POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

CREATIVE ANSWER SP. Z O.O.

NIP 5252384416 | REGON 140793911

Data opracowania:	30 maja 2022r.
Data wdrożenia:	3 czerwca 2022r.
Dokument zatwierdził i wdrożył:	Mikołaj Soszyński

I. Cel, zakres zastosowania i definicje użyte w dokumencie

1. Cel Polityki

1.1 Celem opracowania i wprowadzenia niniejszej Polityki bezpieczeństwa jest opisanie zastosowanych wewnątrz ***CREATIVE ANSWER SP. Z O.O. z siedzibą w Warszawie, ul. Altowa 34, 02-386 Warszawa (w dalszej części jako Administrator)*** środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednich do ryzyka naruszenia praw i wolności w związku z przetwarzaniem danych osobowych.

1.2 Polityka bezpieczeństwa ma umożliwić należyte wywiązywanie się z obowiązków ***Administratora- CREATIVE ANSWER SP. Z O.O. z siedzibą w Warszawie, ul. Altowa 34, 02-386 Warszawa.*** Polityka bezpieczeństwa danych osobowych została opracowana stosownie do przepisów 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.

1.3 Niniejszy dokument będzie wdrożony poprzez jego opublikowanie oraz zapoznawania z nim osób upoważnionych do przetwarzania danych osobowych, a także innych osób mających dostęp do danych osobowych przetwarzanych przez **Administratora.**

2. Zakres zastosowania i wyłączenia ze stosowania

2.1 Polityka obejmuje swym zakresem wszystkie dane osobowe przetwarzane przez **Administratora.**

2.2 Zapisy i wymagania niniejszej Polityki mogą być wyłączone tylko w przypadku, gdy obowiązujące przepisy prawa przewidują takie wyłączenie

3. Definicje

1.	**Administrator**	Creative Answer Sp. z o.o. ul. Altowa 34, 02-386 Warszawa, w odniesieniu do danych co do których decyduje o celach i sposobach przetwarzania
2.	**Dane osobowe**	oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3.	**Dane szczególnych kategorii danych osobowych**	dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby oraz dane wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;
4.	**Prezes urzędu**	Prezes Urzędu Ochrony Danych Osobowych;
5.	**Integralność danych**	właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
6.	**Naruszenie ochrony danych osobowych**	oznacza 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;
7.	**Osoba upoważniona**	osoba posiadające upoważnienie do przetwarzania danych osobowych w imieniu Administratora
8.	**Podmiot danych (lub właściciel danych)**	każda osoba fizyczna, której dane osobowe są przetwarzane przez Administratora lub na zlecenie Administratora w związku z prowadzoną przez nią działalnością;

9.	**Poufność danych**	właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
10.	**Pracownik**	osoba, posiadająca dostęp do danych osobowych, świadcząca pracę na rzecz Administratora na podstawie stosunku pracy;
11.	**Strona trzecia**	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
12.	**Procesor lub Podmiot przetwarzający**	osoba prawna, osoba fizyczna, jednostka organizacyjna nieposiadająca osobowości prawnej lub inny podmiot, który nie decyduje o celach i środkach przetwarzania danych osobowych, któremu Administrator powierzyła do przetwarzania dane osobowe oraz zawarł Umowę powierzenia przetwarzania danych osobowych w rozumieniu art. 28 RODO;
13.	**Przetwarzanie danych osobowych**	oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
14.	**Polityka**	niniejszy dokument, czyli Polityka bezpieczeństwa danych osobowych
15.	**Rozliczalność**	właściwość umożliwiająca wykazanie zgodności Administratora z przepisami RODO;
16.	**RODO lub Rozporządzenie**	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;
17.	**Pseudonimizacja**	oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji,

		pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
18.	**Rejestr czynności przetwarzania**	prowadzony przez Administratora rejestr zawierający minimum następujące dane: a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych; b) cele przetwarzania; c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych; e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń; f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.
19.	**Skarga**	jakiekolwiek pismo (w postaci papierowej lub elektronicznej) przekazane przez podmiot danych (właściciela danych) lub Prezesa Urzędu z treści którego wynika niezadowolenie lub żądanie wyjaśnień / informacji dotyczących przetwarzania danych osobowych przez Administratora
20.	**System informatyczny (lub system IT)**	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

