POLITYKA PRZETWARZANIA DANYCH OSOBOWYCH

OPRACOWANE DLA:

Marta Rasch-Urbaniak
Sadowska-Karolczak Katarzyna
Novomoda s.c. z siedzibą w Poznaniu, os. Pod Lipami 4/22, 61-629 Poznań

OPRACOWAŁA:

r.pr. Magdalena Skrzątek - Urbańska

Poznań, dn. 2018 r.

Spis treści

Preambuła

Niniejszym administrator danych osobowych, biorąc za podstawę m.in. art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119, str. 1), wdraża niniejszą politykę, by móc osiągnąć zgodność z RODO i aby móc taką zgodność wykazać.

Rozdział I

Słownik pojęć

§1

1. **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) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119, str. 1).
2. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
3. **Przetwarzanie danych osobowych** – operacja lub ich zestaw na danych osobowych, dokonywana w sposób zautomatyzowany, jak i niezautomatyzowany, tj. przede wszystkim: zbieranie, utrwalanie, organizowanie, przeglądanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie, przesłanie, rozpowszechnianie, udostępnianie, łączenie, dopasowywanie, ograniczenie, usuwanie lub niszczenie.
4. **Administrator danych** – tj. badany podmiot – osoba fizyczna, prawna lub organ publiczny, który określa sposób i cel przetwarzania danych osobowych.
5. **Odbiorca** - osoba fizyczna, prawna lub organ publiczny, któremu ujawnia się dane osobowe.
6. **Organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych.

Rozdział II

Opis zasad przetwarzania danych osobowych

§1

1. Niniejszym wskazuje się, że administratorem danych osobowych jest: Marta Rausch-

Urbaniak prowadząca działalność gospodarczą pod firmą NOVAMODA MARTA RAUSCH – URBANIAK oraz Katarzyna Sakowska-Karolczak prowadząca działalność gospodarczą pod firmą NOVAMODA KATARZYNA SAKOWSKA KAROLCZAK występujące łącznie jako Novomoda s.c. z siedzibą w Poznaniu przy os. Pod Lipami 4/22, 61-629 Poznań.

2. Wszelkie sprawy dotyczące przetwarzania danych osobowych należy zgłaszać korespondencyjnie administratorowi. Administrator z kolei wszelkie odebrane zgłoszenia realizuje zgodnie z zapisami niniejszej polityki i procedur składowych.

§2

1. W organizacji zarządzanej przez administratora dane osobowe przetwarza się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla podmiotów danych.
2. Administrator danych osobowych dokonał inwentaryzacji procesów przetwarzania danych osobowych, czego dowodem jest Protokół pokontrolny z dnia X 2018 roku, który stanowi Załącznik 1 do niniejszej polityki. Wdrożenie zaleceń z powyższego protokołu stanowi potwierdzenie usunięcia nieprawidłowości i osiągnięcia zgodności z zapisami kolejnych artykułów RODO.
3. Podstawy prawne przetwarzania danych osobowych, które zidentyfikowano w organizacji administratora to:
   a) zgoda osoby, której dane dotyczą, tj. art. 6 ust. 1 lit. a RODO (w odniesieniu do działań marketingowych),
   b) realizacja umowy, której stroną jest osoba, której dane dotyczą (oraz podjęcie działań zmierzających do zawarcia takiej umowy, na żądanie osoby, której dane dotyczą/strony), tj. art. 6 ust. 1 lit. b RODO (niniejszy zapis ma zastosowanie do większości przypadków realizacji statutowej działalności administratora, tj. sprzedaży towarów klientom i ich kupna od kontrahentów),
   c) realizacja obowiązku prawnego ciążącego na administratorze danych, tj. art. 6 ust. 1 lit. c RODO (powyższe odnosi się do realizacji obowiązków prawnych, które ciążą na administratorze jako sprzedawcy towarów, czy też podmiocie zakupującym towary od kontrahentów),
   d) realizacja prawnie uzasadnionego interesu administratora danych, tj. art. 6 ust. 1 lit. f RODO (celem przetwarzania, które jest realizowane na takiej podstawie, to przede wszystkim niektóre działania marketingowe).

   Powyższe podstawy prawne wynikające z RODO w większości przypadków łączą się z podstawami prawnymi wynikającymi z zapisów innych ustaw i rozporządzeń, tj. m.in. ustawa o ochronie danych osobowych, ustawa o rachunkowości i inne.

§3

1. Procesy przetwarzania danych osobowych, które mają miejsce w związku z realizacją statutowej działalności organizacji mają jasne, konkretne, wyraźne i prawnie uzasadnione cele. Powyższe ma poparcie w ust. 3 § 2 niniejszej polityki.
2. W organizacji przestrzega się zasady ograniczenia celu. Powyższe ma swoje uzasadnienie w Protokole pokontrolnym z dnia X 2018 roku, który stanowi Załącznik nr 1 do niniejszej polityki.

§4

1. W organizacji stosuje się zasadę minimalizacji danych.
2. Zakres przetwarzanych danych, które pobiera się od poszczególnych podmiotów danych jest adekwatny do realizowanego celu.
3. Nie przetwarza się danych nadmiernych.
4. W organizacji unika się także przetwarzania szczególnych kategorii danych i pozostałych specyficznych kategorii danych. Takie kategorie danych pojawiają się tylko i wyłącznie w związku z realizacją stosunku pracy, czy też ochroną ewentualnych roszczeń.

