przypadku sprostowania, usunięcia danych osobowych lub ograniczenia przetwarzania, które Administrator wykona zgodnie z art. 16, 17 i 18 RODO, Administrator informuje każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
6. Podstawowe założenia umowy z podmiotem przetwarzającym zawiera Załącznik nr 4 do Polityki Bezpieczeństwa Wzór rejestru umów powierzenia przetwarzania stanowi Załącznik nr 5 do Polityki Bezpieczeństwa.

**ROZDZIAŁ 9**

**ZAPEWNIENIE BEZPIECZEŃSTWA**

1. Administrator, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie.
2. Administrator na bieżąco monitoruje czy, w odniesieniu do konkretnej osoby, które dane przetwarza, upłynął czas, w którym dane mogą być przetwarzana i w konsekwencji usuwa dane takich osób.
3. Administrator zapewnia szkolenia dla osób zatrudnionych w miarę potrzeb, a także w przypadku każdej zmiany przepisów regulujących przetwarzanie danych osobowych. W szczególności szkolenia mogą mieć formę szkoleń prowadzonych przez wyspecjalizowane podmioty zewnętrzne, webinariów itp.

**ROZDZIAŁ 10**

**ZAPEWNIENIE BEZPIECZEŃSTWA FIZYCZNEGO DANYCH OSOBOWYCH**

Dane osobowe są przetwarzane pod adresem głównego miejsca wykonywania działalności gospodarczej przez Administratora na zasadach opisanych w Załączniku nr 6.

**ROZDZIAŁ 11**

**ZAPEWNIENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH**

1. Administrator korzysta z własnych urządzeń biurowych i urządzeń (drukarka, skaner, ksero, komputer) oraz legalnego oprogramowania.
2. Dane osobowe są zabezpieczone w systemach informatycznych Administratora, w sposób opisany w Załączniku nr 6a.

**ROZDZIAŁ 12**

**OGÓLNE ZASADY PROWADZENIE KOMUNIKACJI
Z OSOBĄ, KTÓREJ DANE DOTYCZĄ**

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem prowadzić z osobą, której dane dotyczą wszelką komunikację na podstawie art. 15 – 22 oraz 34 RODO, tj. w przypadku wykonywania przez tę osobę:
2. prawa dostępu do danych osobowych (art. 15 RODO),
3. prawa do sprostowania danych (art. 16 RODO),
4. prawa do usunięcia danych („prawa do bycia zapomnianym”) (art. 17 RODO),
5. prawa do ograniczenia przetwarzania (art. 18 RODO),
6. prawa do przenoszenia danych (art. 20 RODO),
7. prawa do sprzeciwu (art. 21 RODO),
8. prawa do niepodlegania zautomatyzowanemu przetwarzaniu, w tym profilowaniu (art. 22 RODO),

oraz w przypadku powiadomienia osoby, której dane dotyczą o sprostowaniu lub usunięciu lub ograniczeniu przetwarzania danych (art. 19 RODO) oraz zawiadomienia o naruszeniu ochrony danych osobowych (art. 34 RODO).

1. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na podstawie przepisów RODO wskazanych ust. 1 powyżej.
2. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem zgłoszonym przez osobę, której dane dotyczą na podstawie art. 15 – 22 RODO. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. W celu zrealizowania wniosku, Administrator podejmuje czynności wskazane w Rozdziale 9 niniejszej Polityki Bezpieczeństwa.
3. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

**ROZDZIAŁ 13**

**ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

 **ORGANOWI NADZORCZEMU**

1. W przypadku powzięcia informacji, przez jakąkolwiek osobę zatrudnioną u Administratora lub przez któregokolwiek z odbiorców danych, o jakimkolwiek incydencie, który może doprowadzić do naruszenia ochrony danych osobowych (lub podejrzeniu takiego naruszenia) od jakiejkolwiek osoby lub z jakiegokolwiek źródła, w tym od podmiotu przetwarzającego, osoba, która powzięła taką informacje niezwłocznie informuje o tym fakcie Administratora. Incydentem, o którym mowa powyżej może być jakiekolwiek zdarzenie, które zagraża bezpośrednio lub pośrednio bezpieczeństwu przetwarzania danych osobowych, w tym np. naruszenie bezpieczeństwa fizycznego pomieszczeń lub sprzętów (w szczególności podejrzenie włamania, zalania, zagubienia nośnika z danymi osobowymi) lub próby wyłudzenia danych osobowych przez osoby nieupoważnione.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych, Administrator, po przeprowadzeniu analizy 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.
3. Zgłoszenia dokonuje się do organu nadzorczego. Zgłoszenia dokonuje Administrator.
4. Zgłoszenie organowi nadzorczemu musi co najmniej:
5. 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;
6. zawierać imię i nazwisko oraz dane kontaktowe Inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
7. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
8. 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.
9. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki. Wzór zgłoszenia naruszenia stanowi Załącznik nr 7 do Polityki Bezpieczeństwa.
10. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania postanowień niniejszego Rozdziału. Wzór rejestru naruszeń stanowi Załącznik nr 8 do Polityki Bezpieczeństwa.

**ROZDZIAŁ 14**

**ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH**

1. Jeżeli naruszenie ochrony danych osobowych, o którym mowa w Rozdziale 12, może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego Rozdziału, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO, tj.
3. zawierać imię i nazwisko oraz dane kontaktowe Inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
4. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
5. 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.
6. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
7. 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;
8. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
9. wymagałoby ono niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
10. Jeżeli Administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

**ROZDZIAŁ 15**

**OCENA SKUTKÓW DLA OCHRONY DANYCH**

1. W przypadku, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele, z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. Do oceny skutków dla ochron danych osobowych zastosowanie mają przepisy art. 35 RODO, Wytyczne Grupy Roboczej 29 oraz inne wytyczne i procedury wydane przez upoważnione do tego organy.
3. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
4. Jeżeli ocena skutków dla ochrony danych, o której mowa w powyżej, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.

**ROZDZIAŁ 16**

**POSTANOWIENIA KOŃCOWE**

Niniejsza Polityka Bezpieczeństwa wchodzi w życie z dniem 25 maja 2018r.

podpis w imieniu Administratora