Centrum Monitoringu Danych Sp. z o.o.

POLITYKA BEZPIECZEŃSTWA

w zakresie ochrony danych osobowych

Spis treści

I. Wstęp

1.1. Informacje Ogólne

1. Administratorem Danych Osobowych wdrażającym niniejszą Politykę Bezpieczeństwa w zakresie ochrony danych osobowych jest Centrum Monitoringu Danych sp. z o.o. z siedzibą we Łaziskach Górnych (43-170), ul. Cieszyńska 23G (dalej zwaną również: **CMD** lub **Spółka**).
2. Obowiązki Administratora Danych Osobowych w CMD wykonuje Prezes Zarządu, a jeżeli Prezes Zarządu nie został powołany – Członek Zarządu.
3. Celem niniejszej Polityki jest wdrożenie w Spółce procedur w zakresie ochrony danych osobowych zgodnych z Rozporządzeniem 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 (dalej: **RODO**) oraz innymi przepisami prawa w zakresie ochrony danych osobowych.
4. Polityka Bezpieczeństwa odnosi się do danych osobowych przetwarzanych w: **zbiorach tradycyjnych**, w tym w księgach, wykazach, rejestrach i innych zbiorach ewidencyjnych i **systemach informatycznych**, również w razie przetwarzania danych poza zbiorem danych osobowych.
5. Pod szczególną ochroną Spółki znajdują się szczególne kategorie danych osobowych (tzw. dane wrażliwe) w rozumieniu motywu 51 oraz art. 9 ust. 1 RODO.
6. CMD stosuje odpowiednie środki informatyczne, techniczne i organizacyjne, proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych przez CMD, w szczególności zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, przejęciem przez osobę nieuprawnioną, przetwarzaniem niezgodnym z przepisami prawa oraz ich zmianą, utratą, uszkodzeniem lub zniszczeniem.

1.2. Zasady i Cel Przetwarzania danych osobowych

1. Polityka Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych w CMD oraz ich zabezpieczenia przed nieuprawnionym dostępem.
2. CMD przetwarza dane osobowe w szczególności z poszanowaniem zasad:

a) **zgodności z prawem, rzetelności i przejrzystości** dla osób, których dane dotyczą,

b) **ograniczenia celu**, co oznacza, że dane osobowe zbierane są przez CMD w konkretnych, wyraźnych oraz prawnie uzasadnionych celach,

c) **minimalizacji danych**, co oznacza, że przetwarzanie danych osobowych ograniczone jest do zakresu niezbędnego do celów, w których są przetwarzane,

d) **prawidłowości**, co oznacza, że wszelkie dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, powinny być niezwłocznie usunięte lub sprostowane,

e) **ograniczenia przechowywania**, co oznacza, że dane są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres jednak nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane,

f) **integralności i poufności**, co oznacza, że dane przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

g) **rozliczalności**, co oznacza, że Administrator Danych Osobowych odpowiada za przestrzeganie zasad przetwarzania danych osobowych, jak również musi być w stanie wykazać ich przestrzeganie.

3. Przetwarzanie Danych osobowych możliwe jest w przypadku spełnienia jednej z przesłanek określonych w art. 6 ust. 1 lit. a-f Rozporządzenia, tj. w przypadku, gdy:

a) Osoba, której Dane dotyczą wyraziła zgodę na Przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której Dane dotyczą, lub do podjęcia działań na żądanie osoby, której Dane dotyczą, przed zawarciem umowy;

c) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;

d) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innej osoby fizycznej;

e) Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;

f) Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności

osoby, której Dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której Dane dotyczą, jest dzieckiem.

4. Przetwarzanie Szczególnych kategorii Danych osobowych jest zabronione, chyba że spełniony jest jeden z warunków określonych w art. 9 ust. 2 lit. a-k Rozporządzenia, tj. w przypadku, gdy:
   a) Osoba, której Dane dotyczą, wyraziła wyraźną zgodę na Przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której Dane dotyczą, nie może uchylić zakazu, o którym mowa powyżej;
   b) Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której Dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której Dane dotyczą;
   c) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innej osoby fizycznej, a osoba, której Dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
   d) Przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem, że Przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że Dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których Dane dotyczą;
   e) Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której Dane dotyczą;
   f) Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
   g) Przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której Dane dotyczą;
   h) Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania Systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego

lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem odpowiednich warunków i zabezpieczeń;

i) Przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których Dane dotyczą, w szczególności tajemnicę zawodową;

j) Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, zgodnie z art. 89 ust. 1 Rozporządzenia, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której Dane dotyczą;

k) Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której Dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której Dane dotyczą, jest dzieckiem.

5. Administrator śledzi wytyczne, zalecenia oraz najlepsze praktyki określone przez Europejską Radę Ochrony Danych na podstawie art. 70 ust. 1 lit. d-j i m Rozporządzenia i uwzględnia je w swoich działaniach związanych z Przetwarzaniem danych.

6. Dane osobowe w CMD przetwarzane są w celu:

   a) realizacji celów spółki CMD określonych w umowie spółki, z uwzględnieniem realizowanych modeli biznesowych oraz produktów i usług oferowanych przez Spółkę,

   b) zapewnienia prawidłowej, zgodnej z prawem polityki personalnej oraz bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia i współpracy nawiązywanych przez CMD,

   c) realizacji innych usprawiedliwionych celów CMD, z poszanowaniem praw i wolności osób, których dane dotyczą.

7. W przypadkach wskazanych w RODO osoba, której dane osobowe przetwarzane są przez CMD, otrzyma od CMD wszystkie informacje wskazane w Artykule 13 ust. 1 i 2 RODO – w przypadku, gdy dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, oraz

w Artykule 14 ust. 1 i 2 RODO – jeżeli CMD nie pozyskało danych osobowych od osoby, której dane dotyczą **(obowiązek informacyjny).** Wyjątek stanowią sytuacje określone w Artykule 14 ust. 5 RODO.

1.3. Skróty Używane w Polityce Bezpieczeństwa

Użyte w niniejszej Polityce Bezpieczeństwa sformułowania lub skróty oznaczają:

1. **ADO (Administrator Danych Osobowych)** – Centrum Monitoringu Danych Spółka z ograniczoną odpowiedzialnością z siedzibą w Łaziskach Górnych, ul. Cieszyńska 23G, 43-170 Łaziska Górne, który samodzielnie ustala cele oraz sposoby przetwarzania danych w rozumieniu Artykułu 4 pkt. 7)RODO;
2. **IOD (Inspektor Ochrony Danych)** – osoba wyznaczona przez Administratora Danych Osobowych zgodnie z art. 37 ust.1 RODO, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych;
3. **Upoważniony do administrowania siecią** – pracownik lub współpracownik CMD, upoważniony przez ADO do administrowania oraz zarządzania systemami informatycznymi;
4. **Upoważniony do administrowania siecią IT–** pracownik lub współpracownik CMD, upoważniony przez ADO do administrowania oraz zarządzania systemami informatycznymi;
5. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą), przy czym 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 bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
6. **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7. **Anonimizacja** – rozumie się przez to takie przekształcenie danych osobowych, po którym niemożliwe jest przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej, przy czym proces ten jest nieodwracalny;
8. **Ograniczenie przetwarzania** – rozumie się przez to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
9. **Organ nadzorczy** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych;
10. **Użytkownik** – rozumie się przez to pracownika lub współpracownika CMD Sp. z o.o. upoważnionego na piśmie do przetwarzania danych osobowych, któremu nadano Identyfikator i Hasło;
11. **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi;
12. **Identyfikator** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w Systemie informatycznym;
13. **Dane osobowe zwykłe** – rozumie się przez to Dane osobowe, które nie są danymi osobowymi Szczególnych kategorii, ani Danymi dotyczącymi wyroków i naruszeń prawa;
14. **Szczególne kategorie Danych osobowych** – rozumie się przez to Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
15. **Osoba upoważniona do przetwarzania danych osobowych** – rozumie się przez to pracownika lub współpracownika CMD Sp. z o.o., który został upoważniony przez Administratora do przetwarzania danych osobowych u Administratora;
16. **Powierzenie przetwarzania danych osobowych** – rozumie się przez to zlecenie wykonania czynności przetwarzania danych osobowych przez procesora na rzecz Administratora na podstawie stosownego postanowienia w umowie, zapewniającego warunki bezpieczeństwa danych osobowych zgodnie z przepisami Rozporządzenia lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych, zawartej zgodnie z art. 28 ust. 3 Rozporządzenia;

17. **Procesor** – rozumie się przez to podmiot, który przetwarza Dane osobowe w imieniu Administratora;
18. **Odbiorca danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się Dane osobowe, w tym procesora, z wyjątkiem organów publicznych, które mogą otrzymywać Dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem polskim;
19. **Zgoda osoby, której Dane dotyczą** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której Dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na Przetwarzanie dotyczących jej danych osobowych;
20. **Rozporządzenie** (RODO) – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z Przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie o ochronie danych) (Dz.Urz.UE. L. 119, s. 1).

II. Osoby Odpowiedzialne za Ochronę Danych Osobowych

2.1. Informacje Ogólne

Administrator Danych Osobowych wykonuje obowiązki z zakresu ochrony danych osobowych, które określone są w RODO oraz innych przepisach obowiązującego prawa, na zasadach określonych w niniejszej Polityce.

2.2. Obowiązki Administratora Danych

1. Administrator wykonuje swoje obowiązki przestrzegając zasady podejścia opartego na ryzyku. W szczególności jest on zobowiązany do przeprowadzenia analizy procesów przetwarzania i dokonania ogólnej oceny ryzyka, jakie wiąże się z Przetwarzaniem Danych w konkretnym przypadku, ze szczególnym uwzględnieniem ryzyka dla praw lub wolności osób, których Dane dotyczą.
2. Uwzględniając charakter, zakres, kontekst i cele przetwarzania Danych osobowych w strukturach Administratora oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym

prawdopodobieństwie i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby Przetwarzanie odbywało się zgodnie z Rozporządzeniem i aby móc to wykazać. Środki te są w miarę potrzeby poddawane przeglądom i uaktualniane.