§5

1. W organizacji stosuje się zasadę prawidłowości przetwarzanych danych osobowych.
2. Zgodnie z art. 5 ust. 1 lit. d RODO, podejmuje się rozsądne działania, aby dane osobowe były prawidłowe w świetle celów ich przetwarzania. Dlatego też w stosownych przypadkach dane nieprawidłowe są usuwane lub prostowane.
3. Wskazuje się, że organizacja przetwarza dane osobowe kategorii podmiotów, takich jak:
   a) wspólnicy,
   b) klienci,
   c) kontrahenci (dostawcy usług i towarów).

§6

1. Przetwarzane w organizacji dane osobowe przechowywane są w formie umożliwiającej identyfikację osoby, której dane dotyczą (z uwzględnieniem czasu potrzebnego do identyfikacji oraz środków i technologii adekwatnych do realizowanego celu).
2. Dane przetwarza się w sposób tradycyjny lub zautomatyzowany.
3. W organizacji zarządzanej przez administratora stosuje się zasadę ograniczenia przetwarzania, tj. unika się retencji danych.
4. Administrator danych osobowych zidentyfikował następujące maksymalne okresy przetwarzania danych osobowych:
   a) do momentu ustania celu,
   b) do momentu wycofania zgody,

c) do momentu zakończenia realizacji umowy (także okres ew. gwarancji).

Ponadto maksymalne okresy przechowania wyznaczone konkretnym przepisem prawa, które występują w organizacji, to przede wszystkim:

a) okres przedawnienia ewentualnych roszczeń,
b) okres niezbędny do przechowania dokumentów rachunkowych,
c) okresy wewnętrznie ustalone w organizacji.

§7

1. Dane osobowe przetwarzane przez organizację zostały odpowiednio zabezpieczone. Określając zabezpieczenia, administrator danych przede wszystkim skupił się na:
   a) ochronie przed niedozwolonym lub niezgodnym z prawem przetwarzaniem,
   b) ochronie przed przypadkową utratą danych,
   c) ochronie przed zniszczeniem danych oraz ich uszkodzeniem.
2. Zestawienie środków organizacyjnych i technicznych, które zabezpieczają procesy przetwarzania wykazano w Załączniku 2, tj. Ogólna ocena ryzyka związanego z przetwarzaniem danych osobowych oraz w Załączniku 3, tj. Rejestr czynności przetwarzania danych osobowych. We wspomnianym Załączniku 1 i 2 wskazano także obszar przetwarzania danych osobowych.

§8

1. Administrator danych osobowych, m.in. poprzez stworzenie niniejszego środka organizacyjnego, tj. niniejszej polityki, zapewnia nadrzędną zasadę dotyczącą przetwarzania danych osobowych, tj. rozliczalność.

Rozdział III
Zgodność z prawem procesów przetwarzania

§1

1. Inwentaryzacja procesu przetwarzania danych osobowych, której wynik przedstawiono w Załączniku 1 oraz zestawienie wykazane w §2 Rozdziału I niniejszej polityki, obrazuje, że administrator danych osobowych przetwarza w ramach organizacji dane osobowe zgodnie z prawem.
2. Odnośne szczególnych kategorii danych osobowych (dane dot. stanu zdrowia) ustalono, że dane dotyczące stanu zdrowia pojawiają się w związku z realizacją zatrudnienia wspólniczek

Rozdział IV
Prawa osoby, której dane dotyczą

§1

1. Administrator danych osobowych, w przypadku konieczności realizowania rozbudowanego katalogu praw przysługującego podmiotom danych, ułatwia osobom zainteresowanym realizację ww. praw.
2. Informacje, zależnie od sytuacji, będą udzielane przez administratora na piśmie lub elektronicznie.
3. Szczegółowy opis działania został zawarty w Załączniku 4, tj. Procedura realizacji praw podmiotów danych.
4. Informacja podawana w przypadku zbierania danych osobowych jest udzielana wobec podmiotów, takich jak:
   a) klienci,
   b) kontrahenci.

Rozdział V
Realizacja obowiązków ogólnych administratora danych osobowych

§1

1. Tak jak wskazano powyżej, opis odpowiednich środków technicznych i organizacyjnych, które administrator wdrożył, aby przetwarzanie odbywało się zgodnie z RODO, zostały zawarte w Załączniku 2.
2. W przypadku wprowadzenia do organizacji nowych sposobów przetwarzania, administrator danych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności podmiotów danych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania, uwzględni ochronę danych w fazie projektowania. Realizacja powyższego nastąpi w ramach organizacji lub poprzez konsultacje z podmiotem zewnętrznym.
3. Administrator zapewnia domyślną ochronę danych poprzez faktyczne stosowanie zasady minimalizacji danych.
4. Administrator danych zawarł umowy powierzenia do przetwarzania danych osobowych z właściwymi dostawcami usług (procesorami).
5. Administrator danych, pomimo że w jego przypadku nie jest to konieczne, opracował rejestr czynności przetwarzania, który stanowi Załącznik 3 i jest on także prowadzony w formie arkusza elektronicznego.
6. Administrator wdrożył środki organizacyjne, które pozwalają na zgłaszanie ewentualnego naruszenia ochrony danych osobowych organowi nadzorczemu oraz pozwalają na zawiadomienie osoby, której dane dotyczą, o naruszeniu danych osobowych.

