Polityka Ochrony Danych Osobowych
w spółce Modlin spółka z ograniczoną odpowiedzialnością
z siedzibą w Poznaniu

Spis treści

I. Ogólne zasady przetwarzania danych w Spółce

1. Informacje ogólne. Podstawy prawne.

1.1. Spółka opracowuje i zatwierdza Politykę na podstawie przepisów prawnych dotyczących ochrony danych osobowych, w szczególności na podstawie RODO.

1.2. Celem Polityki jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczać dane osobowe, a zatem organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych oraz edukowanie użytkowników systemu ochrony danych osobowych. Polityka określa zadania związane z zachowaniem poufności, integralności oraz rozliczalności danych osobowych oraz innych zasad przetwarzania danych osobowych wymaganych przepisami prawa.

1.3. Definicje

a) **[ADO]** – administrator danych osobowych.
b) **[dane osobowe]** – dane osobowe w rozumieniu RODO, przetwarzane przez Spółkę.
c) **[podmiot danych]** – osoba, której dotyczą przetwarzane dane osobowe.
d) **[Osoba upoważniona]** – osoba posiadająca nadane uprawnienia do przetwarzania Danych Osobowych i wpisana na listę osób upoważnionych do przetwarzania Danych Osobowych.
e) **[Polityka]** – niniejsza Polityka Ochrony Danych Osobowych.
f) **[Przepisy o ochronie danych osobowych]** – wszelkie powszechnie obowiązujące w Polsce akty prawne dotyczące przetwarzania Danych osobowych, w tym w szczególności RODO.
g) **[Przetwarzanie danych osobowych]** – wykonywanie jakichkolwiek operacji na Danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
h) **[RODO]** – 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).
i) **[Spółka]** – spółka pod firmą City 88 spółka z ograniczoną odpowiedzialnością sp.k. z siedzibą w Poznaniu (60-751) przy ul. Wyspiańskiego 26, KRS 0000802735.
j) **[System informatyczny]** – zespół współpracujących ze sobą urządzeń informatycznych i programów komputerowych, wykorzystywanych do przechowywania i zapewniania dostępu do informatycznej bazy danych zawierający Dane osobowe.
k) **[naruszenie ochrony danych osobowych]** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności: a) naruszenie bezpieczeństwa Systemów

informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach; b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym; c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony; d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia; e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania; f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych; g) naruszenie praw osób, których dane są przetwarzane

l) **IOD** – Inspektor Ochrony Danych Osobowych powołany w Spółce, o ile został powołany.

1.4. Podstawy prawne w zakresie Polityki stanowią:

a) RODO,
b) ustawa o ochronie danych osobowych,
c) inne przepisy szczególne dotyczące danych osobowych.

1.5. Polityka ma zastosowanie do wszystkich:

a) danych osobowych przetwarzanych przez Spółkę zarówno w przypadku, gdy jest administratorem, jak i w sytuacji, gdy przetwarza dane powierzone na podstawie umów powierzenia przetwarzania danych osobowych,
b) nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe, lokalizacji - budynków i pomieszczeń Spółki, w których są lub będą przetwarzane dane osobowe,
c) osób stanowiących personel Spółki,
d) innych osób mających dostęp do danych osobowych.

1.5.1. Osoby stanowiące personel Spółki oraz wszystkie inne mające dostęp do danych osobowych zobowiązane są do przestrzegania postanowień Polityki.

1.5.2. Polityka powinna być poddawana bieżącej aktualizacji, ale nie rzadziej niż raz do roku.

1.6. Spółka przetwarza dane osobowe zgodnie z zasadami przetwarzania danych osobowych określonymi w szczególności w art. 5 RODO. Spółka przetwarzając dane osobowe działa według następujących zasad:

1.6.1. zasady legalności (zgodności z prawem), rzetelności i przejrzystości – dane osobowe przetwarzane są w ramach Spółki zgodnie z prawem (w szczególności z uwzględnieniem podstawy prawnej przetwarzania), rzetelnie i w sposób przejrzysty dla podmiotów danych. Spółka realizuje w pełni obowiązki informacyjne wobec podmiotów danych wynikające z przepisów prawa, w tym w szczególności informuje podmioty danych o prowadzeniu operacji przetwarzania dotyczących ich danych i celach przetwarzania. Wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych są łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem;

1.6.2. zasady ograniczenia celu przetwarzania – dane osobowe zbierane są w ramach Spółki wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach, o których informowane są podmioty danych oraz nie są przetwarzane dalej w sposób niezgodny z tymi celami;

1.6.3. zasady minimalizacji danych – Spółka przetwarza wyłącznie dane osobowe adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Dane osobowe przetwarzane są tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami;

1.6.4. zasady prawidłowości przetwarzania – Spółka zapewnia, że dane osobowe przez nią przetwarzane są prawidłowe i w razie potrzeby uaktualniane; Spółka podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

1.6.5. zasady ograniczenia przechowywania – Spółka zapewnia, że dane osobowe przechowywane są w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Spółka określa każdorazowo okres retencji danych osobowych – szczegółowe okresy retencji wskazane są w ramach rejestru czynności. Dane osobowe mogą być przechowywane przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że Spółka zobowiązana będzie wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą;

1.6.6. zasady integralności i poufności – dane osobowe przetwarzane są przez Spółkę 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 określonych szczegółowo w niniejszej Polityce.