21.	**Ustawa**	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
22.	**Upoważnienie**	jedno z poniższych: - pisemne upoważnienie wydane na podstawie art. 29 RODO do przetwarzania danych osobowych nadane Pracownikowi, Współpracownikowi lub pracownikowi Procesora przez wspólnika spółki, - Umowa powierzenia przetwarzania danych osobowych zawarta na piśmie w rozumieniu art. 28 RODO;
23.	**Współpracownik**	osoba, posiadająca dostęp do danych osobowych wykonująca osobiście i bezpośrednio zadania / usługi na rzecz Administratora na innej podstawie prawnej niż stosunek pracy, bez względu na nazwę lub rodzaj łączącej strony umowy;
24.	**Zabezpieczenie danych**	wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
25.	**Zgoda osoby, której dane dotyczą**	osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

II. Obowiązki Creative Answer Sp. z o.o., ul. Altowa 34 02-386 Warszawa jako Administratora

1. Obowiązek spełnienia podstaw prawnych dla przetwarzania danych osobowych

1.1 Każdy Pracownik jak i Współpracownik przed podjęciem decyzji o utworzeniu celu przetwarzania lub poszerzenia zakresu zbieranych danych osobowych do aktualnego celu przetwarzania określonego w Rejestrze czynności przetwarzania (RCP) jest zobowiązany do wskazania i stosowania podstawy prawnej (z RODO) legalizującej przetwarzania takich danych.

2. Obowiązek informacyjny w stosunku do podmiotu danych zgodnie z art. 13 oraz art. 14 RODO

2.1 Każdy Pracownik, Współpracownik, który zbiera (pozyskuje) dane osobowe, w momencie ich zbierania bezpośrednio od właściciela danych, jest zobowiązany poinformować właściciela

danych (np. poprzez przedstawienie odpowiedniego klauzuli) zgodnie z przygotowanymi klauzulami informacyjnymi dotyczącymi art. 13 RODO.

2.2 W przypadku zbierania danych od osób trzecich, a więc nie bezpośrednio od właściciela danych należy poinformować niezwłocznie po utrwaleniu danych o okolicznościach przetwarzani zgodnie z klauzulami informacyjnymi dotyczącymi art. 14 RODO.

2.3 W przypadku korzystania z systemów informatycznych, które automatycznie zbierają dane osobowe, należy zapewnić, aby system ten udzielał informacji, o których mowa w punktach powyżej.

2.4 W przypadku korzystania z podmiotów trzecich (np. agencje marketingowe, rekrutacyjne) należy zapewnić w umowie z takim podmiotem, aby w trakcie zbierania danych osobowych, podmiot ten wykonywał obowiązek informacyjny w imieniu Administratora zgodnie z punktem 2.2. 1) lub 2.2. 2).

3. Obowiązek przestrzegania zasad przetwarzania opisanych w art. 5 RODO

3.1 W trakcie procesów przetwarzania danych osobowych należy dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności przestrzegania zasad określonych w punktach 5-7 Polityki. Obowiązek ten dotyczy zarówno Pracowników, Współpracowników jak i podmiotów, które w imieniu Administratora przetwarzają dane osobowe na podstawie umów powierzenia przetwarzania danych osobowych tj. Procesorów.

4. Obowiązek zawarcia umowy powierzenia przetwarzania danych osobowych (art. 28)

4.1 Jeśli Administrator podejmie decyzję o korzystaniu z usług podmiotu trzeciego, a w ramach świadczenia tych usług podmiot ten będzie przetwarzał dane osobowe na zlecenie lub w imieniu Administratora, to należy zapewnić, aby przed przekazaniem danych temu podmiotowi, została zawarta ***„Umowa powierzenia przetwarzania danych osobowych”*** zgodnie z zasadami określonymi w punkcie 6. Polityki.