7. Ustalano i wykazano, że administrator danych nie jest zobowiązany do wyznaczenia inspektora ochrony danych osobowych (oceniając stan faktyczny uwzględniono wytyczne zawarte w art. 37 ust. 1 lit. a i b RODO).
8. Ustalono i wykazano, że w ramach procesów przetwarzania danych osobowych w organizacji odbywa się transfer danych osobowych do państw trzecich, tj. poza EOG.

Rozdział VI
Postępowanie w przypadku wystąpienia incydentów

§1

1. Administrator ustanowił procedurę reagowania w przypadku wystąpienia incydentów, tj. naruszeń ochrony danych osobowych. Przedmiotowa procedura stanowi Załącznik 7.
2. Procedura zawiera schemat działania zarówno wobec organu nadzorczego, jak i wobec podmiotów danych.

Rozdział VII
Zakończenie

§1

1. Po dokonaniu audytu procesów oraz zastosowaniu podejścia opartego na ryzyku Administrator postanowił ograniczyć zakres opracowanej dokumentacji do tej, o której mowa w niniejszej polityce.
2. Podczas opracowania niniejszej polityki nie istnieje żaden krajowy akt prawny, który narzucałby konieczność opracowania, czy też wdrożenia jakiegokolwiek innego środka organizacyjnego, czy też technicznego poza tymi, o których mowa w RODO.
3. Wszelkie istotne kwestie dotyczące infrastruktury informatycznej zostały zwarte w Załączniku 6.
4. Potrzeby biznesowe Administratora danych nie wskazują na konieczność stworzenia planu ciągłości działania. Elementy działań odtworzeniowych wskazano w Załączniku 2,5 i 6.
5. Zapisy niniejszej polityki obowiązują od dnia X 2018 r.

Wykaz załączników:

- Załącznik 1 – Protokół pokontrolny z dnia 19 czerwca 2018 r.
- Załącznik 2 – Raport z ogólnej oceny ryzyka związanego z przetwarzaniem danych osobowych.
- Załącznik 3 – Rejestr czynności przetwarzania danych osobowych.

- Załącznik 4 – Procedura realizacji praw podmiotów danych.
- Załącznik 5 – Procedura postępowania na wypadek zaistnienia incydentu naruszenia ochrony danych osobowych.
- Załącznik 6 – Zbiór informacji na temat infrastruktury techniczno-informatycznej w badanym przedsiębiorstwie.
- Załącznik 7 – Procedura czystego biurka i ekranu.

Załącznik 1

Protokół pokontrolny z dnia X 2018 roku

Przedmiotowy protokół stanowi odrębny dokument wewnętrzny administratora danych, który jest przechowywany w jego siedzibie. Załącznikiem do przedmiotowego protokołu jest tzw. tabela zgodności.

Załącznik 2

Raport z ogólnej oceny ryzyka związanego z przetwarzaniem danych osobowych

Przedmiotowy dokument stanowi odrębny dokument wewnętrzny administratora danych, który jest przechowywany w jego siedzibie.

Załącznik 3

Rejestr czynności przetwarzania

Przedmiotowy dokument stanowi odrębny dokument wewnętrzny administratora danych, który jest przechowywany w jego siedzibie. Rejestr jest prowadzony w formie elektronicznej (plik Excel), a w razie potrzeby sporządza się stosowny wydruk.

Załącznik 4

Procedura realizacji praw podmiotów danych

Preambuła

Realizując obowiązki, które są nałożone na administratora danych osobowych przepisami RODO, szczególnie istotny wydaje się zakres poświęcony realizacji rozbudowanego katalogu praw podmiotów danych osobowych. Dlatego też schemat działania na wypadek pojawienia się żądań, czy też wniosków podmiotów danych został zawarty w niniejszym dokumencie.

§1

1. Realizacja rozbudowanego katalogu praw odbywa się w terminie miesiąca od otrzymania żądania.
2. Jeżeli zajdzie istotna potrzeba, tj. żądanie będzie miało skomplikowany charakter lub pojawi się w ilości utrudniającej realizację i Administrator danych uzna takie działanie za stosowne, to termin, o którym mowa w ustępie poprzedzającym można przedłużyć o kolejne dwa miesiące.
3. Stosując zapisy ustępu 2, Administrator poinformuje osobę zgłaszającą żądanie o przedłużeniu terminu. W informacji Administrator danych pod przyczynę opóźnienia.
4. Ustala się następujące zasady działania:
   a) jeżeli osoba, która zgłasza żądanie wniesie je drogą elektroniczną, to informacja zwrotna przekazywana jest drogą elektroniczną,
   b) jeżeli osoba, która zgłasza żądanie wniesie je tradycyjną drogą korespondencyjną, to informacja zwrotna jest odsyłana listem poleconym,
   c) jeżeli osoba, która zgłasza żądanie sama zadecyduje o formie dostarczenia jej informacji zwrotnej, to administrator zrealizuje takie żądanie, w miarę posiadanych środków, zgodnie z jego treścią.
5. Obsługą ewentualnej realizacji żądań dotyczących rozbudowanego katalogu praw, Administrator zajmuje się osobiście.
6. W przypadku pojawienia się sytuacji, w której Administrator nie podejmie działań związanych z żądaniem podmiotu danych, podmiot danych zostanie poinformowany o przyczynie odmowy (termin uzasadnienia odmowy: maksymalnie miesiąc od otrzymania żądania). Podmiot danych zostanie także pouczony o możliwości wniesienia skargi do

organu nadzorczego.

