creo concept®

PERFECT WALL

Polityka ochrony danych osobowych w CreoConcept

creo concept®

PERFECT WALL

Wstęp

CreoConcept Sp. z o.o. Sp. k. jest Administratorem Danych Osobowych, a czynności z zakresu ochrony danych osobowych wykonuje Prezes Zarządu, Tomasz Rybka. Jest On zobowiązany do podejmowania wszelkich możliwych działań, koniecznych do zapobiegania zagrożeniom związanym z przetwarzaniem danych osobowych.

Polityka ochrony danych osobowych jest dokumentem opisującym zasady ochrony danych osobowych, stosowanym przez Administratora w celu spełnienia wymagań 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 oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz.2018 r. poz. 1000).

Celem niniejszej Polityki Ochrony Danych Osobowych jest wypełnienie założeń Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przewarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46 WE (ogólne rozporządzenie o ochronie danych, dalej zwane RODO). Stanowi ona zbiór wymogów, zasad i regulacji, dotyczących ochrony danych osobowych u Administratora danych osobowych.

Rozdział I
Postanowienia ogólne

§ 1

Dla potrzeb niniejszego dokumentu wprowadza się następujące definicje:

1. Polityka – Polityka Ochrony Danych Osobowych w CreoConcept Sp. z o.o. Sp. k.,
2. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
3. Zbiór danych – uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
4. Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który samodzielni lub wspólnie z innymi ustala cela i sposoby przetwarzania danych osobowych.
5. Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który w imieniu Administratora przetwarza dane osobowe;
6. Ryzyko – wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Jest ono proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować.
7. Przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie, niszczenie.
8. Odbiorca - osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą uzyskiwać dane osobowe w ramach prowadzonego postępowania zgodnego z prawem UE lub prawem państwa członkowskiego, nie są uznawane za odbiorców.
9. Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie pisemnego oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
10. Naruszenie ochrony danych osobowych (incydent) – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 2

1. Polityka służy:

a) zapewnieniu ochrony danych osobowych przetwarzanych w spółce CreoConcept Sp. z o.o. Sp. k.,

b) ustanowieniu jednolitych reguł postępowania w zakresie przetwarzania danych osobowych,

c) wdrożeniu środków organizacyjnych i technicznych, które zapewniają przetwarzanie danych osobowych zgodnie z prawem, w szczególności z RODO oraz możliwość wykazania tej zgodności.

2. Szczegółowymi celami Polityki są:

a) zapewnienie realizacji praw osób, których dane osobowe dotyczą,

b) określenie obowiązków i odpowiedzialności osób zobowiązanych do realizacji zadań, określonych w Polityce,

c) zapewnienie przeprowadzania oceny skutków dla ochrony danych,

d) zarządzanie naruszeniami ochrony danych osobowych i ograniczanie ich skutków,

e) sposób zapoznawania pracowników ze zmianami w przepisach dot. danych osobowych.

3. Zakres stosowania Polityki

a) Polityka określa sposób przetwarzania danych osobowych i zarządzania procesami związanymi z przetwarzaniem danych osobowych w celu zapewnienia odpowiedniej ochrony tych danych, dla których administratorem lub współadministratorem jest Prezes Zarządu firmy,

b) Polityka określa również sposób przetwarzania danych osobowych i zarządzania procesami związanymi z przetwarzaniem danych osobowych w celu zapewnienia odpowiedniej ochrony tych danych,

c) Polityka określa obowiązki i odpowiedzialność osób zobowiązanych do realizacji zadań związanych z procesami, o których mowa,

d) Polityka ma zastosowanie do przetwarzania danych osobowych, o których mowa, niezależnie od:

   1. sposobu przetwarzania (całkowicie zautomatyzowany, częściowo zautomatyzowany lub inny niż zautomatyzowany),
   2. formy lub postaci przetwarzania (papierowa, elektroniczna lub inna),
   3. kanałów przepływu danych osobowych,
   4. narzędzi informatycznych służących do przetwarzania danych osobowych (systemów, aplikacji, programów),
   5. celu przetwarzania,
   6. źródła pochodzenia danych osobowych,
   7. kategorii danych osobowych,
   8. Politykę stosują wszystkie osoby, które na polecenie Administratora uczestniczą w przetwarzaniu danych osobowych.