1.7. Obowiązki Spółki jako administratora danych osobowych (ADO):

1.7.1. Podstawowym obowiązkiem ADO jest dbanie o to, aby przetwarzanie odbywało się zgodnie z obowiązującymi przepisami, w tym w szczególności w zgodnie z RODO i z zasadami, o których mowa w pkt. 3.2. powyżej. W tym celu, ma ADO wdraża odpowiednie i skuteczne środki techniczne i organizacyjne:

a) mają one zapewniać najwyższy znany i możliwy w chwili przetwarzania danych, poziom ochrony;
b) nie może być to czynność jednorazowa, środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
c) dokonuje tego, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
d) jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te, obejmują wdrożenie przez ADO odpowiednich polityk ochrony danych.

Środki techniczne i organizacyjne wdrożone przez ADO określa szczegółowo niniejsza Polityka.

1.7.2. ADO powołuje obligatoryjnie IOD jeśli:

a) główna działalność ADO lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę;
b) główna działalność ADO lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, czyli danych wrażliwych oraz danych dotyczących wyroków skazujących i naruszeń prawa.

1.7.3. ADO dopuszcza do przetwarzania danych osobowych wyłącznie Osoby upoważnione, tj. przeszkolone i posiadające stosowne upoważnienia lub polecenia.

1.7.4. ADO przekazuje podmiotom danych wszystkie informacje wymagane przepisami prawa, w tym w szczególności informacje o prowadzeniu operacji przetwarzania i jego celach oraz uprawnieniach podmiotu danych. ADO informuje podmioty danych również o fakcie profilowania oraz konsekwencjach profilowania i prawie złożenia sprzeciwu. W ramach obowiązku informacyjnego, ADO:

a) prowadzi komunikację z podmiotem danych i przekazuje mu informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny,
b) ułatwia podmiotom danych wykonywanie ich praw,
c) nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie,
d) weryfikuje tożsamość osób wnoszących żądania udzielenia informacji.

1.7.5. ADO, w szczególności poprzez zastosowanie odpowiednich narzędzi, w tym przystosowanie Systemu informacyjnego, realizuje uprawnienia podmiotów danych do:

a) przenoszenia danych,
b) dostępu do danych,
c) sprostowania i uzupełnienia danych,
d) usunięcia danych (prawo do bycia zapomnianym),
e) ograniczenia przetwarzania,
f) przenoszenia danych,
g) sprzeciwu,
h) niepodlegania profilowaniu.

Realizując prawa podmiotów danych ADO w szczególności:

a) potwierdza czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli ma to miejsce, udziela wskazanych przepisami prawa informacji;
b) ułatwia podmiotowi danych wykonywanie jego praw;
c) informuje podmiot danych o działaniach jakie podjął, w związku z jego żądaniami opartymi o wykonywanie jego praw;
d) uzasadnia odrzucenie żądania podmiotu danych i poucza go o prawie skargi;
e) umożliwia dostęp do danych podmiotu danych;
f) dokonuje sprostowania i uzupełniane danych;
g) usuwa dane;
h) ogranicza przetwarzanie danych;
i) powiadamia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu ich przetwarzania;

j) dokonuje przenoszenia danych;
k) zaprzestaje stosowania profilowania.

1.7.6. ADO uwzględnia zasady ochrony danych osobowych już w fazie projektowania rozwiązań (zasada privacy by design). ADO już na początkowym etapie prac nad przyjmowanymi rozwiązaniami zarówno w ramach procesów biznesowych, jak i w ramach rozwiązań Systemu informatycznego, bierze pod uwagę kwestię ewentualnego przetwarzania danych osobowych w ramach danego projektu/towaru/usługi, a także planuje zastosowanie adekwatnych do ryzyka środków organizacyjnych i technicznych. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, ADO – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa podmiotów danych. Zasady poszanowania prywatności i ochrony danych osobowych wpisano w architekturę Systemu informatycznego oraz procesy biznesowe obsługiwane przez ten system i stosowane są przy projektowaniu każdego nowego rozwiązania przyjętego w Spółki. Wszyscy pracownicy, w szczególności zaś pracownicy odpowiedzialni z kształt Systemu informatycznego, zobowiązani są do analizowania każdego nowego rozwiązania przez pryzmat zasady privacy by design.

1.7.7. ADO wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (zasada privacy by default – domyślna ochrony danych). ADO 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. W tym celu ADO stosuje zasadę minimalizacji zakresu przetwarzania danych osobowych i zasadę, zgodnie z którą zmiana i rozszerzenie celu przetwarzania następuje tylko na podstawie zgody lub przepisów (w tym art. 6 ust. 4 RODO). ADO przyjął ograniczenie okresu przetwarzani danych osobowych w taki sposób, by okresy retencji określone w Polityce retencji znajdującej się w rozdziale V niniejszej Polityki były możliwie najkrótsze, tj. adekwatne do celów przetwarzani danych osobowych. Przy czym okresy retencji ustalane są przez RODO z uwzględnieniem realizacji celów, dla których przetwarzane są dane osobowe, okresu przedawnienia ewentualnych roszczeń wynikających z ww. celów oraz ewentualnych wymogów prawnych w zakresie przechowywania danych osobowych. Nadto, w ramach zasady privacy by default ADO zapewnia, że dane osobowe udostępniane są tylko na podstawie przepisów prawa lub zgody podmiotu danych i tylko tam, gdzie to niezbędne, dla realizacji celu, świadczenia usługi itp. Dane osobowe nie są upubliczniane osobom nieuprawnionym.

1.7.8. ADO powierza dane osobowe innym podmiotom (podmiotom przetwarzającym) wyłącznie na podstawie umowy powierzenia przetwarzania zgodnej z obowiązującymi przepisami prawa, w szczególności z RODO, w ramach której zobowiązuje podmiot przetwarzający do zapewnienia stosownej ochrony danych osobowych. Rodzaj podmiotów, którym ADO powierzył przetwarzanie danych osobowych wskazano w Rejestrze czynności przetwarzania.