3. Realizując swoje obowiązki Administrator współpracuje z Inspektorem Ochrony Danych, Procesorami, współadministratorami i osobami, których Dane dotyczą, a także organem nadzorczym.
4. Administrator realizuje zadania w zakresie ochrony Danych osobowych, zmierzające do zapewnienia przestrzegania przepisów Rozporządzenia, w tym w szczególności:
   a) nadzoruje opracowanie i aktualizację dokumentacji ochrony Danych osobowych;
   b) nadzoruje przestrzeganie zasad określonych w dokumentacji ochrony Danych osobowych;
   c) zapewnia adekwatne do zagrożeń i kategorii przetwarzanych Danych osobowych środki techniczne i organizacyjne zapewniające ochronę danych osobowych;
   d) zabezpiecza Dane osobowe przed:
      - ujawnieniem osobom nieupoważnionym,
      - zabraniem przez osobę nieuprawnioną,
      - zmianą, utratą, uszkodzeniem lub zniszczeniem;
   e) zapewnia legalność przetwarzania Danych osobowych;
   f) jeżeli zachodzą do tego przesłanki powołuje, a w pozostałych przypadkach może powołać w swojej strukturze inspektora ochrony danych, odpowiedzialnego za nadzór nad Przetwarzaniem Danych osobowych zgodnie z przepisami o ochronie danych osobowych;
   g) zapewnia zapoznanie osób, którym mają być nadane upoważnienia do przetwarzania Danych osobowych (upoważnienia nadawane są przed rozpoczęciem wykonywania czynności przetwarzania danych), z przepisami o ochronie danych osobowych oraz zasadami ochrony danych osobowych poprzez zorganizowanie dla nich szkolenia, prowadzonego przez osobę posiadającą odpowiednią wiedzę i kompetencje z zakresu ochrony danych osobowych;
   h) upoważnia swoich pracowników i współpracowników do przetwarzania Danych osobowych w określonym indywidualnie zakresie;
   i) nadzoruje i dba o zgodne z prawem przekazywanie Danych osobowych (Udostępnianie i Powierzanie);
   j) zapewnia Użytkownikom odpowiednie stanowiska pracy, w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z prawem Przetwarzanie Danych osobowych;
   k) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zasad bezpiecznego przetwarzania Danych osobowych.

5. Administrator gwarantuje poszanowanie praw osób, których Dane dotyczą, a w szczególności prawa do uzyskania informacji o:
   - Administratorze,
   - celu, zakresie i sposobie przetwarzania danych osobowych,
   - terminie, od kiedy i jakie Dane osobowe są przetwarzane,
   - źródle, z którego Dane osobowe pochodzą,
   - sposobie ujawniania danych osobowych oraz ich Odbiorcach.
6. Administrator gwarantuje respektowanie praw osób, których Dane dotyczą, w zakresie:
   - żądania sprostowania lub uaktualnienia Danych osobowych,
   - żądania ograniczenia przetwarzania Danych osobowych,
   - wniesienia sprzeciwu wobec przetwarzania Danych osobowych,
   - żądania usunięcia Danych osobowych,
   - żądania potwierdzenia przetwarzania, dostępu do Danych osobowych i uzyskania ich kopii,
   - żądania przeniesienia Danych osobowych,
   - odwołania zgody na Przetwarzanie Danych osobowych,
   - zaniechania zautomatyzowanego podejmowania decyzji.
7. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym w szczególności:
   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.
8. Administrator prowadzi rejestr czynności przetwarzania, za które odpowiada. W rejestrze tym ujmowane są procesy, dla realizacji których niezbędne jest Przetwarzanie Danych osobowych. Rejestr zawiera, co najmniej następujące informacje:
   a) nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów;
   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 Rozporządzenia, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii Danych;
g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia, a także inne Dane umożliwiające przeprowadzenie wstępnej analizy ryzyka, ogólnej analizy ryzyka oraz oceny skutków dla ochrony Danych.

9. Osobą odpowiedzialną za prowadzenie rejestru czynności przetwarzania jest Administrator, bądź wyznaczony przez Administratora Inspektor Ochrony Danych.
10. Za uzupełnianie i aktualizację cząstkowych rejestrów przedmiotowych dla danych zakresów odpowiedzialne są osoby z poszczególnych działów.
11. Rejestr czynności przetwarzania jest prowadzony w formie elektronicznej.
12. Rejestr czynności przetwarzania jest aktualizowany regularnie, nie rzadziej, niż co 6 miesięcy.
13. Na żądanie organu nadzorczego Administrator udostępnia mu rejestr czynności przetwarzania.

2.3. Inspektor Danych Osobowych

1. Administrator Danych Osobowych powołuje Inspektora Ochrony Danych w rozumieniu Artykułu 37 ust. 1 RODO. Zadania IOD zostały zdefiniowane w Artykule 39 RODO.
2. Administrator publikuje dane kontaktowe Inspektora Ochrony Danych na swojej stronie internetowej oraz w swojej siedzibie.
3. Administrator zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
4. Administrator wspiera Inspektora Ochrony Danych w wypełnianiu przez niego zadań, 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.
5. Inspektor Ochrony Danych nie otrzymuje instrukcji dotyczących wykonywania swoich zadań, nie jest odwoływany, ani karany za wypełnianie swoich zadań.
6. Inspektor Ochrony Danych podlega bezpośrednio Administratorowi Danych.

7. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
8. Do zadań Inspektora Ochrony Danych należą w szczególności:
   a) informowanie Administratora, współpracujących z nim Procesorów oraz pracowników, którzy przetwarzają Dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania Rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie Danych oraz Polityki, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony Danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;
   d) współpraca z organem nadzorczym;
   e) pełnienie 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;
   f) kontakt z osobami, których Dane dotyczą, we wszystkich sprawach związanych z Przetwarzaniem ich Danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia;
   g) prowadzenie i aktualizowanie dokumentacji dotyczącej ochrony Danych osobowych u Administratora;
   h) poddawanie, co najmniej raz w roku, przeglądowi Polityki pod kątem jej aktualności oraz zgodności deklarowanego w niej stanu z prawem;
   i) konsultowanie podpisywanych umów Powierzania przetwarzania Danych osobowych z Procesorami;
   j) podejmowanie, wspólnie z Administratorem, odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania Danych osobowych;
   k) przygotowywanie materiałów szkoleniowych z zakresu ochrony Danych osobowych.
9. W celu prawidłowego wykonywania powierzonych zadań, Inspektor Ochrony Danych jest uprawniony do:
   a) wstępu do pomieszczeń, w których zlokalizowane są Dane osobowe i przeprowadzenia wszystkich niezbędnych czynności kontrolnych w celu oceny zgodności przetwarzania danych z Rozporządzeniem, Ustawą o ochronie danych osobowych i Polityką;

b) żądania od pracowników i współpracowników Administratora, w tym od osób upoważnionych, złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego dotyczącego przetwarzania Danych i ich zabezpieczenia;
c) żądania udostępnienia do kontroli zgodności przetwarzania Danych z przepisami o ochronie danych dokumentacji, urządzeń, nośników oraz Systemów informatycznych służących do przetwarzania Danych osobowych u Administratora;
d) występowania w porozumieniu z Administratorem do Procesora o wyjaśnienia i informacje, dotyczące przetwarzania powierzonych Danych;
e) prowadzenia działań kontrolnych u wskazanego przez Administratora Danych Procesora, w zakresie zgodności przetwarzania powierzonych Danych z przepisami o ochronie Danych oraz umową;
f) wyznaczania, rekomendowania i egzekwowania od pracowników i współpracowników Administratora wykonania zadań związanych z ochroną Danych osobowych;
g) wydawania pracownikom i współpracownikom Administratora wiążących poleceń dotyczących przetwarzania i ochrony Danych osobowych u Administratora.

10. Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

2.4. Upoważniony do Administrowania Siecią

1. Administrator Danych Osobowych nadaje upoważnienie, Upoważnionemu do Administrowania Siecią, do którego zadań należy:
   a) bieżący monitoring oraz zapewnienie ciągłości działania systemu informatycznego i baz danych,
   b) nadzór nad procesem optymalizacji wydajności systemu informatycznego, instalacja oraz konfiguracja sprzętu sieciowego oraz serwerowego oraz oprogramowania systemowego i sieciowego,
   c) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego,
   d) tworzenie kopii zapasowych danych przechowywanych w systemie informatycznym, zarządzanie kopiami awaryjnymi danych osobowych i zasobów umożliwiających ich przetwarzanie, konfiguracja oprogramowania systemowego i sieciowego,
   e) administrowanie oprogramowaniem systemowym, sieciowym i zabezpieczającym dane chronione przed nieupoważnionym dostępem,

f) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,

g) monitorowanie poziomu bezpieczeństwa w systemie informatycznym, implementacja mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej oraz monitorowanie działania systemu informatycznego i przekazywanie informacji o zagrożeniach do ADO i IOD,

h) nadawanie (po zatwierdzeniu ADO) oraz cofania uprawnień użytkownikom systemu informatycznego zgodnie z wnioskami przełożonego,

i) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji i aktywny udział w reagowaniu na działania naruszające system bezpieczeństwa w zakresie ochrony danych osobowych oraz usuwanie ich skutków;

j) kontrola przestrzegania zasad bezpiecznego przetwarzania danych w systemie informatycznym.

2. Pod nieobecność Upoważnionego do Administrowania Siecią, ADO pisemnym (lub w formie korespondencji e-mail) upoważnieniem wyznacza osobę zastępującą Administratora Systemu Informatycznego.