5. Obowiązek realizacji żądań osoby, której dane dotyczą

5.1 Jeśli właściciel danych zgłosi się z ustnym lub pisemnym wnioskiem / prośbą o dostęp / kopię danych / przeniesienie danych / usunięcie jego danych / sprostowanie / ograniczenie / zaktualizowanie (niezależnie od formy zgłoszenia papierowo lub elektronicznie) należy niezwłocznie, maksymalnie w ciągu 30 dni zrealizować taki wniosek, jeśli jest zasadny.

5.2 W każdym przypadku realizacja takiego wniosku, o którym mowa w pkt. powyżej powinna być wykonana przez Administratora, który w takim przypadku może wskazać odpowiednio Pracownika, Współpracownika lub inny podmiot do wsparcia przy realizacji takiego wniosku.

5.3 W każdym przypadku Administrator ułatwia właścicielowi danych wykonanie praw przysługujących mu na mocy art. 15–22 RODO. Jeśli Administrator nie możne wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą i prosi o uzupełnienie danych w celu możliwości ustalenia tożsamości właściciela danych.

5.4 Administrator realizując wniosek właściciela danych postępuje zgodnie z ***Procedurą obsługi wniosków Podmiotów danych.***

6. Obowiązek zabezpieczenia danych

6.1 Każdy Pracownik, Współpracownik jest zobowiązany stosować zabezpieczenia:

- organizacyjne (np. polityki, regulaminy, procedury) obowiązujące w organizacji Administratora niezależnie do tego jakim dokumentem wewnętrznym zostały one opisane oraz
- techniczne (np. stosowanie haseł dostępowych, szyfrowany PENDRIVE czy szyfrowanie komputerów oraz urządzeń mobilnych). Obchodzenie zabezpieczeń określonych w dokumentach wewnętrznych lub wdrożonych przez dostawcę IT może stanowić naruszenie ochrony danych osobowych.

6.2 Obowiązek zabezpieczenia danych dotyczy również Procesorów. Szczegółowe wymagania odnośnie zabezpieczania danych osobowych przez procesora powinny być określone w ***Umowie powierzenia przetwarzania danych osobowych***.

7. Obowiązek zgłoszenia nowego celu przetwarzania danych osobowych

7.1 Jeśli Pracownik lub Współpracownik podejmie decyzję o rozpoczęciu zbierania danych osobowych w nowym celu, jest zobowiązany przed przystąpieniem zbierania poinformować o tym fakcie Administratora, powszechnie stosowaną formą komunikacji w organizacji.

7.2 Na podstawie informacji od Pracownika lub Współpracownika Administrator podejmuje decyzję czy dany cel podlega obowiązkowi zarejestrowania go Rejestrze czynności przetwarzania.

7.3 Pracownicy i Współpracownicy są zobowiązani zgłosić bezpośrednio do Administratora wszelkie zmiany dotyczące czynności przetwarzania opisanych w Rejestrze przed wprowadzeniem tych zmian.

8. Obowiązki przy przekazywaniu do państw trzecich

8.1 Przez ewentualnym podjęciem decyzji o wyborze dostawcy spoza EOG lub przekazaniu danych do państwa trzeciego Administrator powinien dokonać dodatkowej analizy lub zasięgnąć opinii ze źródeł zewnętrznych na temat bezpieczeństwa przy przekazywaniu takich informacji.

9. Obowiązki i odpowiedzialność

9.1 Każdy Pracownik i Współpracownik niezależnie od stanowiska czy zadań jest zobowiązany do i odpowiada za:

- zachowanie w poufności danych osobowych oraz sposobu ich zabezpieczeń,
- zapoznanie i stosowanie się do zapisów niniejszej Polityki oraz dokumentów wewnętrznych wydanych na podstawie niniejszej Polityki,
- pisemne potwierdzenie zapoznania się z przepisami o ochronie danych osobowych i niniejszą Polityką,
- przestrzeganie przepisów o ochronie danych osobowych w szczególności Ustawy,
- nieudostępnianie swoich haseł do systemów IT,
- nieudostępnianie lub nieumożliwianie dostępu do danych osobowych osobom nieupoważnionym,
- zgłaszanie każdego zauważonego incydentu / podejrzenia naruszenia ochrony danych osobowych lub niniejszej Polityki zgodnie procedurami.