1.7.9. ADO, jako podmiot przetwarzający dane osobowe powierzone mu przez innego administratora danych osobowych, przestrzega obowiązków określonych w umowie powierzenia przetwarzania. ADO prowadzi rejestr kategorii przetwarzania.

1.7.10. ADO dba i nadzoruje, by udostępnianie i powierzanie do przetwarzania danych osobowych innym podmiotom odbywało się zgodnie z obowiązującymi przepisami prawa i poszanowaniem praw podmiotów danych.

1.7.11. ADO prowadzi dokumentację w zakresie ochrony danych osobowych wymaganą przepisami prawa, w tym w szczególności: rejestr czynności przetwarzania (a działając jako podmiot przetwarzający – rejestr kategorii przetwarzania), dokumentację wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, skutków naruszenia oraz podjętych działań zaradczych, dokumentację oceny skutków dla ochrony danych, dokumentację uprzednich konsultacji z organem nadzorczym.

1.7.12. ADO zobowiązany jest także do:

a) realizacji obowiązku notyfikacyjnego naruszenia ochrony danych osobowych organowi nadzorczemu o zakresie informacyjnym określonym w rozdziale III Polityki,
b) zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych o zakresie informacyjnym określonego w rozdziale IV Polityki.

1.8. Inspektor Ochrony Danych Osobowych (IOD). Wszelkie postanowienia niniejszego dokumentu dotyczące IOD mają zastosowanie wyłącznie jeśli w Spółki powołany zostanie IOD. W chwili wejścia w życie niniejszego dokumentu, Spółka nie miała prawnego obowiązku powołania IOD i IOD nie został powołany.

1.8.1. Status IOD

1.8.1.1. W przypadku powołania IOD Spółka zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
1.8.1.2. Spółka wspiera IOD w wypełnianiu przez niego zadań, o których mowa w pkt. 3.4.2. poniżej, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
1.8.1.3. Spółka zapewnia, by IOD nie otrzymywał instrukcji dotyczących wykonywania jego zadań. Spółka nie jest uprawniona do karania IOD za wypełnianie swoich zadań.
1.8.1.4. IOD bezpośrednio podlega najwyższemu kierownictwu (zarządowi) Spółki.

1.8.1.5. Podmioty danych mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
1.8.1.6. IOD jest zobowiązany do zachowania poufności odnośnie do informacji pozyskanych przez niego w ramach wykonywanych zadań.
1.8.1.7. IOD może wykonywać inne zadania i obowiązki, a Spółka zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

1.8.2. IOD zobowiązany jest do:

a) informowania Spółki, podmiotów przetwarzających dane osobowe powierzone przez Spółkę oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów o ochronie danych i doradzanie im w tej sprawie;
b) monitorowania przestrzegania obowiązujących przepisów o ochronie danych oraz niniejszej Polityki, jak również innych dokumentów w Spółki lub przez podmiot przetwarzający w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
d) współpracy z organem nadzorczym;
e) pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

1.8.3. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

1.9. Obowiązki osoby odpowiedzialnej za systemy informatyczne służące do przetwarzania danych osobowych (ASI) obejmują:

1.9.1. Wdrażanie zasad ochrony danych osobowych określonych w Polityce i dokumentach
z nią związanych;

1.9.2. Zapewnienie prawidłowej eksploatacji systemu, zgodnie z celami przetwarzania danych osobowych;

1.9.3. Realizację wytycznych Spółki i IOD w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem środków informatycznych;

1.9.4. Informowanie Spółki i IOD o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych;

1.9.5. Szkolenie użytkowników systemu informatycznego w zakresie procedur i instrukcji zapewniających ochronę danych osobowych;

1.9.6. Wyjaśnianie - wspólnie z IOD - wszystkich zgłoszonych nieprawidłowości i incydentów;

1.9.7. W szczególności bieżące obowiązki ASI obejmują:
a) przegląd, konserwację oraz uaktualnienie systemów służących do przetwarzania danych,
b) kontrolę bezpieczeństwa w sieci komputerowej,
c) nadawanie, zmiany lub pozbawianie uprawnień dostępu do systemu informatycznego,
d) nadzorowanie ochrony antywirusowej,
e) wykonywanie kopii bezpieczeństwa.

1.9.8. ASI sprawuje nadzór nad wykonaniem zadań lub wykonuje je samodzielnie.

1.10. Obowiązki kierowników działów w ramach Spółki obejmują:

1.10.1. Wdrażanie w ramach podległego danemu kierownikowi działu zasad ochrony danych osobowych określonych w Polityce i dokumentach z nią związanych;

1.10.2. Zapewnienie przestrzeganie przez pracowników podległego kierownikowi działu zasad ochrony danych osobowych określonych w Polityce i dokumentach z nią związanych;

1.10.3. Realizację wytycznych Spółki i IOD w zakresie ochrony danych osobowych;

1.10.4. Informowanie Spółki i IOD o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych;

1.10.5. Informowanie Spółki i IOD o naruszeniach ochrony danych osobowych zgodnie z treścią rozdziału III Polityki.

1.11. Zasady dopuszczenia do przetwarzania danych osobowych

1.11.1. Przetwarzać dane osobowe mogą wyłącznie osoby posiadające do tego pisemne upoważnienie udzielone im przez Spółkę. Każda osoba działająca z upoważnienia Spółki i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie Spółki, chyba że wymagają tego przepisy prawa. Wzór upoważnienia stanowi załącznik nr 1 do Polityki.

1.11.2. Spółka może udzielić IOD pełnomocnictwa do wydawania upoważnień do przetwarzania danych osobowych w imieniu Spółki.