2.5. Upoważniony do Administrowania Siecią IT

1. Administrator Danych Osobowych nadaje upoważnienie, Upoważnionemu do Administrowania Siecią IT, do którego zadań należy:

a) bieżący monitoring oraz zapewnienie ciągłości działania systemu informatycznego i baz danych,

b) nadzór nad procesem optymalizacji wydajności systemu informatycznego, instalacja oraz konfiguracja sprzętu sieciowego oraz serwerowego oraz oprogramowania systemowego i sieciowego,

c) administrowanie oprogramowaniem systemowym, sieciowym i zabezpieczającym dane chronione przed nieupoważnionym dostępem,

d) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego,

e) tworzenie kopii zapasowych danych przechowywanych w systemie informatycznym, zarządzanie kopiami awaryjnymi danych osobowych i zasobów umożliwiających ich przetwarzanie, konfiguracja oprogramowania systemowego i sieciowego,

f) monitorowanie poziomu bezpieczeństwa w systemie informatycznym, implementacja mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej oraz monitorowanie działania systemu informatycznego i przekazywanie informacji o zagrożeniach do ADO i IOD,

g) przeprowadzanie podstawowego szkolenia dla nowo przyjętych pracowników w zakresie korzystania z systemu informatycznego,

h) zapewnienie pomocy użytkownikom przy korzystaniu z systemu informatycznego,

i) zarządzanie licencjami i procedurami ich dotyczącymi,

j) kontrola przestrzegania zasad bezpiecznego przetwarzania danych w systemie informatycznym;

k) czasowy przegląd i weryfikacja m.in.: sprawności użytkowanego sprzętu, legalności zainstalowanego oprogramowania, rozmieszczenia stacji roboczych w poszczególnych pomieszczeniach, przyznanych uprawnień do baz danych i poprawności instalacji aktualizacji systemowych i aktualizacji sygnatur wirusów programu antywirusowego,

l) czasowego testowania, mierzenie i ocenianie skuteczności środków technicznych oraz organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Pod nieobecność Upoważnionego do Administrowania Siecią, ADO pisemnym (lub w formie korespondencji e-mail) upoważnieniem wyznacza osobę zastępującą Administratora Systemu Informatycznego.

2.6. Osoby Upoważnione do Przetwarzania Danych Osobowych

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych (upoważnienie wydawane jest przed rozpoczęciem wykonywania czynności związanych z przetwarzaniem) zobowiązana jest do ich ochrony w sposób zgodny z RODO, innymi aktami prawnymi i wewnętrznymi regulacjami obowiązującymi w CMD. Upoważnienia wydawane są na czas zatrudnienia bądź współpracy na danym stanowisku lub na czas realizacji zleconych czynności.

2. Możliwe jest odwołanie upoważnienia na wniosek przełożonego osoby, której upoważnienie podlega odwołaniu, wskazując jednocześnie powód wymagający odwołania (np. brak dalszej potrzeby uzyskiwania dostępu do danych osobowych przez pracownika).

3. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

4. Każdy pracownik/współpracownik CMD zobowiązany jest:

   a) przestrzegać zasad zachowania bezpieczeństwa i w należyty sposób chronić przed niedozwoloną zmianą, nieupoważnionym dostępem, rozpowszechnianiem, uszkodzeniem lub zniszczeniem dokumentów lub nośników zawierających dane, przetwarzanych zarówno w formie elektronicznej jak i papierowej;

   b) niezwłocznie informować ADO o wszelkich incydentach w zakresie ochrony danych osobowych oraz bezpieczeństwa systemu informatycznego i wykonywać polecenia ADO w zakresie ochrony informacji oraz bezpieczeństwa systemu informatycznego, na zasadach określonych w Załączniku nr 1 do niniejszej Polityki Bezpieczeństwa;

   c) zachować otrzymane indywidualne identyfikatory i hasła w ścisłej tajemnicy;

   d) wszędzie gdzie jest to możliwe – stosować pseudonimizację danych osobowych.

5. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wzór upoważnienia i oświadczenia osoby upoważnionej o zachowaniu poufności stanowią Załącznik nr 2 i Załącznik nr 3 do niniejszej Polityki Bezpieczeństwa.

6. ADO może również udzielić stosownych upoważnień swojemu zastępcy i na wypadek nieobecności osoby upoważnionej, z zachowaniem zasad przewidzianych w RODO i niniejszej Polityce Bezpieczeństwa.

2.7. Zasady Postępowania Osób Upoważnionych

1. Zabrania się:

   a) zapisywania identyfikatorów oraz haseł do systemu informatycznego w miejscach, które umożliwiłyby osobom trzecim zapoznanie się z nimi;

   b) udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej, jak i wydruków) osobom nieupoważnionym;

   c) trwałego lub czasowego kopiowania programów komputerowych;

d) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko;

e) udostępniania osobom postronnym programów komputerowych należących do Spółki oraz udzielania dostępu do wewnętrznej sieci Spółki oraz danych w niej zawartych

f) przechowywania bez zgody ADO na prywatnych nośnikach wymiennych (płyty CD/DVD/Blu-ray, pendrive, dyski przenośne, telefony, karty pamięci, itp.) danych firmy i danych osobowych będących w posiadaniu CMD;

g) wynoszenia poza siedzibę CMD danych firmy i danych osobowych w formie elektronicznej lub papierowej bez pisemnej zgody wydanej przez ADO. Powyższe jest dopuszczalne bez zgody ADO, jeśli jest to związane z bezpośrednim wykonaniem czynności służbowej lub uzgodnioną z ADO pracą zdalną, a dane w formie elektronicznej znajdują się na urządzeniu odpowiednio zabezpieczonym lub zaszyfrowanym.

2. W celu zwiększenia bezpieczeństwa danych oraz sieci komputerowej, każdy użytkownik ma obowiązek usunięcia danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych oraz do trwałego usuwania danych z nośników, które przeznaczone są do likwidacji.

3. O ile Administrator Danych lub inna upoważniona osoba nie postanowi inaczej, pracownik/współpracownik CMD może używać stacji roboczej CMD do celów prywatnych (dotyczy to również przypadków, gdy do celów służbowych używany jest sprzęt prywatny), jednakże w każdym wypadku zobowiązany jest przestrzegać postanowień niniejszej Polityki Bezpieczeństwa, jak również stosować inne środki mające na celu zachowanie bezpieczeństwo danych znajdujących się na powierzonych urządzeniach.

III. Ocena skutków dla ochrony danych

Jeżeli z przeprowadzonej analizy ryzyka wynika, że dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. W celu określenia, czy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator weryfikuje:

a) charakter,
b) zakres,
c) kontekst,

d) cele przetwarzania.

3.1. Kryteria dokonywania oceny skutków dla ochrony danych

1. Ocena skutków dla ochrony danych, jest wymagana w szczególności w przypadku, gdy Przetwarzanie spełnia dwa lub więcej z poniższych kryteriów:
   a) przetwarzanie wiąże się z oceną lub punktacją, w tym profilowaniem i prognozowaniem, w szczególności na podstawie aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której Dane dotyczą;
   b) dochodzi do automatycznego podejmowania decyzji, wywołującej wobec osoby, której Dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływającej;
   c) przetwarzanie obejmuje szczególne kategorie Danych osobowych lub Dane o charakterze wysoce osobistym;
   d) dochodzi do przetwarzania Danych na dużą skalę;
   e) przetwarzanie jest wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których Dane dotyczą, w tym Danych gromadzonych za pośrednictwem sieci lub w ramach Systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie;
   f) dochodzi do dopasowywania lub łączenia zbiorów Danych, w szczególności pochodzących z co najmniej dwóch różnych operacji przetwarzania Danych, przeprowadzonych w różnych celach lub przez różnych Administratorów Danych w sposób wykraczający poza uzasadnione oczekiwania osób, których Dane dotyczą;
   g) przetwarzanie obejmuje Dane osobowe osób wymagających szczególnej opieki, w tym np. dzieci lub pracowników;
   h) następuje innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych;
   i) samo Przetwarzanie uniemożliwia osobom, których Dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.
2. Dla podobnych operacji przetwarzania Danych, wiążących się z podobnym wysokim ryzykiem, Administrator przeprowadza pojedynczą ocenę.
3. Administrator uwzględnia wykazy rodzajów operacji przetwarzania podlegających lub niepodlegających wymogowi dokonania oceny skutków dla ochrony Danych, ustanowione przez organ nadzorczy zgodnie z art. 35 ust. 4 i 5 Rozporządzenia.
4. W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony Danych, Administrator przeprowadza taką ocenę.

3.2. Szczegółowe zasady dotyczące dokonywania oceny skutków dla ochrony danych

1. Ocena skutków dla ochrony Danych powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania. Jeżeli zachodzi taka potrzeba, w szczególności ze względu na zastosowane w projekcie środki techniczne lub organizacyjne, w miarę postępu procesu rozwoju lub w związku z istotną modyfikacją procesu, poszczególne etapy oceny należy powtórzyć.
2. Dokonując oceny skutków dla ochrony Danych, Administrator konsultuje się z Inspektorem Ochrony Danych, a wyniki konsultacji i podjęte decyzje dokumentuje w ramach oceny skutków dla ochrony Danych.
3. Jeżeli dana operacja przetwarzania jest całkowicie lub częściowo realizowana przez Procesora, Administrator konsultuje się z Procesorem.
4. Administrator, jeżeli uzna to za właściwe, zasięga opinii osób, których Dane dotyczą lub ich przedstawicieli. Jeżeli ostateczna opinia Administratora różni się od opinii osób, których Dane dotyczą, Administrator dokumentuje powody podjęcia, bądź niepodjęcia decyzji. Administrator uzasadnia także niezasięgnięcie opinii osób, których Dane dotyczą, jeśli uzna je za niewłaściwe.
5. W stosownych przypadkach Administrator zasięga opinii niezależnych ekspertów z różnych dziedzin (np. prawników, informatyków, ekspertów z zakresu bezpieczeństwa).
6. W razie potrzeby, przynajmniej, gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator dokonuje przeglądu, by stwierdzić, czy Przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
7. Administrator sporządza ocenę skutków dla ochrony danych na piśmie lub w formie elektronicznej.
8. Dokonując oceny skutków dla ochrony Danych, Administrator uwzględnia i dokumentuje, co najmniej:
   a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez Administratora;
   b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   c) ocenę ryzyka naruszenia praw lub wolności osób, których Dane dotyczą;
   d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę Danych osobowych i wykazać przestrzeganie dotyczących jej przepisów, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których Dane dotyczą i innych osób, których sprawa dotyczy.
9. W celu przyczynienia się do zwiększenia zaufania, którym obdarza się Administratora, oraz w celu wykazania rozliczalności i przejrzystości, Administrator publikuje wnioski z oceny skutków dla ochrony Danych na swojej stronie internetowej.