Rozdział II

Inwentaryzacja danych.
Zasady przetwarzania danych osobowych.
Odpowiedzialność.
Obowiązek informacyjny.
Porozumienia i kontakty ze stronami zewnętrznymi.

§ 3

1. Dane osobowe wymagające ochrony wykazano w załączniku do niniejszej polityki (Załącznik nr 1 – Wykaz zbiorów danych osobowych).
2. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Każdy zbiór opisano w sposób umożliwiający przeprowadzenie analizy ryzyka.
4. Opis zbiorów obejmuje takie informacje, jak:
   a) nazwę zbioru,
   b) opis celów przetwarzania,
   c) charakter, zakres, kontekst, dokumentowane dane osobowe,
   d) odbiory,
   e) funkcjonalny opis operacji przetwarzania,
   f) aktywa służące do przetwarzania danych osobowych,
   g) informacja o konieczności przeprowadzenia oceny skutków dla zbioru,
   h) kategorię osób, których dane dotyczą,
   i) dane administratora – osoby odpowiedzialnej za gromadzone dane,
   j) planowane terminy usunięcia danych,
   k) podstawę prawną przetwarzania.

§ 4

1. Administrator oraz podmiot przetwarzający zapewniają, że dane osobowe przetwarzane są zgodnie z poniższymi regułami:
   a) zgodnie z prawem i rzetelnie oraz w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość),
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach (ograniczenie celu),
   c) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane (minimalizacja danych),
   d) prawidłowe i w razie potrzeby uaktualniane (prawidłowość),
   e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania, z wyjątkami wskazanymi w rozporządzeniu (ograniczenie przechowywania),
   f) 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 środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczone przed ich udostępnieniem osobom nieupoważnionym lub wejściem w posiadanie przez osobę nieuprawnioną (integralność i poufność),
   g) Wobec osób, których dane są przetwarzane, wykonano tzw. obowiązek informacyjny – prawo dostępu do danych, ich przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania i sprzeciwu.
2. Administrator prowadzi rejestr czynności przetwarzania. Rejestr stanowi równocześnie wykaz zbiorów danych osobowych przetwarzanych przez Administratora (załącznik nr 1).
3. Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania.

§ 5

1. Do stosowania zasad określonych przez niniejszy dokument zobowiązani są wszyscy pracownicy CreoConcept Sp. z o.o. Sp. k., niezależnie od podstawy zatrudnienia oraz osoby realizujące czynności na gruncie umów cywilnoprawnych, którzy w ramach obowiązków służbowych przetwarzają dane osobowe.
2. Każda osoba mająca dostęp do danych osobowych przetwarzanych w CreoConcept Sp. z o.o. Sp. k. jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 6

1. Administrator/podmiot przetwarzający odpowiada za nadawanie oraz anulowanie upoważnień do przetwarzania danych osobowych w zbiorach papierowych, systemach informatycznych.
2. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia Administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenia Administratora, chyba że wymaga tego przepis prawa
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych (kierowników/dyrektorów działów). Kierownicy jednostek organizacyjnych określają zakres kompetencji przetwarzania danych osobowych.
4. Upoważnienia określają zakres operacji na danych.
5. Upoważnienia powinny być przechowywane w aktach osobowych pracowników (ewentualnie w dokumentacji odpowiednich komisji), powinny być udostępniane tylko osobom upoważnionym oraz aktualizowane w przypadku zmiany zakresu obowiązków.
6. Upoważnienia mogą być wyjątkowo nadawane w formie poleceń, np. upoważnienie do przeprowadzenia kontroli, audytów, wykonania czynności służbowych.
7. Administrator danych prowadzi ewidencję osób upoważnionych, w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja stanowi załącznik do niniejszej Polityki (Załącznik nr 2 - Wzór ewidencji osób upoważnionych). Ewidencja prowadzona jest w formie elektronicznej).