1.11.3. Spółka prowadzi listę osób upoważnionych do przetwarzania danych osobowych oraz aktualizuje ją na bieżąco, a także przechowuje upoważnienia, o których mowa w pkt. 3.7.1.

1.11.4. Każda osoba upoważniona przez Spółkę do przetwarzania danych osobowych jest zobowiązana do utrzymania w tajemnicy danych osobowych, do których ma dostęp (zobowiązanie do zachowania poufności), a w szczególności:
   a) zabronione jest zapoznawanie osób trzecich z treścią danych osobowych;
   b) zabronione jest przekazywanie osobom trzecim dokumentów i innych nośników informacji, na których utrwalone zostały dane osobowe.

1.11.5. Osoby upoważnione mogą wykorzystywać dane osobowe wyłącznie zgodnie z celem, dla którego te dane zostały zebrane.

1.11.6. W przypadku przetwarzania danych osobowych z wykorzystaniem Systemu informatycznego, każdej z osób upoważnionych nadaje się indywidualne uprawnienie do przetwarzania danych osobowych zgodnie z pkt. 2.2..

II. Środki techniczne i organizacyjne służące ochronie danych (art. 32 RODO)

2. Informacje ogólne

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, ADO wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2.1. Uprawnienia do obsługi Systemu informatycznego

2.1.1. Osoba odpowiedzialna za nadawanie uprawnień to ASI, Piotr Utrajczak.
2.1.2. Procedury nadawania, zmiany i odbierania uprawnień do przetwarzania danych osobowych w systemie informatycznym

2.1.2.1. Procedura nadawania uprawnień

- Osoba nadająca uprawnienie, po nadaniu dostępu, przekazuje użytkownikowi login drogą mailową, natomiast hasło jest przesyłane telefonicznie przez wiadomość sms.
- Użytkownik-pracownik może zdecydować o sposobie uwierzytelniania się w Systemie informatycznym. Uwierzytelnianie jest możliwe w oparciu o numer IP lub login oraz hasło.
- Login użytkownika jest przekazywany drogą mailową, natomiast hasło jest przesyłane telefonicznie przez wiadomość sms.

— Użytkownik przed rozpoczęciem pracy w systemie powinien mieć możliwość zmiany hasła na nowe.

2.1.2.2. Procedura zmiany uprawnień

Procedura zmiany uprawnień odbywa się w analogiczny sposób jak procedura nadawania uprawnień.

2.1.2.3. Procedura odbierania uprawnień

Odbiór uprawnień następuje m.in. gdy zajdzie jedna z poniższych sytuacji:

a) ustanie stosunku pracy lub zakończenie współpracy na podstawie umowy cywilnoprawnej,
b) zmiana zakresu obowiązków,
c) uzasadnione ryzyko nadużycia.

Za odbiór uprawnień do Systemu informatycznego odpowiada osoba odpowiedzialna za nadawanie uprawnień dla poszczególnych systemów.

2.1.3. Uprawnienia obejmują indywidualną, niepowtarzalną nazwę użytkownika (login) oraz hasło składające się z co najmniej ośmiu niepowtarzalnych znaków, w tym małych i wielkich liter oraz cyfr lub znaków specjalnych. Okres ważności hasła wynosi 180 dni. System informatyczny automatycznie wymusi zmianę hasła z upływem tego terminu. System informatyczny rejestruje każdą nieudaną próbę wprowadzenia hasła dla danego identyfikatora użytkownika. ADO lub upoważniona osoba blokuje dostęp do Systemu informatycznego dla danej nazwy użytkownika w przypadku powzięcia informacji, iż osoby postronne mogły wejść w posiadanie nazwy użytkownika oraz hasła. W takim przypadku nadawane jest nowe hasło, bądź nowa nazwa użytkownika wraz z nowym hasłem. W przypadku, gdy użytkownik zapomni przydzielonego mu hasła, informuje o tym niezwłocznie ADO.

2.1.4. Przed przystąpieniem do pracy w Systemie informatycznym, bezpośrednio, bądź za pośrednictwem stacji roboczej, Osoba upoważniona:

a) loguje się do Systemu informatycznego za pomocą nadanej nazwy użytkownika oraz hasła;
b) uruchamia aplikację umożliwiającą dostęp do danych osobowych.

2.1.5. Hasło należy wprowadzać w taki sposób, aby uniemożliwić zapoznanie się z nim osobom nieupoważnionym. Podczas przerwy w pracy z Systemem informatycznym, Osoba upoważniona zobowiązana jest wylogować się z systemu, tak aby System informatyczny był niedostępny w czasie przerwy w pracy dla osób nieuprawnionych. Kończąc pracę z Systemem informatycznym należy się wylogować i następnie zamknąć aplikację umożliwiającą dostęp do danych osobowych.

2.1.6. Osoba upoważniona korzystająca z komputera przenośny umożliwiającego dostęp do danych osobowych, zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym w szczególności obowiązana jest stosować środki ochrony kryptograficznej przetwarzanych danych osobowych.

2.1.7. ADO zapewnia, że System informatyczny rejestruje dla każdej z Osób upoważnionych:

a) operacje wykonywane na przetwarzanych danych osobowych;
b) przesyłanie danych osobowych pomiędzy użytkownikami oraz do obiorców;

c) nieudane próby dostępu do Systemu informatycznego;
d) błędy w działaniu Systemu informatycznego podczas pracy danej Osoby upoważnionej.

2.1.8. Zapis działań Osoby upoważnionej uwzględnia: identyfikator użytkownika, datę i czas, w jakim zdarzenie miało miejsce; identyfikator stacji roboczej oraz rodzaj zdarzenia.