§2

1. W związku z płaską strukturą badanej organizacji, ustala się, że prawa osób, których dane dotyczą będą realizowane przez Administratora..

§3

1. Podczas realizacji rozbudowanego katalogu praw podmiotów danych, tj. udzielanie odpowiedzi na zapytania i żądania, nie stosuje się opłat.
2. W stosunku do ustępu poprzedzającego, zgodnie z zapisami RODO, wyznacza się następujące wyjątki:
   a) pobranie opłaty (celem pokrycia kosztów administracyjnych udzielenia informacji zwrotnej i podjęcia innych działań niezbędnych do jej zrealizowania) w sytuacji, gdy żądanie ma charakter nadmierny i/lub nieuzasadniony i/lub ustawiczny,
   b) odmówienie podjęcia działań w sytuacji, gdy żądanie ma charakter nadmierny i/lub nieuzasadniony i/lub ustawiczny.
3. Stosując zapis wynikający z ustępu poprzedzającego, Administrator będzie każdorazowo wykazywał, że przedmiotowe żądanie było nieuzasadnione i/lub nadmierne.

§4

1. Administrator danych realizując rozbudowany katalog praw, w przypadku pojawienia się uzasadnionych wątpliwości, zażąda od osoby zgłaszającej dodatkowych informacji celem potwierdzenia jej tożsamości.
2. Powyższe czynności zostaną dokonane przez Administratora samodzielnie lub w oparciu o konsultacje z wyspecjalizowanym podmiotem zewnętrznym.

§5

1. Każda osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy w ramach organizacji przetwarzane są dane osobowe jej dotyczące.
2. Jeżeli Administrator stwierdzi, że dane osoby, która zgłasza przedmiotowe żądanie są przetwarzane w organizacji, to udziela informacji zwrotnej, na którą składają się następujące elementy:
   a) określenie celu przetwarzania,
   b) określenie kategorii odnośnych danych osobowych,
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną

ujawnione (dodatkowo ewentualnie informacja o odbiorcach w tzw. państwach trzecich i o zabezpieczeniach takiego transferu – *vide* art. 46 RODO),

d) określenie planowanego okresu przetwarzania danych osobowych lub ewentualnie kryteria określania takiego okresu,

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz o prawie do wniesienia sprzeciwu wobec takiego przetwarzania,

f) informacje o prawie wniesienia skargi do organu nadzorczego,

g) informacje o źródle danych – jeżeli dane osobowe nie zostały pozyskane bezpośrednio od osoby, której dane dotyczą,

h) informacje o zautomatyzowanym podejmowaniu decyzji – jeżeli ma zastosowanie.

3. Jeżeli żądanie dostępu wiąże się z żądaniem otrzymania kopii przetwarzanych danych, to taką kopię danych podlegających przetwarzaniu Administrator dostarcza osobie, której dane dotyczą (każda kolejna kopia wydawana osobie, której dane dotyczą pozwala pobrać opłatę, o której mowa w § 3 ust. 2 lit. a niniejszej procedury).

§6

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania jej nieprawidłowych danych osobowych lub uzupełnienia jej niekompletnych danych osobowych.
2. Administrator danych, uzupełniając dane niekompletne, bierze pod uwagę przede wszystkim cel przetwarzania i na tej podstawie ocenia zasadność ewentualnych czynności.
3. Przyjmuje się, że Administrator zażąda od osoby zgłaszającej chęć skorzystania z prawa do sprostowania dodatkowego oświadczenia, w którym żądanie zostanie doprecyzowane. Po dokonaniu czynności takie oświadczenie zostaje zniszczone.

§7

1. Osoba, której dane dotyczą ma prawo żądać usunięcia jej danych, tj. skorzystać z prawa do bycia zapomnianym. W przypadku odebrania takiego żądania Administrator usuwa dane takiej osoby bez zbędnej zwłoki, jeżeli zachodzi jeden z poniższych warunków:

a) dane osobowe nie są już niezbędne do realizacji celów, dla których zostały zebrane,

b) osoba, której dane i żądanie dotyczą wycofała zgodę na przetwarzanie danych, a nie istnieje żadna inna podstawa prawna przetwarzania,

c) jeżeli przetwarzanie danych osobowych odbywało się na podstawie prawnie uzasadnionego interesu administratora lub w celu realizacji marketingu bezpośredniego,

a osoba, której dane dotyczą wnosi sprzeciw wobec przetwarzania danych osobowych i Administrator nie ma innych nadrzędnych prawnie uzasadnionych podstaw przetwarzania,

d) dane osobowe były przetwarzane niezgodnie z prawem,

e) dane osobowe muszą zostać usunięte w związku z obowiązkiem, który wynika z konkretnego przepisu prawa,