§ 7

1. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym nadawane są na wniosek przełożonych (kierowników/dyrektorów działów) osób, które mają przetwarzać dane. Gdy sytuacja tego wymaga, z wnioskiem takim mogą wystąpić pracownicy. Prośbę o udostępnienie zasobu związanego z danymi osobowymi kieruje się droga mailową do informatyka w ramach organizacji, informując o tym także osobę przełożoną (mail DW).
2. Kierownicy jednostek organizacyjnych działów określają systemy informatyczne, do których dostęp mają pracownicy ich działów oraz zakres kompetencji.
3. Uprawnienie, o którym mowa w pkt. 1 jest anulowane z chwilą zaprzestania przetwarzania danych osobowych przez osobę, której uprawnienie zostało nadane bądź z ustaniem zatrudnienia.

§ 8

1. Administrator pozyskując dane osobowe od osoby, której dotyczą, jest zobowiązany podać jej następujące informacje:
   a) swoją tożsamość i dane kontaktowe,
   b) cele przetwarzania danych oraz podstawę prawną przetwarzania,
   c) jeżeli przetwarzanie danych osobowych jest związane z realizacją prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią - należy wskazać prawnie uzasadnione interesy,
   d) informacje o odbiorcach danych osobowych lub od kategoriach odbiorców,
   e) w przypadkach gdy ma to zastosowanie informacje o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej,
   f) okres, przez który damy osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   g) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   h) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (reguła ta ma zastosowanie do przetwarzania danych na podstawie zgody wyrażonej w jednym, lub większej liczbie celów oraz przetwarzania danych o szczególnej kategorii na podstawie zgody osoby której dane dotyczą),
   i) informacje o prawie wniesienia skargi do organu nadzorczego
   j) informacje czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
   k) informacje o zautomatyzowanym podejmowaniu decyzji.
2. W przypadku, gdy Administrator pozyskuje dane osobowe z innego źródła niż osoba, której dane dotyczą, Administrator jest zobowiązany podać tej osobie wszystkie informacje wymienione w pkt. 1, a dodatkowo: podać informacje o źródle pochodzenia danych osobowych..
3. Informacje, o których mowa w pkt. 2 Administrator podaje w rozsądnym terminie po pozyskaniu danych, najpóźniej w ciągu miesiąca mając na uwadze konkretne okoliczności przetwarzania danych osobowych. W przypadku, gdy dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą, administrator przekazuje dane najpóźniej przy pierwszej takiej komunikacji. Jeżeli planuje się ujawnić dane osobowe innemu odbiorcy najpóźniej przy ich pierwszym ujawnieniu.

§ 9

1. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane przez okres nie dłuższy niż jest to niezbędne dla osiągnięcia celów, dla których dane te są przetwarzane. Dane osobowe mogą być przechowywane przez okres dłuższy, jeżeli będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów naukowych lub historycznych lub do celów statystycznych.
2. Dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób których dotyczą.
3. Osoba której dane dotyczą ma prawo żądać od Administratora sprostowania dotyczących jej danych, które są nieprawidłowe.
4. Osoba, której dane dotyczą ma prawo żądać od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane, jeżeli zachodzi jedna z przesłanek:
   a) dane osobowe nie są już niezbędne dla celów, dla jakich zostały zebrane,
   b) osoba, której dane dotyczą cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej do ich przetwarzania,
   c) osoba, której dane dotyczą, wnosi sprzeciw na mocy przepisów prawa i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
   d) dane osobowe były przetwarzane niezgodnie z prawem,
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego,
   f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.
5. Osoba, której dane dotyczą, ma prawo żądać ograniczenia przetwarzania w następujących przypadkach:
   a) osoba, której dane dotyczą, kwestionuje ich prawidłowość,
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu danych,
   c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń,
   d) Osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania.
6. 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.
7. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

§ 10

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, wiążąc podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, jego charakter i cel, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
3. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji, zalecane jest zawarcie umowy powierzenia.