3.3. Uprzednie konsultacje

1. Jeżeli ocena skutków dla ochrony Danych wskaże, że przy braku lub niedostatecznym poziomie planowanych zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko, Przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a Administrator uznaje, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, to przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.
2. Konsultując się z organem nadzorczym, zgodnie z ust. 1, Administrator przedstawia mu:
   a) gdy ma to zastosowanie - odpowiednie obowiązki Administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
   b) cele i sposoby zamierzonego przetwarzania;
   c) środki i zabezpieczenia mające chronić prawa i wolności osób, których Dane dotyczą;
   d) Dane kontaktowe Inspektora Ochrony Danych;
   e) ocenę skutków dla ochrony Danych.
3. Administrator udziela, na żądanie organu nadzorczego, wszelkich innych informacji.
4. Projektując operacje przetwarzania, wymagające uprzednich konsultacji, Administrator uwzględnia określone w art. 36 ust. 2 Rozporządzenia terminy na udzielenie przez organ nadzorczy zaleceń lub podjęcie środków naprawczych.
5. Administrator uwzględnia zalecenia organu nadzorczego wydane na skutek uprzednich konsultacji i stosuje się do innych środków podjętych przez organ.

IV. Środki organizacyjne i Techniczne Zabezpieczenia Danych Osobowych

W celu realizacji założeń niniejszej Polityki Bezpieczeństwa, w CMD wdrożone zostały następujące środki organizacyjne i techniczne zabezpieczenia danych osobowych:

4.1. Zasady Postępowania Osób Upoważnionych

1. wdrożono **Politykę Bezpieczeństwa**, zawierającą również procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
2. opracowano i bieżąco prowadzi się **rejestr czynności przetwarzania** oraz **rejestr kategorii czynności**;
3. wyznaczono Inspektora Ochrony Danych oraz nadano upoważnienia do Administrowania Siecią oraz Administrowania Siecią IT w imieniu Administratora Danych;
4. do przetwarzania danych dopuszczone są **wyłącznie osoby posiadające upoważnienia** nadane przez ADO lub osobę przez niego upoważnioną;
5. osoby mające dostęp do danych osobowych zostały **zapoznane z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego**;
6. osoby upoważnione do przetwarzania danych **zobowiązane są do zachowania ich w tajemnicy**;
7. w miejscu przetwarzania danych utrwalonych w formie papierowej **pracownicy oraz współpracownicy zobowiązani są do stosowania zasady tzw. czystego biurka**. Zasada ta oznacza w szczególności nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym dostęp do nich osobom nieuprawnionym oraz wygaszanie ekranów monitorów w razie chwilowego odejścia od stacji roboczej. Za realizację powyższej zasady odpowiedzialny jest na swoim stanowisku każdy z pracowników;
8. niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywa się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. **z wykorzystaniem niszczarek lub poprzez obsługę podmiotu zewnętrznego** w zakresie niszczenia dokumentów;
9. **obszar**, na którym przetwarzane są dane osobowe, poza godzinami pracy CMD, **chroniony jest alarmem bądź innymi środkami bezpieczeństwa**;
10. urządzenia służące do przetwarzania danych osobowych oraz dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w CMD **w zamykanych elektronicznym kluczem pomieszczeniach** chyba, że Administrator wyraził zgodę na pracę poza siedzibą Spółki. Wówczas użytkownik sprzętu zobowiązany jest przechowywać sprzęt w miejscu uniemożliwiającym jego użytkowanie osobą trzecim ,
11. w umowach z kontrahentami CMD zawierane są **zapisy mające na celu właściwe zabezpieczenie kwestii poufności informacji,**
12. **zasady odnośnie realizacji praw osób**, których dane osobowe dotyczą **określone w RODO**, takie jak prawo dostępu do danych, prawo do przenoszenia danych, prawo wniesienia sprzeciwu czy

prawo do bycia zapomnianym, **określone są w odpowiednich politykach prywatności lub klauzulach informacyjnych,**

13. **każdy nowy pracownik oraz współpracownik**, przed dopuszczeniem do przetwarzania danych osobowych, zostaje **niezwłocznie** przeszkolony z zakresu prawa ochrony danych osobowych. Pracownicy oraz współpracownicy CMD odbywają **również cykliczne szkolenia przypominające** w zakresie bezpieczeństwa danych osobowych. ,
14. procedury określone w niniejszej Polityce Bezpieczeństwa i inne zasady postępowania odnośnie w zakresie bezpieczeństwa systemu informatycznego oraz bezpieczeństwa danych, w tym dane dostępu oraz zakresy upoważnień do przetwarzania danych, weryfikowane są w poszczególnych obszarach struktury organizacyjnej nie rzadziej niż raz na pół roku.

4.2. Środki Techniczne

1. wewnętrzną sieć komputerową zabezpieczono za pomocą **systemu typu firewall**;
2. stanowiska komputerowe wyposażono w **ochronę antywirusową** lub inne analogiczne zabezpieczenie typu Endpoint Protection, w szczególności oznacza to, że systemowo blokowane są urządzenia pamięci masowej z interfejsem USB;
3. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą **indywidualnego identyfikatora** użytkowania;
4. wprowadzono **system podwójnej weryfikacji logowania** do konta pocztowego oraz innych danych umieszczonych na dysku Google;
5. dane osobowe są, co do zasady przechowywane lokalnie na stacjach roboczych, serwerach oraz w chmurze zlokalizowanej w Europejskim Obszarze Gospodarczym;
6. w możliwie szerokim zakresie stosuje się **pseudonimizację danych osobowych**,
7. pliki zawierające dane osobowe przesyłane są pocztą elektroniczną w formie załącznika, którego otworzenie wymaga hasła;
8. dostępna w CMD **sieć Wi-Fi jest zabezpieczona hasłem**, które może być udostępniane wyłącznie pracownikom i współpracownikom. Dodatkowa sieć Wi-Fi może zostać udostępniona innym osobom z zachowaniem dodatkowych zasad bezpieczeństwa określonych przez ADO.

V. Postępowanie w Przypadku Stwierdzenia Naruszenia Bezpieczeństwa Informatycznego

1. W razie stwierdzenia przez użytkownika możliwości naruszenia zabezpieczeń systemu informatycznego, na które mogą wskazywać m.in.:

   a) ślady włamania lub prób włamania do obszaru, w którym znajdują się poszczególne elementy systemu np. serwery, stacje robocze lub urządzenia sieciowe,

   b) stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),

   c) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,

   d) błędy w funkcjonowaniu systemu (np. komunikaty informujące o niespójności, błędach w danych, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),

   e) znaczne spowolnienie działania systemu informatycznego,

   f) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny, jest on zobowiązany natychmiast powiadomić o tym ADO oraz Upoważnionego do Administrowania Siecią oraz Inspektora Danych Osobowych.

2. Upoważniony do Administrowania Siecią lub inna upoważniona osoba powinna w pierwszej kolejności:

   a) zapisać informacje dotyczące zdarzenia, w tym dokładny czas wystąpienia incydentu, czas odnotowania incydentu, lokalizacji incydentu oraz sporządzić opis incydentu,

   b) zabezpieczyć miejsce zdarzenia przed ingerencją osób trzecich, aż do jego pełnego wyjaśnienia lub udokumentować jego stan za pomocą np. zdjęć czy notatki,

   c) niezwłocznie podjąć odpowiednie kroki w celu: (i) powstrzymania lub ograniczenia dostępu do systemu oraz danych osoby niepowołanej, (ii) zminimalizowania okoliczności mogących sprzyjać dalszemu powstawaniu szkód oraz (iii) zabezpieczenia systemu przed usunięciem śladów ingerencji osoby niepowołanej,

   d) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą oraz podpisem,

e) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w szczególności do określenia skali zniszczeń i metody dostępu do systemu osoby niepowołanej,

f) przywrócić normalny stan działania systemu.

3. Po wyeliminowaniu zagrożenia Upoważniony Do Administrowania Siecią, Administrowania Siecią IT lub inna upoważniona osoba przez ADO ma obowiązek dokonać analizy stanu systemu informatycznego, w tym również sprawdzić stan urządzeń wykorzystywanych do przetwarzania danych osobowych, zawartość zbioru danych osobowych, sposób działania programów, jakość komunikacji w sieci telekomunikacyjnej, obecność wirusów komputerowych oraz innego złośliwego oprogramowania.