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

2. Ustala się, że organizacja ze względu na charakter swojej działalności nie upublicznia danych osobowych.

§8

1. Osoba, której dane dotyczą ma także prawo żądania od Administratora ograniczenia przetwarzania danych osobowych. Takie działanie może być zrealizowane przez Administratora w następujących przypadkach:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych i żąda ograniczenia przetwarzania na okres, w którym Administrator sprawdzi ich prawidłowość,

b) osoba, której dane dotyczą, stwierdzi, że jej dane osobowe są przetwarzane niezgodnie z prawem, lecz nie żąda ich usunięcia, żądając w zamian ograniczenia ich wykorzystania,

c) osoba, której dane dotyczą sprzeciwia się usunięciu danych przez Administratora, a w zamian domaga się ich ograniczonego przetwarzania przez Administratora, ponieważ uznaje, ze takie przetwarzanie będzie jej potrzebne do ustalenia, dochodzenia i obrony roszczeń,

d) osoba, której dane dotyczą zgłosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych, które odbywa się na podstawie prawnie uzasadnionego interesu Administratora; wówczas ograniczenie przetwarzania trwa do momentu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstawy sprzeciwu osoby, której dane dotyczą.

2. Jeżeli realizacja prawa do ograniczenia przetwarzania okaże się zasadna, to dane takie będą jedynie przechowywane. W przypadku konieczności podjęcia innych czynności na danych objętych ograniczeniem, Administrator wystąpi do osoby, której dane dotyczą o zgodę na przetwarzanie (ewentualnie dopuszcza się też przetwarzanie w celu ochrony roszczeń).

3. Jeżeli Administrator zdecyduje się odstąpić od ograniczenia przetwarzania, to poinformuje o takim działaniu osobę, która żądała ograniczenia. Do takiej czynności stosuje się schemat

działania, o którym mowa w § 1 niniejszej procedury.

§9

1. Osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe, jeżeli:
   a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz
   b) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego paragrafu pozostaje bez uszczerbku dla prawa do bycia zapomnianym.
4. Prawo omawiane w niniejszym paragrafie nie może niekorzystnie wpływać na prawa i wolności innych.

§10

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, opartego na prawnie uzasadnionych interesach realizowanych przez Administratora lub osobę trzecią.
2. Nadto osoba, której dane dotyczą może wnieść sprzeciw co do przetwarzania jej danych osobowych na potrzeby marketingu bezpośredniego, w dowolnym momencie, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
3. Sprzeciw może zostać wniesiony w dowolnej formie, a więc również w czasie rozmowy telefonicznej, pocztą elektroniczną, czy za pomocą faksu. Nie wymaga również uzasadnienia.

Załącznik 5

Procedura postępowania na wypadek incydentu ochrony danych osobowych

§1

1. W przypadku naruszenia danych osobowych (przykłady incydentów zawiera tabela) osoba, która stwierdziła takie naruszenie zgłasza je administratorowi.
2. Administrator danych, zgłasza takie naruszenie właściwemu organowi nadzorczemu, tj. Prezesowi Urzędu Ochrony Danych Osobowych.
3. Ustala się, zgodnie z zapisami RODO, że całość procedury zgłoszenia nie może przekroczyć 72 godzin od momentu stwierdzenia naruszenia. Jeżeli naruszenie zgłosi się po 72 godzinach, do takiego zgłoszenia należy załączyć wyjaśnienia, które opiszą powód opóźnienia.
4. Administrator sam określa wagę incydentu, a przede wszystkim to, czy naruszenie skutkuje ryzykiem naruszenia prawa lub wolności osoby fizycznej. W tym celu do rozpatrzenia każdego incydentu powołać należy komisję w składzie: wspólnicy (ewentualnie konsultant zewnętrzny), administrator (tj. właściciel organizacji) oraz osoba odpowiedzialna za obsługę systemów informatycznych – przy założeniu, że incydent nastąpił z użyciem systemów informatycznych (skład komisji może zostać rozszerzony, jeżeli organizacja uzna to za konieczne).
5. Jeżeli administrator stwierdzi naruszenie danych osobowych, co do których jest podmiotem przetwarzającym lub odbiorcą, to zgłasza takie naruszenia drugiemu administratorowi danych bez zbędnej zwłoki.
6. Zgłoszenie do organu nadzorczego zawiera:
    a) charakter naruszenia ochrony danych osobowych wraz ze wskazaniem kategorii i przybliżonej liczby osób, których dane dotyczą oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
    b) imię i nazwisko oraz dane kontaktowe osoby, która posiada szczegółowe informacje odnośnie incydentu, a organizacja wyznaczyła ją do załatwiania spraw związanych z ochroną danych osobowych,
    c) opis możliwych konsekwencji naruszenia danych osobowych,
    d) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach opis środków możliwych do podjęcia w celu minimalizacji skutków naruszenia.
7. Administrator prowadzi rejestr naruszeń zgodnie z zapisem art. 33 ust. 5 RODO.

§2

1. Ustala się, zgodnie z regulacjami RODO, że jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator, bez zbędnej zwłoki zawiadomi osoby, których dane dotyczą, o takim naruszeniu.
2. Zawiadomienie w miarę możliwości będzie realizowane drogą elektroniczną, tj. e-mail lub pocztą tradycyjną.
3. Zawiadomienie będzie sformułowane jasnym i prostym językiem, a ponadto będzie zawierało elementy, takie jak:
   a) imię i nazwisko oraz dane kontaktowe osoby, która posiada szczegółowe informacje odnośnie incydentu, a organizacja wyznaczyła ją do załatwiania spraw związanych z ochroną danych osobowych,
   b) opis możliwych konsekwencji naruszenia danych osobowych,
   c) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach opis środków możliwych do podjęcia w celu minimalizacji skutków naruszenia.
4. Przyjmuje się, że zawiadomienie nie będzie wymagane, gdy:
   a) ustali się, że administrator zastosował odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, tj. w szczególności środki, takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   c) wymagałoby to niewspółmiernie dużego wysiłku – wówczas administrator wyda publiczny komunikat lub zastosowany zostanie podobny środek; osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§3

Przykładowy wykaz incydentów dla badanego.