2.2. System informatyczny zapewnia stosowanie pseudonimizacji oraz szyfrowania danych osobowych jako jednego ze środków ochrony danych osobowych poprzez BitLocker, VeraCrypt, TLS oraz SSL.

2.3. System zapewnia poufność, integralność, dostępność i odporność Systemu informatycznego w zakresie przetwarzania danych osobowych.

2.3.1. Kierownik jednostki organizacyjnej lub inna upoważniona osoba tworzy lub nadzoruje proces tworzenia kopii bezpieczeństwa baz danych zawierających dane osobowe oraz oprogramowania służącego do ich przetwarzania. Kopie bezpieczeństwa wykonywane są nie rzadziej niż raz dziennie. Kopie bezpieczeństwa przechowywane są w taki sposób, aby osoby nieupoważnione nie mogły uzyskać do nich dostępu. Okres przechowywania kopii bezpieczeństwa wynosi maksymalnie 180 dni od dnia jej sporządzenia. Jeżeli kopia bezpieczeństwa była przechowywana na nośniku zewnętrznym, po upływie okresu przechowywania kopii bezpieczeństwa, wszelkie informacje przechowywane na nośniku zostaną usunięte np. poprzez fizyczne zniszczenie nośnika lub w inny sposób, tak aby niemożliwy był odczyt danych, które się na nim znajdowały.

2.3.2. Dane osobowe zapisane na elektronicznych nośnikach informacji (dysk twardy, płyta CD, DVD, dyskietka, pendrive lub inne) mogą być wynoszone poza obszar przeznaczony do przetwarzania danych osobowych wyłącznie po ich zabezpieczeniu zapewniającym poufność i integralność zawartych na nich danych, realizowanym w szczególności poprzez zabezpieczenie dostępu do danych osobowych utrwalonych na nośniku za pomocą hasła składającego się z co najmniej ośmiu niepowtarzalnych znaków, w tym małych i wielkich liter oraz cyfr lub znaków specjalnych. Przenośne nośniki informacji przechowywane są w pomieszczeniu znajdującym się w obszarze przetwarzania danych osobowych w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, w szczególności w szafie zamykanej na klucz. Usunięcie danych z elektronicznego nośnika informacji polega na fizycznym zniszczeniu nośnika z zastrzeżeniem zdania następnego. Usunięcie danych zapisanych na elektronicznych nośnikach informacji, których zniszczenie jest ekonomicznie nieuzasadnione (dysk twardy, pendrive), polega na ich wykasowaniu w taki sposób, aby nie można było ich odzyskać.

2.3.3. W przypadku zaistnienia konieczności wykonania wydruku z Systemu informatycznego zawierającego dane osobowe, z wydrukami należy postępować w sposób właściwy danych osobowych w postaci papierowej (nieelektronicznej), w tym w szczególności należy je przechowywać w sposób uniemożliwiający zapoznanie się z nimi osobom postronnym, np. w szafie zamykanej na klucz. Wydruki podlegają zniszczeniu po ich wykorzystaniu zgodnie z celem, dla którego zostały wykonane. Wydruki należy niszczyć za pomocą urządzenia do niszczenia dokumentów.

2.3.4. System informatyczny podłączony do sieci publicznej (np. Internet) chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych

zabezpieczeń (np. firewall). System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:

l.p.	Obszar chroniony	Rodzaj ochrony	Typ
1.	Stacje robocze	Uwierzytelnianie oprogramowanie antywirusowe	Login i hasło Eset Antivirus
2.	Sieć wewnętrzna	Firewall sprzętowy, Vlany	Cisco
3	Poczta e-mail	szyfrowanie	Tsl
4.	Serwery	Szyfrowanie Antywirus	Bitlocker Eset smart security

2.3.5. System informatyczny jest automatycznie skanowany. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy. W przypadku wykrycia wirusa należy:

a) uruchomić program antywirusowy i skontrolować użytkowany system,
b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego. Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
a) zakończyć pracę w systemie komputerowym,
b) odłączyć zainfekowany komputer od sieci,
c) powiadomić o zaistniałej sytuacji ADO lub kierownika jednostki organizacyjnej.

2.3.6. W przypadku zastosowania zabezpieczeń logicznych, obejmują one co najmniej:

a) kontrolę przepływu informacji pomiędzy Systemem informatycznym a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i Systemu informatycznego.

2.3.7. Identyfikator użytkownika i hasło, które są przesyłane za pośrednictwem sieci publicznej, chronione są za pomocą szyfrowania kryptograficznego. System informatyczny, jak i każda stacja robocza wyposażona jest w oprogramowanie antywirusowe umożliwiające również wykrywanie złośliwego oprogramowania oraz oprogramowania szpiegującego. Kierownik jednostki organizacyjnej lub inna upoważniona osoba profilaktycznie, nie rzadziej niż raz na dwa tygodnie, wykonuje pełne skanowanie Systemu informatycznego. System informatyczny zapewnia na bieżąco aktualizację definicji wirusów oraz bazy złośliwego i szpiegującego oprogramowania.

2.3.8. Zabrania się używania w Systemie informatycznym nośników niewiadomego pochodzenia bez uprzedniego zweryfikowania ich za pomocą programu, o którym mowa w pkt. 2.11.1 powyżej.

2.3.9. Zabrania się pobierania za pomocą stacji roboczych z sieci publicznej plików niewiadomego pochodzenia.

2.3.10. Obowiązki określone w niniejszym rozdziale Polityki w odniesieniu do poszczególnych stacji roboczych spoczywają w pierwszej kolejności na ich użytkownikach.

2.4. ADO zapewnia zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego poprzez wirtualizację, SLA z dostawcami sprzętu oraz prowadzenie systemu kopii zapasowych.