VI. Postępowanie w Przypadku Stwierdzenia Naruszenia Ochrony Danych Osobowych

1. Naruszenie ochrony Danych osobowych oznacza każde naruszenie bez względu na jego przyczynę prowadzące do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, a w szczególności:
    a) nieautoryzowany dostęp do Danych osobowych;
    b) utratę nośników zawierających Dane osobowe;
    c) nieautoryzowaną modyfikację lub zniszczenie Danych osobowych;
    d) bezpodstawne udostępnienie Danych osobowych;
    e) pozyskiwanie Danych osobowych z nielegalnych źródeł.
2. Osoba, która powzięła informację o zdarzeniu mogącym świadczyć o wystąpieniu przypadku naruszenia danych osobowych, bezpieczeństwa informacji lub ryzyka wystąpienia takich sytuacji, zobowiązana jest do natychmiastowego poinformowania o tym fakcie ADO, Inspektora Danych Osobowych lub osobę przez niego upoważnioną, a następnie stosowania się do podjętych przez te osoby decyzji.
3. O naruszeniu ochrony danych osobowych mogą świadczyć symptomy występujące w szczególności w następujących obszarach:
    a) w obrębie pomieszczeń, szafek lub miejsc przechowywania: (i) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych, w szczególności do serwerowni oraz miejsca gdzie przechowuje są nośniki kopii zapasowych, (ii) włamanie lub próby włamania do szafek, w których przechowywane są, w postaci elektronicznej lub papierowej, nośniki danych osobowych;

b) w obrębie sprzętu informatycznego: (i) kradzież komputera, w którym przechowywane są dane osobowe, (ii) rozkręcona obudowa komputera;

c) w obrębie systemu informatycznego i aplikacji: (i) brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych, (ii) brak możliwości zalogowania się do tej aplikacji mimo wykorzystania prawidłowego identyfikatora i hasła, (iii) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych), (iv) poszerzone uprawnienia w obrębie aplikacji w stosunku do dotychczas przyznanych (na przykład wgląd do szerszego zakresu danych), (v) inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar);

d) zagubienie bądź kradzież przenośnego nośnika danych;

e) zgłoszenie przypadku naruszenia danych osobowych otrzymanych od osoby trzeciej.

4. Powiadomienie o naruszeniu ochrony danych osobowych powinno obejmować:
   a) opis naruszenia ochrony Danych osobowych;
   b) określenie sytuacji, miejsca i czasu, w jakim stwierdzono naruszenie ochrony Danych osobowych;
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia;
   d) określenie znanych danej osobie sposobów zabezpieczenia Systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

5. Po otrzymaniu zgłoszenia określonego w ust. -2, ADO wyznacza IOD bądź inną osobę upoważnioną według posiadanych kwalifikacji do stwierdzenia, czy rzeczywiście doszło do naruszenia ochrony danych osobowych, sprawdzenia okoliczności zdarzenia oraz wyjaśnienia jego przyczyn, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich oraz podjęcie stosownych kroków zaradczych.

6. Administrator lub wyznaczona przez Administratora osoba określa, na podstawie zebranych informacji, przyczyny zaistnienia incydentu i przekazuje te informacje - IOD. Jeśli incydent był spowodowany celowym działaniem, ADO może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym CMD.

7. Administrator lub inna upoważniona przez Administratora osoba podejmuje wszelkie działania mające na celu:
   a) minimalizację negatywnych skutków zdarzenia i ich późniejsze zupełne usunięcie;
   b) wyjaśnienie okoliczności zdarzenia;
   c) zabezpieczenie dowodów zdarzenia;
   d) umożliwienie dalszego bezpiecznego przetwarzania Danych osobowych.

8. W celu realizacji procedury postępowania w przypadku naruszenia ochrony Danych osobowych, Administrator lub wyznaczona przez Administratora osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
    a) żądania wyjaśnień od pracowników i współpracowników;
    b) korzystania z pomocy konsultantów (w tym zewnętrznych podmiotów);
    c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania Danych osobowych.
9. Odmowa udzielenia przez pracownika wyjaśnień lub współpracy z Administratorem może być traktowana, jako ciężkie naruszenie podstawowych obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1) Kodeksu pracy.
10. Administrator lub wyznaczona przez Administratora osoba, po stwierdzeniu naruszenia ochrony Danych osobowych, opracowuje raport końcowy, w którym przedstawia:
    a) okoliczności i charakter powstałego naruszenia, w tym:
        - kategorie i przybliżoną liczbę osób, których Danych dotyczy naruszenie,
        - kategorie i przybliżoną liczbę Danych osobowych, których dotyczy naruszenie,
        - możliwe konsekwencje powstałego naruszenia;
    b) wnioski i zalecenia ograniczające możliwość wystąpienia podobnego zdarzenia w przyszłości;
    c) opis podjętych działań zaradczych.
11. W przypadku stwierdzenia **naruszenia ochrony Danych osobowych** Administrator bez zbędnej zwłoki – **nie później jednak, niż w terminie 72 godzin od stwierdzenia naruszenia** – zgłasza je organowi nadzorczemu. Jeżeli zgłoszenie zostanie dokonane po upływie 72 godzin – należy dołączyć wyjaśnienie przyczyn opóźnienia**.**
12. Jeżeli w zakreślonym wyżej czasie Administrator nie jest w stanie zgromadzić i przekazać organowi nadzorczemu wszystkich wymaganych informacji – może ich udzielać sukcesywnie – bez zbędnej zwłoki.
13. Zgłoszenie naruszenia ochrony Danych osobowych nie jest wymagane, jeśli jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Za dokonanie oceny istnienia lub nieistnienia powyższego ryzyka odpowiada Administrator.
14. W sytuacji, kiedy naruszenie ochrony Danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – Administrator bez zbędnej zwłoki zawiadamia także osobę, której Dane dotyczą, o wystąpieniu naruszenia.
15. W zawiadomieniu, o którym mowa powyżej, umieszcza się informacje w zakresie:
    a) imienia i nazwiska oraz danych kontaktowych Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji nt. naruszenia;
    b) konsekwencji naruszenia ochrony Danych osobowych, które mogą pojawić się dla osoby, której Dane dotyczą w związku z zaistnieniem naruszenia;
    c) środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach, także środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
16. Zawiadomienie, o którym mowa powyżej, nie jest wymagane w następujących przypadkach:
    a) zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony, które zostały zastosowane do Danych osobowych, których dotyczy naruszenie – w szczególności środki takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych Danych;

b) następnie zostały zastosowane środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której Dane dotyczą;
c) wymagałoby to niewspółmiernie dużego wysiłku – w takim wypadku należy wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby, których Dane dotyczą, zostają poinformowane w równie skuteczny sposób.

17. Inspektor Danych Osobowych lub inna osoba wyznaczona przez ADO prowadzi rejestr naruszeń i incydentów.

VII. Budynek i Pomieszczenia, w Których Wykonywane są Operacje Przetwarzania Danych Osobowych

1. Z zastrzeżeniem ust. 3 poniżej oraz punktu 3.2 ust. 5, wszelkie dane osobowe przetwarzane są przez CMD w budynku zlokalizowanym przy ul. Cieszyńskiej 23G w Łaziskach Górnych. Dane osobowe przetwarzane w formie papierowej przechowywane są w oddzielnych pomieszczeniach zamykanych na elektroniczny klucz, do którego dostęp mają tylko osoby upoważnione.
2. W uzasadnionych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na urządzeniach przenośnych), z zachowaniem ostrożności podczas transportu danych, przechowywania oraz użytkowania (m.in. zastosowanie środków ochrony kryptograficznej dla danych, które znajdują się na komputerach przenośnych).
3. Dane osobowe przetwarzane są przez CMD również w chmurze oraz serwerach zlokalizowanych w Europejskim Obszarze Gospodarczym.
4. W sytuacjach określonych w RODO, CMD zawiera umowę dotyczącą powierzenia przetwarzania danych lub umowę o udostępnienie danych z podmiotem trzecim.

VIII. Powierzenie przetwarzania danych osobowych

1. Przetwarzanie Danych przez Procesora, z którego usług korzysta Administrator, odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i Administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj Danych osobowych oraz kategorie osób, których Dane dotyczą, obowiązki i prawa Administratora.

2. Przetwarzanie Danych przez Procesora, z którego usług korzysta Administrator, nie powoduje zmiany właściwego Administratora.
3. Powierzenie Danych osobowych podmiotom mającym siedzibę w jednym z państw EOG podlega ogólnym zasadom powierzenia Danych osobowych wynikającym z Rozporządzenia. Powierzenie Danych osobowych podmiotom mającym siedzibę w państwie trzecim lub organizacji międzynarodowej wymaga dodatkowo wypełnienia przesłanek i obowiązków nałożonych przepisami rozdziału V Rozporządzenia.
4. Dokonując wyboru Procesora, Administrator korzysta z usług tylko takich Procesorów, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby Przetwarzanie Danych spełniało wymogi przepisów i chroniło prawa osób, których Dane dotyczą. Administrator bierze pod uwagę w szczególności fachową wiedzę, wiarygodność i zasoby Procesora.
5. Jeżeli inny podmiot polecił Administratorowi Przetwarzanie Danych osobowych w jego imieniu, Administrator, działając jako podmiot przetwarzający, zobowiązany jest:
   a) przetwarzać Dane osobowe wyłącznie na udokumentowane polecenie powierzającego;
   b) zapewnić, by osoby upoważnione do przetwarzania Danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   c) podejmować wszelkie środki dotyczące bezpieczeństwa przetwarzania, wymagane na mocy art. 32 Rozporządzenia;
   d) przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 Rozporządzenia;
   e) uwzględniając charakter przetwarzania, w miarę możliwości pomagać powierzającemu Dane poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której Dane dotyczą;
   f) uwzględniając charakter przetwarzania oraz dostępne informacje, pomagać powierzającemu Dane wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia;
   g) po zakończeniu świadczenia usług związanych z Przetwarzaniem - zależnie od decyzji powierzającego – usunąć lub zwrócić powierzającemu wszelkie Dane osobowe oraz usunąć wszelkie istniejące kopie tych Danych, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie Danych osobowych;
   h) udostępniać powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym ustępie oraz umożliwić powierzającemu lub upoważnionej przez niego osobie przeprowadzenie audytów, w tym inspekcji i przyczyniać się do nich;
   i) prowadzić rejestr kategorii czynności przetwarzania.
6. Umowa, na podstawie której odbywa się Przetwarzanie Danych, powinna określać:
   a) przedmiot przetwarzania,
   b) czas trwania przetwarzania,
   c) charakter przetwarzania,
   d) cel przetwarzania,
   e) rodzaj powierzonych danych osobowych,
   f) kategorie osób, których Dane dotyczą,
   g) obowiązki i prawa Administratora,
   h) obowiązki Procesora, w tym dotyczące przeprowadzania audytu przez Administratora,

i) warunki dalszego powierzenia przetwarzania danych, w szczególności wskazanie, czy wymaga ono szczegółowej, czy ogólnej pisemnej zgody Administratora.