Incydenty spowodowane lub mające związek z czynnikiem ludzkim
Kradzież danych (m.in. kradzież zarówno w formie elektronicznej, kradzież dokumentów

papierowych, czy też fizycznych nośników danych lub stacji roboczych, włamanie do siedziby organizacji, tj. ingerencja w fizyczny obszar przetwarzania danych osobowych)
Błąd ludzki (m.in. pozostawienie danych – w formie dokumentu lub nośnika fizycznego – poza obszarem przetwarzania bez możliwości kontroli osób, które mają dostęp do tak pozostawionych danych osobowych, omyłkowe przesłanie korespondencji zawierającej dane osobowe do podmiotu nieuprawnionego, pozostawienie osoby nieupoważnionej w obrębie przetwarzania danych osobowych bez nadzoru)
Oszustwo (m.in. podwykonawca udostępnia dane osobowe podmiotom nieupoważnionym w celu osiągnięcia dodatkowych korzyści finansowych)
Incydent spowodowany zaniedbaniem (pozostawienie niezabezpieczonych dokumentów zawierających dane osobowe po godzinach pracy w miejscu, do którego mają dostęp osoby nieuprawnione do przetwarzania danych osobowych)
Incydent spowodowany zaniechaniem (m.in. wspólnik pomimo tego, że dysponuje odpowiednimi środkami technicznymi np. zamykanymi szafkami, nie korzysta z nich w celu zabezpieczenia danych osobowych)
Incydent spowodowany pojawieniem się osób nieupoważnionych w obszarze przetwarzania danych osobowych (np. kurier dostarczający przesyłki wskutek złego ustawienia monitora stacji roboczych ma wgląd do przetwarzanych danych osobowych i wykonuje zdjęcia ekranu, a następnie publikuje je w sieci Internet)
Incydenty spowodowane lub mające związek z czynnikiem technologicznym
Incydent spowodowany awarią sprzętu/brak zasilania (m.in. wskutek braku zasilania fizyczny obszar przetwarzania danych osobowych zostanie pozbawiony energii elektrycznej, a co za tym idzie urządzeń alarmowych, co ułatwia dokonanie kradzieży)
Incydent spowodowany wirusem (m.in. wspólnik instaluje na stacji roboczej samowolnie nieautoryzowane oprogramowanie, które zawiera wirusy)
Incydent spowodowany złośliwym oprogramowaniem (jw.)
Incydent spowodowany włamaniem do sieci lub do kont użytkowników stacji roboczych (m.in. wspólnik używa hasła do stacji roboczej, które składa się z jego imienia i nazwiska)
Utrata kopii zapasowych (m.in. kradzież niezabezpieczonej kopii zapasowej)

REJESTR INCYDENTÓW – WZÓR

Rejestr incydentów naruszenia danych osobowych						
Lp.	**Rodzaj incydentu wraz ze wskazaniem zbioru danych, którego dotyczy**	**Data zauważenia incydentu**	**Osoba zgłaszająca**	**Podjęte środki działania**	**Możliwość wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych (TAK/NIE)**	**Środki techniczne i organizacyjne, które miały za zadanie uniemożliwić powstania takiego incydentu**
1.						
2.						

Załącznik 6

Zbiór informacji na temat infrastruktury techniczno-informatycznej w badanym przedsiębiorstwie.

§1

1. Niniejsza instrukcja reguluje w szczególności:
   a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
   b) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
   c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
   d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
   e) sposób i miejsce przechowywania elektronicznych nośników informacji, zawierających dane osobowe oraz kopii zapasowych, o których mowa w podpunkcie powyższym,
   f) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
   g) sposób realizacji odnotowania informacji o odbiorcach, którym dane zostały udostępnione, a także o dacie i zakresie tego udostępnienia,
   h) procedurę wykonywania przeglądów i konserwacji systemu informatycznego oraz nośników informacji służących do przetwarzania danych osobowych.
2. Całość regulacji niniejszej instrukcji określa poziom bezpieczeństwa przetwarzania danych osobowych.
3. Administrator dopuszcza do przetwarzania danych osobowych tylko upoważnione osoby, tj. użytkowników systemu (wspólnicy oraz ew. podwykonawcy).
4. Do przetwarzania danych osobowych dopuszcza się elementy składowe systemu informatycznego, które przede wszystkim:
   a) pochodzą z pewnych źródeł i zapewniają wysoki standard pracy,
   b) są wyposażone w mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika,
   c) są wyposażone w mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych,
   d) są wyposażone w mechanizmy pozwalające na wykrycie próby nieautoryzowanego dostępu do systemu informatycznego, czy też przekroczenie przyznanych uprawnień podczas przetwarzania danych w systemie,

e) umożliwiają odnotowanie pierwszego wprowadzenia danych do systemu.