2.5. ADO zapewnia regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2.5.1. ADO przeprowadza okresowe kontrole sprawności Systemu informatycznego.
2.5.2. Prace serwisowe prowadzone w Systemie informatycznym mogą być wykonywane wyłącznie pod nadzorem kierownika jednostki organizacyjnej lub innej upoważnionej osoby.
2.5.3. W przypadku, gdy prace serwisowe muszą być przeprowadzone poza siedzibą Spółki, Spółka, obowiązana jest zapewnić, aby przekazywany System informatyczny nie zawierał nośników, na których znajdują się dane osobowe, bądź aby dane osobowe zostały wykasowane w sposób uniemożliwiający ich odtworzenie.
2.5.4. Każda awaria lub konieczność wykonania prac serwisowych na stacji roboczej podlega niezwłocznemu zgłoszeniu do kierownika jednostki organizacyjnej. Osoby upoważnione bezwzględnie stosują się do poleceń wydanych w tym zakresie przez ADO lub upoważnioną osobę.

2.6. Spółka stosuje następujące środki organizacyjne w zakresie zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe:

a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie Osoby upoważnionej.
b) Zamykanie pomieszczeń tworzących obszar przetwarzania danych osobowych na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
c) Wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów.
d) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.

III. Procedury zgłaszania naruszeń organowi nadzorczemu

3.1. W przypadku naruszenia ochrony danych osobowych, Spółka zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, tj. Prezesowi Urzędu Ochrony Danych Osobowych.

3.2. Prezes Urzędu Ochrony Danych Osobowych prowadzi system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych.

3.3. Procedura oceny zgłaszania i oceny naruszenia ochrony danych osobowych

3.3.1. Każdy pracownik, który stwierdzi, że doszło do naruszenia ochrony danych osobowych przekazuje kierownikowi działu niezwłocznie, nie później niż w terminie 3 godzin, informację o możliwym naruszeniu. Przez naruszenie ochrony danych osobowych rozumie się sytuację określoną w pkt. 1.3. lit. k) Polityki.
3.3.2. Kierownik działu niezwłocznie po otrzymaniu od pracownika informacji o naruszeniu, o której mowa w pkt. 3.3.1. powyżej, nie później jednak niż w terminie 3 godzin od

otrzymania informacji, zgłasza Spółce lub IOD naruszenie ochrony danych osobowych w drodze mailowej na adres iod@citypark.com.pl.

Informacja o możliwym naruszeniu ochrony danych osobowych powinna co najmniej opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę podmiotów danych, których naruszenie może dotyczyć, opisywać sposób w jaki prawdopodobnie doszło do naruszenia oraz miejsce i czas naruszenia.

3.3.3. Spółka konsultuje z IOD (a w razie potrzeby również z ASI) zgłoszone naruszenie i dokonuje niezwłocznie oceny czy występuje ryzyko naruszenia praw lub wolności osoby fizycznej. Ocena czy występuje ryzyko naruszenia praw lub wolności osoby fizycznej powinna być oparta na obiektywnych kryteriach (dotychczasowe doświadczenie, wiedza z zakresu bezpieczeństwa informacji) oraz na uwzględnieniu okoliczności konkretnego naruszenia ochrony danych osobowych (charakter danych, skala naruszenia, kategoria podmiotów danych, etc.). W toku dokonywania oceny naruszenia Spółka bierze pod uwagę wszelkie możliwe szkody i krzywdy, które mogą wyniknąć z danego zdarzenia dla osób fizycznych takie jak np. utrata kontroli nad danymi, negatywne konsekwencje wizerunkowe, możliwość zawarcia przez inne osoby umów z wykorzystaniem danych, straty finansowe, negatywny odbiór społeczny.

Uznaje się, że istnieje małe prawdopodobieństwo, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych jeśli

a) doszło do przypadkowego skasowania danych osobowych będącego efektem błędu systemu teleinformacyjnego,
b) dane osobowe były zaszyfrowane z wykorzystaniem odpowiedniego algorytmu szyfrującego (np. zagubiono nośnik z danymi albo doszło do wycieku danych osobowych, które były należycie zabezpieczone poprzez szyfrowanie).

3.3.4. W przypadku uznania, że jest mało prawdopodobne, by naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, Spółka nie dokonuje zgłoszenia do organu nadzorczego.

3.3.5. W przypadku uznania, że zgłoszone naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, Spółka zgłasza je organowi nadzorczemu zgodnie z procedurą wskazaną w pkt. 3.4. poniżej.

3.4. W przypadku, o którym mowa w pkt. 3.3.5. Spółka zgłasza Prezesowi Urzędu Ochrony Danych Osobowych stwierdzone naruszenie ochrony danych osobowych w terminie nie dłuższym niż 72 godziny od stwierdzenia naruszenia. Zgłoszenie dokonywane jest w ramach systemu teleinformatycznego prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych. Zgłoszenie dokonywane jest przez IOD lub pracownika upoważnionego do tego przez Spółkę lub IOD. Wzór zgłoszenia stanowi załącznik nr 2 do Polityki.

3.5. W przypadku niedotrzymania terminu, o którym mowa w pkt. 3.4. powyżej, Spółka dołącza do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin wyjaśnienie przyczyn opóźnienia. Wyjaśnienie przyczyn opóźnienia sporządza Spółka w porozumieniu z IOD.

3.6. Zgłoszenie, o którym mowa w pkt. 3.4. powyżej, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę podmiotów danych oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez Spółkę w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3.7. Jeżeli – i w zakresie, w jakim – zgłoszenie nie będzie zawierało wszystkich informacji wskazanych w pkt. 3.6. lit. a-d powyżej, Spółka udzieli organowi nadzorczemu brakujących informacji sukcesywnie bez zbędnej zwłoki w trybie uzupełnienia zgłoszenia.