9.2 Obowiązki i odpowiedzialność kadry kierowniczej

- nadzorowanie podległych pracowników czy stosują zasady opisane w niniejszej Polityce,
- potrzeb informacyjnych / szkoleniowych w zakresie przepisów o ochronie danych osobowych,

- zatwierdzanie wszelkich zmian dotyczących celów przetwarzania danych osobowych **przed ich wprowadzeniem**,
- nadzorowanie przypisanych celów przetwarzania danych osobowych czy zakres przetwarzania zgodnie z Rejestrem czynności przetwarzania,
- weryfikację dotyczącą nowych rozwiązań informatycznych, które wiążą się z transferem danych osobowych do podmiotu trzeciego,
- zapewnienie zawarcia umowy powierzenia przetwarzania przez Administratora z każdym podmiotem, któremu Administrator zamierza powierzyć przetwarzanie danych osobowych.

9.3 Obowiązki i odpowiedzialność dostawcy IT (jeżeli występuje)

Każdy pracownik dostawcy IT przydzielony do współpracy z Administratorem jest zobowiązany do i odpowiada za:

- nadzorowanie czy wdrożone i utrzymywane zabezpieczenia (fizyczne, logiczne, systemowe) są skutecznie,
- nadzorowanie czy wdrożone ograniczenia dostępów do obszarów przetwarzania danych są skuteczne,
- uwzględniania przepisów RODO oraz Polityki w trakcie projektowania i wdrażania nowych rozwiązań dotyczących bezpieczeństwa informatycznego lub fizycznego,
- na wniosek Administratora sporządzanie opinii i informacji dotyczących zabezpieczeń stosowanych w organizacji.

10. Zasady postępowania w przypadku skarg na przetwarzanie danych osobowych

10.1 Skargi / wnioski wnoszone przez właściciela danych

1) W przypadku pisemnej skargi / wniosku (niezależnie od formy doręczenia czy zatytułowania) przesłanej przez właściciela danych do Administratora należy rozpatrzyć niezwłocznie, nie dłużej niż w terminie nie przekraczającym 30 dni od daty wpłynięcia.
2) Odpowiedź na skargę / wniosek należy udzielić na piśmie (przesyłką rejestrowaną) jeśli wnoszący podał adres do doręczeń natomiast w przypadku braku takiego adresu tą samą drogą, którą skarga / wniosek został złożona, chyba, że wnioskujący poprosił o inną formę. W przypadku odpowiedzi za pomocą poczty elektronicznej kopię odpowiedzi należy w każdym przypadku archiwizować dla wypełnienia rozliczalności Administratora Danych Osobowych.
3) Jeśli właściciel danych zgłosi się z wnioskiem, prośbą o zmianę lub aktualizację danych osobowych, należy uczynić to niezwłocznie po uzyskaniu takiego wniosku.
4) Jeśli właściciel danych zgłosi się z wnioskiem, prośbą o usunięcie lub zaprzestania przetwarzania jego danych, a dane te były zbierane tylko na podstawie zgody tej osoby, należy usunąć niezwłocznie jego dane osobowe lub zaprzestać przetwarzania do celów na jakie wyraził wcześniej zgodę.

5) Dane osobowe przetwarzane na podstawie zawartej umowy, po odwołaniu wszystkich zgód właściciela danych, mogą być przetwarzane nadal w innych celach (np. wykonanie umowy, podatkowe), jeśli takowe wynikają z Rejestru czynności przetwarzania.
6) Jeśli właściciel danych zgłosi się z wnioskiem o dostęp do jego danych osobowych lub uzyskanie kopii danych to na taki wniosek należy odpowiedzieć niezwłocznie, nie przekraczając 30 dni.
7) Właściciel danych może skorzystać z prawa do kopii danych przetwarzanych na podstawie umowy lub zgody, które zostały dostarczone przez właściciela administratorowi nieodpłatnie. Za każdą kolejną kopię danych Administrator może naliczyć rozsądną opłatę administracyjna związaną z przygotowaniem takiej kopii danych.