5. Administrator oświadcza, że:
   a) nie udostępniania dostępu do stacji roboczych osobom nieupoważnionym oraz ujawniania haseł ww. osobom,
   b) nie korzysta z oprogramowania nielicencjonowanego,
   c) nie umożliwiania dostępu do zasobów wewnętrznych sieci informatycznej oraz sieci internetowej osobom nieupoważnionym.

§2

1. Pod pojęciem nadania uprawnień do przetwarzania danych osobowych w systemach informatycznych należy rozumieć nadanie użytkownikowi systemu unikalnego identyfikatora i hasła pozwalającego na uwierzytelnianie w systemie oraz aplikacjach i rozpoczęcie pracy.
2. Przydzielenie użytkownikowi systemu przedmiotowych uprawnień następuje poprzez nadanie mu loginu oraz hasła tymczasowego, które musi zostać zmienione po pierwszym zalogowaniu.
3. O odebraniu uprawnień do przetwarzania danych osobowych w systemie informatycznym decyduje administrator danych osobowych. Blokada konta użytkownika jest równoznaczna z pozbawieniem użytkownika systemu możliwości zalogowania się do wszystkich aplikacji i systemu informatycznego występującego w organizacji.

§3

1. Stosowanymi w organizacji środkami uwierzytelnienia są identyfikator użytkownika (login) oraz hasło dostępu.
2. Wymienione w poprzednim paragrafie hasła tymczasowe przekazywane są użytkownikowi systemu w formie pisemnej lub elektronicznej przez administratora (sytuacje, w których nadaje się hasło tymczasowe, oprócz zakładania nowego konta, to także: utrata, zgubienie lub zapomnienie hasła oraz istotna zmiana oprogramowania lub sprzętu, która wymusza zmianę hasła).
3. Tryb przekazania hasła tymczasowego powinien wykluczyć dostęp do hasła osób trzecich.
4. Po otrzymaniu hasła tymczasowego użytkownik systemu, tak jak opisano to wyżej, po pierwszym zalogowaniu zmienia hasło tymczasowe na hasło stałe.
5. W stosunku do haseł stałych ustalanych przez użytkowników stacji roboczych, systemów i aplikacji ustanawia się następujące wytyczne:
   a) hasło nie może składać się z imienia lub nazwiska danego użytkownika systemu,

b) hasło musi składać się z co najmniej 8 znaków, a ponadto zawierać duże i małe litery, a także cyfry lub znaki interpunkcyjne lub specjalne,
c) hasła nie może składać się z ciągu takich samych znaków, liter lub cyfr,
d) hasło nie może pokrywać się z identyfikatorem użytkownika,
e) hasło nie powinno być powielane, tj. nie powinno się stosować ponownie hasła, które zostało zmienione w przeszłości,
f) hasło stało powinno być zmieniane 6 miesięcy lub w uzasadnionym przypadku, tj. np. gdy dostało się ono w posiadanie osoby nieuprawnionej,
g) hasło, w momencie wpisywania, nie może być wyświetlane na ekranie.

6. Użytkownik systemu jest zobligowany do utrzymania hasła w tajemnicy. W przypadku wystąpienia uzasadnionych podejrzeń, że hasło przestało być bezpieczne, użytkownik systemu informuje natychmiast administratora danych osobowych, a ponadto, tak jak zaznaczono powyżej, dokonuje zmiany hasła.
7. Identyfikator użytkownika nie może być zmieniany. Po usunięciu danego identyfikatora z systemu informatycznego niedopuszczalne jest, by został on ponownie nadany innemu użytkownikowi systemu.

§4

Rozpoczęci, zakończenie i zawieszenie pracy w systemie informatycznym następuje wg schematu:

<u>Rozpoczęcie pracy</u>

Przed uruchomieniem stacji użytkownik systemu jest zobligowany do sprawdzenia, czy nie występują oznaki sugerujące zewnętrzną ingerencję osoby nieupoważnionej w stację roboczą. W przypadku stwierdzenia takich naruszeń, użytkownik systemu powinien odstąpić od dalszych czynności i niezwłocznie poinformować administratora danych.

Rozpoczęcie pracy przez użytkownika systemu informatycznego służącego do przetwarzania danych osobowych każdorazowo rozpoczyna się od uruchomienia stacji roboczej, wybrania właściwego identyfikatora oraz wpisania hasła dostępu.

<u>Zawieszenie pracy</u>

Użytkownik systemu, który czasowo zawiesza swoją pracę przy przetwarzaniu danych osobowych w systemie informatycznym, musi każdorazowo wylogować się z systemu poprzez wciśnięcie kombinacji klawiszy: WinKey/Start + L. Sugeruje się, by użytkownik systemu przed

wylogowaniem zakończył pracę poszczególnych aplikacji i zapisał wprowadzone zmiany.

Ponadto, użytkownicy systemu informatycznego zobligowani są do zabezpieczenia treści widocznych na ekranie monitora poprzez stosowanie wygaszacza ekranu.

Zakończenie pracy

Zakończenie pracy przez użytkownika systemu oznacza zamknięcie wszystkich aplikacji i zapisanie wprowadzonych zmian. Następnie użytkownik wylogowuje się z systemu i wyłącza stację roboczą. Użytkownik systemu pozostaje przy stacji roboczej do momentu zakończenia procesu wyłączania, a następnie dokonuje odłączenia komputera od sieci zasilającej.