7. Administrator odnotowuje w rejestrze kategorii czynności przetwarzania umowy powierzenia przetwarzania w sytuacji, gdy jest on podmiotem przetwarzającym.
8. Administrator w miarę potrzeby przeprowadzi audyt Procesora w zakresie zgodności wykonywania przez niego czynności przetwarzania Danych osobowych z postanowieniami umowy, oraz obowiązującymi przepisami o ochronie Danych, w szczególności w celu sprawdzenia wykonywania przez Procesora ciążących na nim obowiązków.
9. Administrator przekaże Procesorowi, po przeprowadzonym audycie, pisemne zalecenia i wytyczne wraz z terminem ich realizacji, dotyczące w szczególności zabezpieczenia danych osobowych pod względem technicznym i organizacyjnym oraz sposób wykonywania czynności ich przetwarzania.
10. Administrator może zrezygnować z przeprowadzenia audytu u Procesora.

IX. Zasady ujawniania danych odbiorcom innym, niż Procesorowi

1. Ujawnianie Danych osobowych może nastąpić tylko po uprzednim przedstawieniu wniosku o ich ujawnienie.
2. Wniosek powinien mieć formę pisemną lub dokumentową i zawierać:
    a) oznaczenie wnioskodawcy;
    b) wskazanie podstaw legalizacyjnych uzasadniających żądanie ujawnienia;
    c) określenie rodzaju i zakresu żądanych informacji oraz formy ich przekazania lub udostępnienia;
    d) wskazanie imienia, nazwiska i stanowiska osoby upoważnionej do otrzymania Danych osobowych lub zapoznania się z ich treścią.
3. Ujawnianie Danych osobowych na podstawie ustnego wniosku zawierającego wszystkie cztery elementy określone w ust. 2 może nastąpić wyłącznie, gdy zachodzi konieczność niezwłocznego działania.
4. Osoba udostępniająca Dane osobowe jest obowiązana zażądać od osoby uprawnionej pokwitowania ujawnienia danych, zawierającego informacje przekazane na podstawie wniosku złożonego na piśmie albo potwierdzenie faktu uzyskania wglądu w treść informacji.
5. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie otrzymania informacji. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę.
6. Ujawnianie Danych osobowych podmiotom mającym siedzibę w jednym z państw Europejskiego Obszaru Gospodarczego podlega ogólnym zasadom przetwarzania Danych osobowych wynikającym z Rozporządzenia. Administrator danych z EOG, tak samo jak Administrator przetwarzający Dane na terytorium Polski, jest zobowiązany m.in. do wypełnienia jednego z warunków legalności przetwarzania Danych osobowych oraz do wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających odpowiedni stopień bezpieczeństwa danych.

X. Prawa podmiotu danych

1. W celu realizacji swoich praw, podmiot danych kontaktuje się z Inspektorem Ochrony Danych. W innym wypadku podmiot Danych powinien kontaktować się z Administratorem Danych.
2. Przetwarzanie Danych osobowych przez Administratora powinno być zgodne z prawem i rzetelne. Dla osób, których Dane dotyczą, powinno być przejrzyste, że dotyczące ich Dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te Dane osobowe są lub będą przetwarzane. Wszelkie informacje i wszelkie komunikaty związane z Przetwarzaniem tych Danych osobowych powinny być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których Dane dotyczą, o tożsamości Administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych Danych osobowych ich dotyczących.
3. Osobom, których Dane dotyczą, należy uświadamiać ryzyka, zasady, zabezpieczenia i prawa związane z Przetwarzaniem Danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim Przetwarzaniem. W szczególności, konkretne cele przetwarzania Danych osobowych przez Administratora, powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.
4. Jeżeli Dane osobowe osoby, której Dane dotyczą, zbierane są od tej osoby, Administrator podczas pozyskiwania Danych osobowych podaje jej informacje określone w art. 13 ust. 1, 2 i 3 Rozporządzenia, chyba że ta osoba dysponuje już tymi informacjami.
5. Jeżeli Danych osobowych nie pozyskano od osoby, której Dane dotyczą, Administrator podaje jej informacje określone w § 14 ust. 1, 2 i 4 Rozporządzenia, chyba że:
    a) osoba ta dysponuje już tymi informacjami;
    b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
    c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której Dane dotyczą; lub
    d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.
6. Informacje, o których mowa w ust. 5, Administrator podaje:
    a) w rozsądnym terminie po pozyskaniu Danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania Danych osobowych;
    b) jeżeli Dane osobowe mają być stosowane do komunikacji z osobą, której Dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której Dane dotyczą; lub
    c) jeżeli planuje się ujawnić Dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.
7. Jeżeli podstawą przetwarzania Danych osobowych jest Zgoda osoby, której Dane dotyczą, Administrator musi być w stanie wykazać, że osoba, której Dane dotyczą, wyraziła zgodę na Przetwarzanie swoich Danych osobowych.

8. Zgoda powinna być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, którym osoba, której Dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na Przetwarzanie dotyczących jej Danych osobowych w konkretnym celu. Na różne cele przetwarzania powinna być odbierana osobna Zgoda.
9. Jeżeli osoba, której Dane dotyczą, wyrazi zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
10. Administrator umożliwia osobie, której Dane dotyczą, wycofanie zgody w dowolnym momencie w taki sam sposób, w jaki nastąpiło jej wyrażenie. Administrator w jasny i przejrzysty sposób informuje osobę, której Dane dotyczą, o możliwości wycofania zgody. W przypadku wycofania zgody, Administrator niezwłocznie zaprzestaje przetwarzania Danych tej osoby.
11. Wyrażenie zgody na Przetwarzanie Danych nie może stanowić warunku zawarcia umowy lub świadczenia usługi.
12. W przypadku planu zmiany celu przetwarzania Danych, Administrator ponownie zwraca się do osoby, której Dane dotyczą, o zgodę na Przetwarzanie jej Danych, co do zmienianego celu.
13. Administrator umożliwia osobie, której Dane dotyczą, uzyskanie potwierdzenia, czy przetwarzane są Dane osobowe jej dotyczące, a jeżeli ma to miejsce, również uzyskanie dostępu do nich i informacji określonych w art. 15 ust. 1 i 2 Rozporządzenia.
14. Administrator dostarcza osobie, której Dane dotyczą, kopię Danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której Dane dotyczą, Administrator pobiera odpowiednio opłatę w wysokości, która wynika z kosztów administracyjnych. Jeżeli osoba, której Dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w korespondencji mailowej.
15. Administrator dokonuje sprostowania nieprawidłowych Danych na żądanie osoby, której Dane dotyczą, niezwłocznie po otrzymaniu takiego żądania.
16. Administrator uzupełnia niekompletne Dane osobowe na żądanie osoby, której Dane dotyczą, niezwłocznie po otrzymaniu takiego żądania. Administrator odmawia uzupełnienia Danych osobowych, gdy jest ono niezgodne z celami przetwarzania.
17. Administrator weryfikuje merytoryczną poprawność Danych osobowych wskazanych w żądaniu sprostowania lub uzupełnienia Danych.
18. Administrator informuje o sprostowaniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą o tych odbiorcach, jeżeli osoba, której dane dotyczą tego zażąda.
19. Na żądanie osoby, której Dane dotyczą, Administrator usuwa dotyczące jej Dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
    a) Dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b) osoba, której Dane dotyczą, cofnęła zgodę, na której opiera się Przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
    c) osoba, której Dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której Dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 Rozporządzenia wobec przetwarzania;

d) Dane osobowe były przetwarzane niezgodnie z prawem;
e) Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;
f) Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

20. Administrator może odmówić usunięcia Danych w zakresie, w jakim jest ono niezbędne:
    a) do korzystania z prawa do wolności wypowiedzi i informacji;
    b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
    c) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, o ile prawdopodobne jest, że usunięcie Danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
    d) do ustalenia, dochodzenia lub obrony roszczeń.
21. Administrator zaniecha przetwarzania Danych osobowych niezwłocznie po otrzymaniu sprzeciwu osoby, której Dane dotyczą. Administrator może nie uwzględnić sprzeciwu, jeżeli wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której Dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
22. Administrator zaniecha przetwarzania Danych osobowych do celów marketingu bezpośredniego, niezwłocznie po otrzymaniu sprzeciwu osoby, której Dane dotyczą, wobec przetwarzania do takich celów.
23. Żądanie usunięcia danych lub sprzeciw osoba, której Dane dotyczą, może złożyć w formie pisemnej, elektronicznej, w tym za pośrednictwem strony internetowej Administratora, telefonicznie lub ustnie do protokołu w siedzibie Administratora.
24. Jeżeli Przetwarzanie odbywa się na podstawie zgody osoby, której Dane dotyczą i w sposób zautomatyzowany, Administrator umożliwia osobom, których Dane dotyczą, otrzymanie kopii ich Danych osobowych w formie elektronicznej, w formacie *.xml, *.json, *.csv lub innym powszechnie używanym, ustrukturyzowanym formacie, nadającym się do odczytu, umożliwiającym tej osobie przesłanie Danych do innego dostawcy usług, odczytanie Danych w sposób automatyczny przez innego dostawcę i korzystanie z Danych w ramach usług innego dostawcy.
25. O ile jest to technicznie możliwe, na żądanie osoby, której Dane dotyczą, Administrator przesyła Dane osobowe bezpośrednio innemu Administratorowi.
26. Administrator może odmówić udostępnienia kopii Danych, jeżeli mogłoby ono niekorzystnie wpływać na prawa i wolności innych.
27. Administrator ogranicza Przetwarzanie Danych na żądanie osoby, której Dane dotyczą, w następujących przypadkach:
    a) osoba, której Dane dotyczą, kwestionuje prawidłowość Danych osobowych - na okres pozwalający Administratorowi sprawdzić prawidłowość tych Danych;
    b) Przetwarzanie jest niezgodne z prawem, a osoba, której Dane dotyczą, sprzeciwia się usunięciu Danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

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 na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której Dane dotyczą.