3.8. Spółka dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Spółka dokumentuje wszystkie naruszenia danych osobowych, w tym również te do których doszło u podmiotów przetwarzających dane. Dokumentacja obejmuje także naruszenia, których Spółka nie zgłosiła do organu nadzorczego z uwagi na małe prawdopodobieństwo, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osoby fizycznej. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania obowiązków Spółki, o których mowa w niniejszym rozdziale Polityki.

3.9. Spółka działająca jako podmiot przetwarzający powierzonych mu danych osobowych po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki, jednak w terminie nie dłuższym niż 24 godziny, zgłasza je administratorowi.

3.10. Podmiot przetwarzający dane osobowe powierzone mu przez Spółkę po stwierdzeniu naruszenia ochrony powierzonych mu danych osobowych bez zbędnej zwłoki, jednak w terminie nie dłuższym niż 24 godziny, zgłasza je Spółki.

IV. Zawiadamianie podmiotu danych o naruszeniu ochrony danych osobowych

4.1. Spółka w porozumieniu z IOD dokonuje oceny czy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocena dokonywana jest z wykorzystaniem procedury i kryteriów, o których mowa w pkt. 3.3. powyżej. Gdy Spółka w porozumieniu z IOD uzna, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (a zatem jest bardzo prawdopodobne, że efektem naruszenia ochrony danych osobowych stanie się naruszenie praw lub wolności podmiotu danych), Spółka bez zbędnej zwłoki, jednak w terminie nie dłuższym niż 72 godziny od stwierdzenia naruszenia, zawiadamia podmiot danych o takim naruszeniu.

4.2. Zawiadomienie przekazywane jest w formie zależnej od posiadanych przez Spółkę danych kontaktowych podmiotu danych - pisemnie, telefonicznie, w formie wiadomości e-mail lub sms, z zastrzeżeniem, że zawiadomienie powinno być sporządzone w formie, która pozwala podmiotowi danych na wielokrotne jej przeczytanie. Jeśli zawiadomienie dokonywane jest telefonicznie, konieczne jest jego potwierdzenie co najmniej w formie wiadomości e-mail lub

sms przekazanej podmiotowi danych. Zawiadomienia dokonuje IOD lub pracownik upoważniony przez Spółkę lub IOD.

4.3. Zawiadomienie, o którym mowa w pkt. 4.1. powyżej jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje i środki:

a) imię i nazwisko oraz dane kontaktowe IOD (adres e-mail: iod@citypark.com.pl) lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
c) opis środków zastosowanych lub proponowanych przez Spółkę w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4.4. Zawiadomienie, o którym mowa w 4.1. powyżej, nie jest wymagane, w następujących przypadkach:

a) Spółka wdrożyła 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) Spółka zastosowała następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności podmiotów danych;
c) wymagałoby ono niewspółmiernie dużego wysiłku.

4.5. Spółka w porozumieniu z IOD stwierdza, czy spełniony został jeden z warunków, o których mowa w pkt. 4.3. lit. a-c powyżej. W przypadku, o którym mowa w pkt. 4.3. lit. c powyżej, Spółka wydaje publiczny komunikat lub stosuje podobny środek, za pomocą którego podmioty danych zostaną poinformowane w równie skuteczny sposób. W przypadku, o którym mowa w zdaniu poprzednim, sposób poinformowania podmiotów danych, ustala Spółka w porozumieniu z IOD.

4.6. Jeżeli Spółka nie zawiadomiła jeszcze podmiotu danych o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może zażądać od Spółki zawiadomienia podmiotu danych lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w pkt. 4.3. lit a-c powyżej.

V. Polityka retencji

Rodzaj danych osobowych	Podstawa ich przechowywania (podstawa ustalenia okresu przechowywania)	Okres przechowywania danych
Ogólne		
Akta osobowe pracowników	• Art. 22^1 w zw. z art. 94 ust. 9a Kodeksu pracy, • Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	- 50 lat od dnia zakończenia pracy u danego pracodawcy - 10 lat od dnia zakończenia pracy u danego pracodawcy – w stosunku do osób zatrudnionych po 31 grudnia 2018 r.