§5

1. Za wykonanie kopii zapasowych odpowiedzialny jest podwykonawca działający na zlecenie administratora danych.
2. Procesor kontroluje kopie zapasowe, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonej stacji roboczej. Odtworzenie testowe poszczególnych kopii wykonuje się co najmniej raz w miesiącu.
3. Pełna kopia zapasowa baz danych i plików wykonywana jest codziennie.
4. Nośnik danych zawierający kopię zapasową jest zabezpieczony przez procesora i przechowywany w jego siedzibie, w wydzielonym pomieszczeniu, do którego dostęp mają tylko podmiotu upoważnione.

§6

1. Kopia zapasowa jest przechowywana w ww. miejscu wyznaczonym przez administratora danych osobowych (siedziba procesora). Miejsce to zapewnia bezpieczeństwo przechowania kopii.
2. Elektroniczne nośniki informacji, które zawierają dane osobowe są przechowywane w obszarze przetwarzania danych osobowych, o którym mowa Polityce bezpieczeństwa w zakresie przetwarzania danych osobowych, tj. w wydzielonych i zabezpieczonych pomieszczeniach, a także w zamykanych szafach lub zamykanych szufladach.
3. Okres przechowywania danych osobowych na elektronicznym nośniki uzależnia się od użyteczności, celu lub obowiązku prawnego kształtującego proces przetwarzania konkretnych danych osobowych.

§7

1. W związku z podłączeniem stacji roboczej, na której przetwarzane są dane osobowe, do sieci Internet, administrator podjął szereg środków, które zabezpieczają system informatyczny przed zagrożeniami, takimi jak m.in. oprogramowanie zawierające złośliwy kod (wirusy), tzw. konie trojańskie, czy też ataki hakerów.
2. Podstawowym sposobem zabezpieczenia przed jest zastosowanie na stacji roboczej oprogramowania antywirusowego oraz zapory sieciowej systemu operacyjnego Windows. Oprogramowanie antywirusowe jest cykliczne i automatycznie aktualizowane.
3. Użytkownicy systemu nie stosują nieautoryzowanego oprogramowania i aplikacji.

§8

1. Systemy oraz nośniki służące do przetwarzania danych są konserwowane przez wyspecjalizowany podmiot zewnętrzny, z którym administrator zawarł stosowne umowy.
2. Każda stacja robocza jest kontrolowana minimum jeden raz w roku – dot. kwestii hardware (wyjątkiem są stacje robocze objęte gwarancją sprzedawcy/dostawcy – wówczas przeglądy mogą być dokonywane rzadziej).
3. Wszystkie nieprawidłowości stwierdzone w trakcie przeglądów są natychmiast usuwane.
4. Usuwanie danych osobowych utrwalonych na nośnikach elektronicznych następuje poprzez działanie wyspecjalizowanego podmiotu zewnętrznego i kończy się wydaniem stosownego potwierdzenia wykonania operacji.
5. Za prawidłowość przeprowadzenia przeglądów i konserwacji odpowiada administrator.

Załącznik 7

Procedura czystego biurka i ekranu

§1

1. Osoby przetwarzające dane nie powinny pozostawiać dokumentów zawierających dane

osobowe (a także inne istotne dla organizacji dane i informacje) na biurku podczas dłuższej nieobecności przy stanowisku pracy.

2. Powyższe kroki powinny być przede wszystkim dochowane, gdy w obszarze przetwarzania danych osobowych pojawia się osoba nieupoważniona.
3. Zakańczając pracę, wspólnik powinien schować całą dokumentację papierową zawierającą dane osobowe (a także tę, która zawiera inne istotne dla organizacji dane i informacje) do zamykanych szaf i szuflad, stosując w ten sposób techniczne środki zabezpieczenia przetwarzania danych osobowych.
4. Powyższe zapisy mają także zastosowanie do przenośnych fizycznych nośników danych.

§2

1. Osoby przetwarzające muszą stosować wygaszacze ekranu i procedurę wylogowania z systemu operacyjnego zgodnie z zapisami Instrukcji zarządzania systemem informatycznym w odniesieniu do przetwarzania danych osobowych.
2. Ekrany stacji roboczych powinny być, w miarę możliwości, ustawione tak, by w momencie pojawienia się osób nieupoważnionych w pomieszczeniach biurowych, osoby te nie mogły widzieć treści wyświetlanych na ekranach stacji roboczych (mowa tu przede wszystkim o klientach, interesantach, czy też np. kurierze).
3. W przypadku zakończenia pracy przy stacji roboczej należy podjąć kroki, które określone zostały w Instrukcji zarządzania systemem informatycznym w odniesieniu do przetwarzania danych osobowych.

§3

1. Po zakończeniu pracy pomieszczenia biurowe należy zamknąć, a klucze zabezpieczyć.
2. Integralnym elementem procedury utrzymania czystego biurka i ekranu jest także proces niszczenia danych. Dlatego wspólnicy podczas przetwarzania danych osobowych powinni stosować niszczarki mechaniczne lub powinni segregować dokumenty, w ten sposób, by odseparować ew. dokumenty przeznaczone do niszczenia przez podmiot wyspecjalizowany, tj. firmę zewnętrzną.