28. Administrator przechowuje Dane, których Przetwarzanie zostało ograniczone zgodnie z ust. 27, a w pozostałym zakresie przetwarza je wyłącznie:
    a) za zgodą osoby, której Dane dotyczą, lub
    b) w celu ustalenia, dochodzenia lub obrony roszczeń, lub
    c) w celu ochrony praw innej osoby fizycznej lub prawnej, lub
    d) z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
29. Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której Dane dotyczą, która żądała ograniczenia.
30. Administrator informuje o ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
31. Administrator dopuszcza podejmowanie decyzji, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołują skutki prawne wobec osoby, której Dane dotyczą, lub w podobny sposób istotnie na nią wpływają, wyłącznie, jeżeli taka decyzja:
    a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której Dane dotyczą, a Administratorem;
    b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której Dane dotyczą; lub
    c) opiera się na wyraźnej zgodzie osoby, której Dane dotyczą.

XI. Retencja Danych

1. Dla każdego rozpoznanego procesu przetwarzania danych osobowych (czynności przetwarzania) należy określić okres, przez który dane osobowe, przetwarzane w ramach danego procesu, będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.

2. Kryteria ustalania okresu, o których mowa w ust. 1 mogą być określane w poniższy sposób:
    a) przez okres wymagany przepisami prawa,
    b) do czasu zakończenia realizacji umowy i przedawnienia roszczeń,
    c) do czasu wycofania zgody lub zgłoszenia sprzeciwu,
    d) przez okres ustalony przez administratora danych.

3. Każdy nowy proces przetwarzania danych osobowych będzie bez zbędnej zwłoki zgłaszany do ADO oraz IOD, wraz z informacją o zakładanym czasie przetwarzania danych w danym procesie.

4. Informacje, co do ustalonego czasu, przez który dane osobowe będą przechowywane, lub kryteria ustalania tego okresu, będą umieszczane w klauzulach informacyjnych podczas realizacji procesu zbierania danych osobowych, zarówno bezpośrednio od osoby, której dane dotyczą (zgodnie z art. 13 RODO) oraz w sytuacji zbierania danych z innych źródeł (zgodnie z art. 14 RODO).

5. Dane o nowym procesie przetwarzania danych osobowych lub zmianie odnośnie rozpoznanych procesów przetwarzania danych będą następnie umieszczane w rejestrze czynności przetwarzania.

6. Osoby odpowiedzialne organizacyjnie za obszar, w którym realizowany jest dany proces zbierania danych osobowych, będą odpowiedzialne za realizację wymogów wskazanych w ust. 4 i 5 powyżej.

7. Pracownik lub współpracownik mający dostęp do danych osobowych będzie odpowiedzialny za bieżące wykonywanie polityki w zakresie retencji danych i po uzgodnieniu z przełożonym.

8. W przypadku zakończenia ustalonego czasu retencji danych osobowych w danym procesie, osoba, o której mowa w ust. 6 powyżej, podejmie niezbędne działania w celu usunięcia danych z nośników elektronicznych lub dokumentacji papierowej (w przypadku danych zawartych na nośnikach elektronicznych – z udziałem lub po uzgodnieniu z Upoważnionym do Administrowania siecią IT). Szczegółowe zasady dotyczące usunięcia danych z nośników elektronicznych oraz dokumentacji papierowej uregulowane zostały w Procedurze niszczenia danych, stanowiącej Załącznik nr 4 do niniejszej Polityki bezpieczeństwa.

9. W razie wątpliwości, działania określone powyżej zostaną skonsultowane z Inspektorem Ochrony Danych.

10. Administrator Ochrony Danych przy współpracy z Inspektorem Ochrony Danych lub osoba przez niego wskazana okresowo monitoruje realizację wymogów dotyczących usuwania lub anonimizacji danych osobowych.

XII. Postanowienia Końcowe

1. Wszyscy pracownicy oraz współpracownicy CMD są zobowiązani do zapoznania się z treścią niniejszej Polityki Bezpieczeństwa.

2. ADO przy współpracy z IOD oraz Upoważnionymi podejmuje działania mające na celu cykliczną, nie rzadziej niż raz w roku, weryfikację stosowanych procedur i zabezpieczeń poprzez przeprowadzenie stosownego audytu, w tym audytu wewnętrznego.

3. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych w wersji papierowej powinien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

4. Zakres szkolenia, o którym mowa powyżej będzie obejmować zaznajomienie użytkownika z regulacjami dotyczącymi ochrony danych osobowych, niniejszą Polityką Bezpieczeństwa oraz innymi dokumentami obowiązującymi w tym zakresie w CMD. Szkolenie zostanie zakończone podpisaniem przez osobę uczestniczącą w szkoleniu oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu, jak również zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych.

5. Polityka Bezpieczeństwa wchodzi w życie z dniem jej podpisania.

6. Załączniki stanowią integralną część niniejszej Polityki Bezpieczeństwa.

XIII. Załączniki

Załącznik nr 1 - Zasady postępowania w razie incydentów w zakresie bezpieczeństwa systemu informatycznego oraz przypadków naruszeń danych osobowych

Załącznik nr 2 - Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 3 - Wzór upoważnienia i oświadczenia osoby upoważnionej o zachowaniu poufności.

Załącznik nr 4 - Procedura niszczenia danych.

…… ……

(Malgorzata Bugajska- Członek Zarządu)

Załącznik Nr 1

Incydenty naruszenia bezpieczeństwa systemu informatycznego lub ochrony danych osobowych- zasady postępowania w Centrum Monitoringu Danych Sp. z o.o.

1. Zasady postępowania w razie stwierdzenia naruszenia bezpieczeństwa systemu informatycznego i naruszenia ochrony danych osobowych **określone zostały w Polityce Bezpieczeństwa w zakresie ochrony danych osobowych. Każdy pracownik i współpracownik CMD zobowiązany jest do zapoznania się** z tym dokumentem oraz niniejszymi zasadami postępowania.

2. **Pamiętaj!** Zgodnie z RODO w razie naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu (Prezes Urzędu Ochrony Danych Osobowych).

3. Oznacza to, że w takich sytuacjach **bardzo istotny jest czas reakcji**. Jeżeli w Twojej ocenie mogło dojść do naruszenia bezpieczeństwa systemu informatycznego lub ochrony danych osobowych, **natychmiast zgłoś taki incydent: Inspektorowi Danych Osobowych bądź osobie wskazanej w Polityce Bezpieczeństwa.**

4. **Jeżeli masz wątpliwość**, czy powstała sytuacja stanowi incydent, o którym mowa powyżej, **nie rozstrzygaj tego samodzielnie – poinformuj odpowiednią osobę, zgodnie z Polityka Bezpieczeństwa.**

5. Incydent w zakresie naruszenia bezpieczeństwa systemu informatycznego lub ochrony danych osobowych może mieć charakter techniczny lub prawny, w związku z tym – **dla ułatwienia zasad działania – zawsze zgłaszaj incydent na adres mailowy: iod@monitoringdanych.pl**

6. Inspektor Danych Osobowych może przekierować zgłoszoną sprawę do Upoważnionego Administrowania Siecią oraz Administrowania Siecią IT w kopii do Administratora Danych lub wskazanej przez niego osoby.

7. Jeżeli incydent został zgłoszony bezpośrednio do właściwej osoby zgodnie z Polityką Bezpieczeństwa, taka osoba również informuje Inspektora Danych Osobowych zgodnie z powyższymi zasadami.

Załącznik Nr 2

WZÓR EWIDENCJI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Centrum Monitoringu Danych Sp. z o.o.
[ADMINISTRATOR DANYCH]
EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Rok	LP	Obszar	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia do przetwarzania danych osobowych	Uwagi

Załącznik Nr 3

WZÓR UPOWAŻNIENIA I OŚWIADCZENIA OSOBY UPOWAŻNIONEJ O ZACHOWANIU POUFNOŚCI

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA* Nr……..
do przetwarzania danych osobowych

w systemach informatycznych lub w zbiorach w wersji papierowej
w Centrum Monitoringu Danych Spółka z ograniczoną odpowiedzialnością
z siedzibą w Łaziskach Górnych, ul. Cieszyńska 23G, 43-170 Łaziska Górne

_____

Część I – wersja podstawowa upoważnienia

Z dniem DD-MM-RRRR upoważniam / anuluję upoważnienie*

Panią/Pani/Pana* *(podać imię i nazwisko)*

pracownika *(podać nazwę jednostki lub działu),* zatrudnionego na stanowisku *(podać stanowisko)* do przetwarzania danych osobowych

_____

Część II – wersja rozszerzona upoważnienia

w zbiorach: podać nazwy zbiorów (zakres/typ/kategorie osób)

w zakresie: (WG) wglądu, (W) wprowadzania, (M) modyfikacji, (U) usuwania, (A) archiwizacji, (U) udostępniania innym podmiotom, (I) koniecznym do wykonywania obowiązków pracowniczych*

_____

Upoważnienie dotyczy przetwarzania danych osobowych **w systemach informatycznych:** podać nazwy systemów lub programów/nie dotyczy*

_____

Upoważnienie dotyczy przetwarzania danych osobowych **w zbiorach papierowych**: podać nazwy tych zbiorów/nie dotyczy*

_____

....
(miejscowość i data) (pieczęć i podpis Administratora)

EWIDENCJA UŻYTKOWNIKA SYSTEMÓW INFORMATYCZNYCH

Nazwa systemu / programu: podać nazwę

Identyfikator użytkownika: podać identyfikator
Zakres uprawnień użytkownika: np. dostęp do modułu kadry, drukowanie list płac, odczyt, zapis
Data zarejestrowania w systemie: DD-MM-RRRR
Data wyrejestrowania użytkownika: DD-MM-RRRR

.....
(podpis Administratora)

*) niepotrzebne skreślić

.....
(miejscowość, data)

.....
(imię i nazwisko Pracownika/Współpracownika)

.....
(stanowisko)

OŚWIADCZENIE
O OBOWIĄZKU ZACHOWANIA W POUFNOŚCI DANYCH OSOBOWYCH
w Centrum Monitoringu Danych Sp. z o.o.