10.2 Skargi przekazywane przez Prezesa urzędu

1) W przypadku skargi złożonej przez właściciela danych do Prezesa Urzędu, które organ przekazał do Administratora, należy niezwłocznie przekazać wspólnikowi spółki.
2) Termin udzielania odpowiedzi na taką skargę doręczoną przez Prezesa Urzędu wynosi 7 dni (chyba, że Prezes Urzędu wyznaczy inny).
3) Odpowiedź przygotowuje wskazany przez Administratora Pracownik bądź Współpracownik lub też jeden ze wspólników spółki a do Prezesa Urzędu ostateczną wersję odpowiedzi kieruje wspólnik spółki.

III. Zasady przetwarzania danych osobowych przez Administratora

1. **Zasada legalności, rzetelności i przejrzystości**

   Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Nie wolno przetwarzać danych osobowych bez podstawy prawnej. Przed przystąpieniem do przetwarzania nowej kategorii danych osobowych lub danych w nowym celu należy wskazać podstawę prawną do ich przetwarzania.

2. **Zasada minimalizacji danych**

   Dane osobowe muszą być przetwarzane wyłącznie w konkretnym i jasno sprecyzowanym celu, a właściciel danych musi być o tym celu poinformowany. Dane osobowe musza być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

3. **Zasada minimalizacji**

   Można zbierać tylko tyle danych, ile jest adekwatne do realizacji celu. Nie można zbierać „na zapas” ze względu na to, że w przyszłości się „przydadzą”. Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

4. **Zasada prawidłowości**

   Wszystkie osoby upoważnione do przetwarzania i Procesorzy odpowiadają za poprawność merytoryczną danych. Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

5. **Zasada ograniczenia przetwarzania**

   Można przetwarzać dane osobowe tylko tak długo jak długo istnieje cel przetwarzania lub określają to przepisy prawa. Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

6. **Zasada poufności i integralność**

   Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

7. **Zasada zaznajamiania osób upoważnionych z przepisami wewnętrznymi i zewnętrznymi w zakresie ochrony danych osobowych**

   Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zapoznawania się na bieżąco z przepisami wewnętrznymi i zewnętrznymi w zakresie ochrony danych osobowych. W przypadku braku wiedzy można konsultować się bezpośrednio

   z wspólnikiem spółki. Każda osoba upoważniona po zapoznaniu się z przepisami i zasadami w zakresie ochrony danych osobowych, potwierdza ten fakt poprzez pisemne podpisanie stosownego oświadczenia.

8. **Zasada ograniczonego dostępu**

   Dostęp do danych osobowych zawsze musi być ograniczony tylko dla osób upoważnionych. Ograniczanie dostępu może być organizacyjne (np. osobiste nadzorowanie, wprowadzanie procedur), fizyczne (np. zamykanie na klucz, karty zbliżeniowe pomieszczeń) lub informatyczne (np. stosowanie loginów haseł).

9. **Zasada podwójnego dostępu**

   Dostęp do danych osobowych zawsze musi być ograniczony poprzez zastosowanie minimum **dwóch ograniczeń dostępu** dowolnego rodzaju.

10. **Zasada czystego biurka**

    Po skończonej pracy, na biurku Pracownika / Współpracownika nie mogą się znajdować żadne dokumenty lub ogólnodostępne nośniki informatyczne zawierające dane osobowe. Wszystkie takie dokumenty / nośniki powinny być zamknięte na klucz w szafach / kantorkach.

11. **Zasada bezpiecznego niszczenia dokumentów i nośników danych**

    Usuwanie danych poprzez niszczenie dokumentów w postaci papierowej lub w postaci elektronicznej odbywa się zgodnie z „***Procedurą bezpiecznego usuwania danych***”.

12. **Zasada rozliczalność**

    Działania osoby upoważnionej lub Procesora na danych osobowych w szczególności w systemach informatycznych muszą być zawsze przypisane w sposób jednoznaczny tylko jednej osobie upoważnionej do przetwarzania danych osobowych. To oznacza, że dany login do systemu IT może być przypisany TYLKO JENDEJ OSOBIE. **Zakazane jest**

współdzielenie loginów przez dwie i więcej osób. Działania przypisane w systemie IT do konkretnego loginu zawsze będę przypisywane osobie, która posługiwała się tym loginem. Ponadto wykonując obowiązki i zadania z przepisów RODO oraz niniejszej Polityki, każda osoba upoważniona jest zobowiązana wykazać, że przestrzega przepisów RODO i Polityki.