Rozdział III

Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych.

Instrukcja postępowania z incydentami.

§ 11

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstawania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik spółki zobowiązany jest niezwłocznie, najpóźniej do 24 godzin, do powiadomienia o stwierdzeniu podatności lub wystąpieniu incydentów bezpośredniego przełożonego. Jeżeli incydent dotyczy wycieku danych cyfrowych, o fakcie tym poinformować należy także dział IT.
2. Do typowych podatności bezpieczeństwa danych osobowych należą w szczególności:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą w szczególności:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczeni, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych,
   c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów lub danych, działanie wirusów I innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (w przypadku danych cyfrowych włączając do działań dział IT) prowadzi postępowanie wyjaśniające, w toku którego:
   a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   b) inicjuje ewentualne działania dyscyplinarne,
   c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
   d) rekomenduje działania prewencyjne (zapobiegawcze), zmierzające do eliminacji podobnych incydentów w przyszłości, lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (Załącznik nr 3 - Zgłoszenie naruszenia ochrony danych osobowych),

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu.
8. W przypadku zaistnienia incydentu Administrator powiadamia osoby, których dane dotyczą, o zaistniałym incydencie.

Rozdział IV

Regulamin ochrony danych osobowych, polityka kluczy.

§ 12

1. Regulamin określa podstawowe obowiązki z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami, dla: pracowników, współpracowników, pracowników podmiotów trzecich posiadających dostęp do danych osobowych przetwarzanych przez administratora, użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez administratora.
2. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (Załącznik nr 5 - Oświadczenie o zachowaniu w tajemnicy danych osobowych uzyskanych w trakcie pracy).

Rozdział V
Szkolenia / audyt

§ 13

1. Każdy użytkownik przed dopuszczeniem do przetwarzania danych osobowych, zobowiązany jest zapoznać się z przepisami w tym zakresie oraz poznać wynikające z nich zadania i obowiązki.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom wewnętrznym.
3. Za przeprowadzanie szkoleń odpowiada Administrator danych osobowych.
4. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych, wskazane jest udokumentowanie odbycia tego szkolenia.
5. Po przeprowadzeniu szkolenia z zasad ochrony danych osobowych, uczestniczy są zobowiązani do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.
6. Zgodnie z artykułem 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania.

Rozdział VI

Środki organizacyjne i techniczne, zabezpieczające dane osobowe

§ 14

1. Zgodnie z artykułem 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich. W razie incydentu fizycznego lub technicznego.
2. Procedury przywracania dostępności danych osobowych i dostępu do nich zostały opracowane jako załącznik (Załącznik nr 10 - Plan ciągłości działania).

Rozdział VII

Wykaz pomieszczeń gdzie przetwarzane są dokumenty, zawierające dane osobowe w CreoConcept Sp. z o.o. Sp. k.

§ 15

Wykaz pomieszczeń należących do firmy CreoConcept Sp. z o.o. Sp. k. w których dokonuje się operacji na danych osobowych, z uwzględnieniem pomieszczeń szczególnie chronionych, stanowi załącznik do niniejszej polityki:

Załącznik nr 4 - Wykaz pomieszczeń.

Załącznik nr 1 – Wykaz zbioru danych osobowych Administratora

Załącznik nr 2 - Wzór ewidencji osób upoważnionych

Załącznik nr 3 – Zgłoszenie naruszenia ochrony danych osobowych

Załącznik nr 4 - Wykaz pomieszczeń

Załącznik nr 5 – Oświadczenie o zachowaniu w tajemnicy danych osobowych uzyskanych w trakcie pracy

creo concept®

PERFECT WALL

Polityka ochrony danych osobowych dla spółki CreoConcept Sp. z o.o. Sp. k. została przyjęta w dniu 8 grudnia 2023 r.

THINK CREO