Dokumentacja płacowa (listy płac, karty wynagrodzeń, inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty)	• Art. 22^1 w zw. z art. 94 ust. 9a Kodeksu pracy • Art. 125a ust. 4 ustawy o emeryturach i rentach z FUS • Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	- 50 lat od dnia zakończenia pracy u danego pracodawcy - 10 lat od dnia zakończenia pracy u danego pracodawcy – w stosunku do osób zatrudnionych po 31 grudnia 2018 r.
Dane zakładowego funduszu świadczeń socjalnych	• Art. 22^1 w zw. z art. 94 ust. 9a kodeksu pracy • Ustawa z dna 4 marca 1994 roku o zakładowym funduszu socjalnym • Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	- 50 lat od dnia zakończenia pracy u danego pracodawcy - 10 lat od dnia zakończenia pracy u danego pracodawcy – w stosunku do osób zatrudnionych po 31 grudnia 2018 r.
Zbiór oświadczeń pracowników dla celów obliczania miesięcznych zaliczek na podatek dochodowy od osób fizycznych	• Art. 31 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych • Rozporządzenie Ministra Finansów z dnia 23 listopada 2015 r. w sprawie określenia niektórych wzorów oświadczeń, deklaracji i informacji podatkowych obowiązujących w zakresie podatku dochodowego od osób fizycznych • Art. 51u ustawy o narodowym zasobie archiwalnym i archiwach	- 50 lat od dnia zakończenia pracy u danego pracodawcy - 10 lat od dnia zakończenia pracy u danego pracodawcy – w stosunku do osób zatrudnionych po 31 grudnia 2018 r.
Zgłoszenia do ZUS	• Art. 36 ust. 8 ustawy o systemie ubezpieczeń społecznych	5 lat
Dokumentacja BHP	• Art. 237^4 Kodeksu pracy • Rozporządzenie Ministra Gospodarki i Pracy z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy • Rozporządzenie Rady Ministrów z dnia 1 lipca 2009 r. w sprawie ustalenia okoliczności i przyczyn wypadków przy pracy • Art. 125a ust. 4 ustawy o emeryturach i rentach z FUS	- 50 lat od dnia zakończenia pracy u płatnika - 10 lat od dnia zakończenia pracy u danego pracodawcy – w stosunku do osób zatrudnionych po 31 grudnia 2018 r.
Protokoły ustalenia okoliczności i przyczyn wypadku przy pracy, dokumentacja powypadkowa	• Art. 234 ust. 3^1 Kodeksu pracy	10 lat
Zbiór dokumentów aplikacyjnych kandydatów do pracy	• Art. 22^1 § 1 Kodeksu pracy • Ew. zgoda kandydata.	Do zakończenia procesu rekrutacji / w przypadku zgody na dalsze rekrutacje – do czasu odwołania zgody
Zbiór danych osób świadczących pracę na podstawie umów cywilnoprawnych, które zostały oskładkowane	• Art. 42 ust. 2 pkt 1) w zw. z art. 41 ust 1 ustawy o podatku dochodowym od osób fizycznych • Art. 36 ust 2 w zw. z art. 9 w zw. z 6 ust. 1 pkt 4 w ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych	- 50 lat od zakończenia pracy ubezpieczonego u danego płatnika - 10 lat gdy ubezpieczony zakończył pracę u danego płatnika składek, w przypadku ubezpieczonego zgłoszonego u danego płatnika składek do ubezpieczeń po dniu 31 grudnia 2018 r.
Zbiór umów cywilnoprawnych z	• Art. 42 ust. 2 pkt 1) w zw. z art. 41 ust 1	- 50 lat od zakończenia pracy

pracownikami, które zostały oskładkowane	ustawy o podatku dochodowym od osób fizycznych • Art. 125a ust. 4 ustawy o emeryturach i rentach z FUS • Art. 36 ust 2 w zw. z art. 9 w zw. z 6 ust. 1 pkt 4 w ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych	ubezpieczonego u danego płatnika - 10 lat gdy ubezpieczony zakończył pracę u danego płatnika składek, w przypadku ubezpieczonego zgłoszonego u danego płatnika składek do ubezpieczeń po dniu 31 grudnia 2018 r.
Zbiór danych osób świadczących pracę na podstawie umów cywilnoprawnych, które nie zostały oskładkowane	• Art. 6 ust. 1 lit. b) i f) RODO • Kodeks cywilny z dnia 23 kwietnia 1964 roku	Do upływu terminu przedawnienia roszczeń wynikających z danego stosunku prawnego (umowa o dzieło, umowa zlecenia – 2 lata)
Zbiór umów cywilnoprawnych z pracownikami, które nie zostały oskładkowane	• Art. 6 ust. 1 lit. b) i f) RODO • Kodeks cywilny z dnia 23 kwietnia 1964 roku	Do upływu terminu przedawnienia roszczeń wynikających z danego stosunku prawnego (umowa o dzieło, umowa zlecenia – 2 lata)
Newsletter wysyłany środkami komunikacji elektronicznej, działalność marketingowa	• Art. 10 ust. 2 ustawy o świadczeniu usług drogą elektroniczną • Art. 6 ust. 1 lit. a) lub f) RODO • Art. 172 prawa telekomunikacyjnego	2 lata lub do złożenia sprzeciwu na przetwarzanie danych osobowych w celach marketingowych lub do cofnięcia zgody na przesyłanie newslettera pochodzącej od osoby, której dane są przetwarzane,
Zbiór dokumentacji finansowo-księgowej	• Art. 32 ust. 1, art. 86 ust. 1, art. 88 ust. 1 Ordynacji podatkowej • Art. 74 ustawy o rachunkowości	5 lat, jednak nie krócej niż do czasu upływu okresu przedawnienia zobowiązania podatkowego
Monitoring	Brak regulacji w tym zakresie	W krajach UE zwykle przyjmuje się okres do 30 dni
Dane osobowe kontrahentów	• Art. 6 ust. 1 lit. b) i f) RODO	Do upływu terminu przedawnienia roszczeń wynikających z danego stosunku prawnego
Klienci salonu kosmetycznego	• Zgoda podmiotu danych – art. 6 ust. 1 lit. a) oraz art. 9 ust. 2 lit. a RODO	przez okres 6 lat od momentu ostatniej wizyty lub do momentu cofnięcia przez nich zgody

VI. Rejestr czynności przetwarzania, rejestr kategorii przetwarzania

Załącznik nr 1 do Polityki Ochrony Danych - UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH oraz OŚWIADCZENIE O ZAPOZNANIU SIĘ Z REGULACJAMI DOTYCZACYMI PRZETWARZANIA DANYCH OSOBOWYCH WRAZ ZE ZOBOWIAZANIEM DO ICH PRZESTRZEGANIA

Załącznik nr 2 do Polityki Ochrony Danych - ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

....., dn. ..... r.
[data sporządzenia]

Do
Prezesa Urzędu Ochrony Danych Osobowych
.....

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora Danych Osobowych	
Miejsce i dzień naruszenia	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Opis charakteru naruszenia ochrony danych	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

.....
[podpis osoby uprawnionej do reprezentowania Administratora]