13. **Zasada tajemnicy i jakości haseł dostępowych**

Pod żadnym pozorem nie wolno ujawnić swojego hasła dostępowego (ani przełożonemu, ani Pracodawcy ani żadnej innej osobie nawet pracownikom organów państwowych). Hasło po otrzymaniu od administratora systemu należy zmienić tego samego dnia. **Hasło musi mieć minimum 8 znaków w tym duża litera, mała litera, cyfra i znak specjalny.**

IV. Zasady powierzania przez Administratora przetwarzania danych osobowych podmiotom trzecim

1. **Stosowanie umów powierzenia**

W przypadku zawierania umowy o świadczenie usług, które jest związane z powierzeniem przetwarzania danych osobowych dostawcy usługi, należy zawrzeć pisemną umowę powierzenia przetwarzania zgodną z art. 28 RODO.

2. **Obowiązki i odpowiedzialności Procesorów**

W trakcie tworzenia umowy powierzenia przetwarzania danych osobowych należy bezwzględnie zapisać następujące kwestie:

a) przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora oraz Procesora,

b) Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny,

c) Procesor zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

d) Procesor podejmuje wszelkie środki wymagane na mocy art. 32 RODO,

e) Procesor nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian,

f) Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania Procesor korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa powyżej, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym,

g) Procesor biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO,

h) Procesor uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO,

i) Procesor po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,

j) Procesor udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych art. 28 RODO oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

3. Obowiązki i odpowiedzialności osób nadzorujących Procesorów

Administrator jest zobowiązany osobiście lub poprzez wyznaczonego pracownika nadzorować Procesora czy spełnia wymagania zawartej umowy powierzenia przetwarzania danych.

4. Kontrola Procesorów

W każdej umowie powierzenia przetwarzania danych osobowych, obowiązkowo stosuje się zapis o możliwości przeprowadzenia kontroli (audytu) zgodności przetwarzania powierzonych danych z Umową oraz przepisami. Kontrolę taką może przeprowadzać osoba pisemnie upoważniona przez Administratora.

5. Weryfikacja Procesora

Każdy Procesor przed podpisaniem umowy powierzenia winien być zweryfikowany zgodnie z Procedurą weryfikacji Dostawcy.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Środki organizacyjne zabezpieczenia danych osobowych

W celu wzmocnienia nadzoru nad procesami przetwarzania danych osobowych zostały wprowadzone środki organizacyjne zabezpieczenia danych opisane w niniejszym punkcie.

2. Szkolenia wewnętrzne

Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązania do odbycia minimum jednego szkolenia stacjonarnego lub e-learningowego na rok w zakresie przepisów o ochronie danych osobowych.

3. Wprowadzanie zasad i procedur

Polityka bezpieczeństwa danych osobowych daje podstawę do opracowania i wdrożenia innych procedur ochrony danych osobowych, których proponowany wykaz został wprowadzony w punkcie 9.

4. Planowanie wykonywania kopii zapasowych zbiorów danych osobowych

Dan osobowe przetwarzane w systemach informatycznych są zabezpieczone za pomocą systemów kopii zapasowych nadzorowanych przez Zarząd lub dostawcę IT. Systemy te tworzą kopie zapasowe zgodnie z harmonogramem określonym przez Zarząd lub dostawcę IT.

5. Minimalne środki techniczne zabezpieczenia danych osobowych

Opisane w niniejszym punkcie środki techniczne zabezpieczenia danych są stosowane do zborów danych osobowych jednak nie wszystkie do wszystkich zbiorów. W zależności od kategorii, rodzaju, charakteru, celu przetwarzania danych osobowych są stosowane adekwatne środki bezpieczeństwa i zapewniające zgodność przetwarzania z przepisami RODO.

a. Środki ochrony fizycznej

1) Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem dostępu za pomocą drzwi zamykanych na klucz.
2) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

b. Środki zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2) Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
3) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
4) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
5) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

6. Środki ochrony w oprogramowaniu IT użytkowanym przez Administratora.

1) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych;

2) Dostęp do danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

3) Zastosowano kryptograficzne środki ochrony danych osobowych.

4) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

5) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.