W związku z dopuszczeniem mnie do przetwarzania danych osobowych w ramach obowiązków pełnionych przeze mnie w **Centrum Monitoringu Danych sp. z o.o.** (dalej jako: „Administrator danych"), niniejszym oświadczam, że:

1. Zapoznałem/am się z wewnętrznymi regulacjami obowiązującymi u Administratora danych w zakresie danych osobowych oraz obowiązkami w zakresie ochrony danych osobowych wynikającymi z przepisów prawa, w tym w szczególności z 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 (RODO) i **zobowiązuję się do ich przestrzegania**;
2. W razie uzyskania dostępu do danych osobowych i informacji poufnych, **zobowiązuję się zachować ich treść w tajemnicy w trakcie współpracy z Administratorem danych oraz po jej zakończeniu;**
3. **Zobowiązuję się do niewykorzystywania** danych osobowych w celach niezgodnych z zakresem i celem zadań powierzonych przez Administratora danych;
4. **Zapewnię bezpieczeństwo przetwarzanych przeze mnie danych osobowych** poprzez ich ochronę przed przypadkowym lub niepowołanym dostępem, przetwarzaniem, nieuzasadnioną modyfikacją, utratą, zniszczeniem i niezgodnym z prawem ujawnieniem lub pozyskaniem;

5. **Zachowam w tajemnicy dane osobowe i sposoby ich zabezpieczeń**, do których uzyskam dostęp w trakcie współpracy z Administratorem danych jak i po jej zakończeniu;

6. **Znane mi są zasady odpowiedzialności prawnej** za przetwarzanie danych osobowych niezgodne z RODO oraz innymi przepisami prawa oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji dotyczących ochrony danych osobowych, kodeksu pracy oraz kodeksu cywilnego;

7. Przyjmuję do wiadomości, że Informacjami Chronionymi są wszelkie nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjno-finansowe lub inne informacje posiadające wartość gospodarczą, których wykorzystanie, przekazanie lub ujawnienie osobie nieuprawnionej zagraża lub narusza interesy CMD sp. z o.o. Dotyczy to zarówno informacji przekazywanych w formie elektronicznej, pisemnych, ustnych, czy w jakiejkolwiek innej formie, w tym sam fakt przekazania takich informacji, z wyłączeniem przypadków, w których CMD sp. z o.o. zezwoli na ich upublicznienie;

8. Zobowiązuję się nie ujawniać Informacji Poufnych większej liczbie swoich pracowników, współpracowników i doradców niż jest to konieczne;

9. Zapewniam, że wszelkie osoby, którym ujawnione zostaną Informacje Poufne, zostaną pisemnie zobowiązane do zachowania ich w tajemnicy oraz podpiszą deklaracje o zachowaniu poufności;

10. Jestem świadomy, że po zakończeniu niniejszej współpracy obowiązek zachowania tajemnicy w zakresie przekazanych w trakcie niniejszej współpracy Informacji Poufnych nie ustaje,(tj. pozostaje w mocy jako bezterminowe zobowiązanie), chyba, że informacje te staną się powszechnie znane;

11. Jestem świadomy, iż w przypadku naruszenia obowiązku zachowania tajemnicy ponoszę odpowiedzialność za wszelkie szkody spowodowane ujawnieniem Informacji Poufnych na zasadach określonych w obowiązujących przepisach prawa. Jednocześnie oświadczam, iż mam świadomość, że naruszenie powyższego zobowiązania może stanowić czyn nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (j.t. Dz. U. 2022, nr 153, poz. 1233 ze zm.).

……

(data i podpis Pracownika/Współpracownika)

Załącznik Nr 4

PROCEDURA NISZCZENIA DANYCH

w Centrum Monitoringu Danych Spółka z ograniczoną odpowiedzialnością z siedzibą w Łaziskach Górnych, ul. Cieszyńska 23G, 43-170 Łaziska Górne

I. POSTANOWIENIA WSTĘPNE

1. Jednym z obowiązków administratora danych osobowych, w zakresie ich przetwarzania, jest ich usuwanie, w momencie, kiedy ustanie celowość ich przetwarzania zgodnie z wytycznymi wynikającymi z odrębnych ustaw.
2. Usuwanie danych osobowych, polega na:
   a) trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie, przez osoby niepowołane, przy zastosowaniu powszechnie dostępnych metod,
   b) anonimizacji danych osobowych, zbiorów, polegającej na pozbawieniu danych osobowych, ich zbiorów, cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.
3. W zależności od nośnika, na którym przechowywane są dane osobowe, ich usuwanie polega na:
   a) dokumentacja tradycyjna (wydruki, notatki, dokumenty) – dokumentację należy zniszczyć, bądź zanonimizować w sposób uniemożliwiający odczyt, przy użyciu niszczarek spełniających odpowiednie wymagania – niszczarki paskowe lub niszczarki o podwyższonym standardzie. Dokumentacja papierowa niszczona jest również za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji),
   b) nośniki optyczne (płyty CD/DVD/BLU-RAY – analogicznie do dokumentacji tradycyjnej, należy w taki sposób zniszczyć nośnik, aby uniemożliwić odczytanie danych z płyty. W tym przypadku również zalecane jest wykorzystanie niszczarek spełniających odpowiednie wymagania,
   c) nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – obecnie istniejące sposoby niszczenia danych można podzielić na dwie główne grupy metod:
      – niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwia odczytanie danych. Istnieje specjalne oprogramowanie

dostępne na rynku służące do nadpisywania (definitywnego usuwania) danych. Wadą tej metody jest możliwość częściowego odzyskania danych za pomocą specjalistycznego oprogramowania, zaletą natomiast możliwość ponownego wykorzystania nośnika,

- niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń. Wadą tej metody jest brak możliwości ponownego wykorzystania nośnika, zaletą natomiast całkowity brak możliwości nawet częściowego odzyskania danych,

d) nośniki magnetyczne (dyskietki/dyski twarde HDD) – oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych, istnieje również możliwość demagnetyzacji nośników, jako jednego z rodzajów niszczenia sprzętowego.

4. Niezależnie od nośnika, na którym są przechowywane dane osobowe przeznaczone do zniszczenia, samo ich zniszczenie powinno odbyć się komisyjnie, a z samej operacji powinien zostać sporządzony protokół.
5. Procedura niszczenia danych osobowych:
   a) niszczenie danych osobowych ma na celu zniszczenie danych zawartych na nośniku, w celu uniemożliwienia identyfikacji osób, których dane osobowe będą niszczone,
   b) niszczenie danych osobowych następuje wyłącznie na wniosek Administratora lub upoważnionej przez niego osoby,
   c) sposób zniszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii,
   d) niszczenie danych osobowych musi odbywać się komisyjnie,
   e) zniszczenie danych osobowych musi zostać potwierdzone spisaniem protokołu,
   f) Administrator lub upoważniona przez niego osoba dokonuje kontroli prawidłowości usunięcia informacji.

II. PROCEDURA NISZCZENIA DANYCH NA NOŚNIKACH ELEKTRONICZNYCH

1. Wszystkie kopie zapasowe (backup), które znajdują się w systemach, mogą zostać trwale zniszczone po 180 dniach.
2. W odniesieniu do nośników przenośnych (pen-drive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych, stosowane są mechanizmy bezpiecznego kasowania informacji:
   a) za pomocą specjalistycznego oprogramowania,
   b) przy użyciu demagnetyzacji,
   c) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników.
3. Administrator dokonuje kontroli prawidłowości usunięcia informacji.
4. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.

5. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada Użytkownik.
6. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada właściwy administrator.
7. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia.

III. PROCEDURA NISZCZENIA DANYCH NA NOŚNIKACH PAPIEROWYCH

1. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie.
2. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji).

……

data i podpis Administratora

PROTOKÓŁ USUNIĘCIA DANYCH OSOBOWYCH

Dnia ..... Komisja powołana przez……

(imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:

1. Przewodniczący: .....
2. Członkowie: .....

.....

dokonała trwałego zniszczenia zbioru danych osobowych o nazwie ……

(Nazwa zbioru).

Zniszczenie obejmuje:

- wersję papierową zbioru. Zniszczenia dokonano poprzez ……*
- bazę danych. Zniszczenia dokonano poprzez ……*
- kopie bezpieczeństwa. Zniszczenia dokonano poprzez ……*

**Opisać sposoby zniszczenia*

Dokonanie ww. czynności zostaje potwierdzone własnoręcznymi podpisami Komisji:

.....

.....

.....

PROTOKÓŁ ZNISZCZENIA USZKODZONYCH NOŚNIKÓW KOMPUTEROWYCH

.... dnia .....r.

(akcept powołującego komisję)

Protokół nr .....

zniszczenia uszkodzonych nośników komputerowych

.....

(jednostka, komórka organizacyjna xxx)

Dnia ..... komisja powołana przez .....

(data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:
1. Przewodniczący: .....
2. Członkowie: .....
.....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....