Polityka Bezpieczeństwa

ZASADY OCHRONY DANYCH OSOBOWYCH

ŚWIERKOT Spółka z ograniczoną odpowiedzialnością
z siedzibą w Studzionce

2022-05-24

I. Spis treści

II. Podstawowe informacje

A. Podstawa prawna

Polityka Bezpieczeństwa (zwana dalej Polityką) wraz z **Instrukcją Zarządzania Systemem Informatycznym** (zwana dalej Instrukcją) opisują działania organizacyjne i techniczne podejmowane przez **Świerkot Spółką z ograniczoną odpowiedzialnością** z siedzibą w Studzionce (43-245) przy ulicy Powstańców Śląskich 113, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Katowice – Wschód w Katowicach Wydział VIII Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000469608, NIP: 6381808184 jako Administratora Danych, których celem jest osiągnięcie i utrzymanie akceptowalnego poziomu bezpieczeństwa przetwarzanych danych osobowych oraz podniesienie poziomu świadomości pracowników w zakresie ochrony tych danych/informacji.

Polityka Bezpieczeństwa stanowi jednocześnie politykę ochrony danych w rozumieniu art. 24 ust. 2 RODO.

Do wyznaczonego celu **Administrator** dąży poprzez wdrożenie odpowiedniego systemu ochrony danych osobowych przed zagrożeniami wewnętrznymi i zewnętrznymi.

Polityka Bezpieczeństwa ma status dokumentu przeznaczonego do użytku wewnętrznego i może być udostępniona osobom trzecim jedynie za zgodą Administratora.

Podstawowymi aktami prawnymi, które realizuje Polityka Bezpieczeństwa są:

1) ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000) - **dalej zwana UODO**;

2) Rozporządzenia Parlamentu Europejskiej i Rady (UE) 2016/679 (RODO)

3) Ustawa o ochronie danych osobowych z dnia 10 maja 2018 z póż. Zm

Z dniem 25 maja 2018 roku Polityka Bezpieczeństwa realizuje przepisy rozporządzenia z dnia 27 kwietnia 2016 roku Parlamentu Europejskiego i Rady 2016/679 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) - Dziennik Urzędowy UE L 119 z dnia 4 maja 2016 – **dalej zwane RODO.**

B. Definicje

a) **Administrator -** rozumie się przez to **Świerkot Spółką z ograniczoną odpowiedzialnością** z siedzibą w Studzionce (43-245) przy ulicy Powstańców Śląskich 113, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Katowice – Wschód w Katowicach Wydział VIII Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000469608, NIP: 6381808184;

b) Osoba upoważniona - każda osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora;

c) **Użytkownik systemu -** każda osoba, posiadająca upoważnienie do przetwarzania danych osobowych wydane przez Administratora zarejestrowana w systemie /posiadająca unikalny identyfikator i hasło/ przetwarzająca dane osobowe;

d) **Dane osobowe -** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio;

e) **Szczególne kategorie danych osobowych** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, a także dane osobowe dotyczące wyroków

skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa ;

f) **Zbiór danych -** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

g) Przetwarzanie danych - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

h) Usuwanie danych - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

i) Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

j) Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

k) Uwierzytelnianie - to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

l) Bezpieczeństwo informacji - zachowanie poufności, integralności, dostępności i rozliczalności informacji

m) Poufność - właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom i podmiotom;

n) Dostępność - właściwość polegającym na byciu dostępnym i użytecznym na żądanie upoważnionego podmiotu lub upoważnionej osoby;

o) **Integralność** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

p) Rozliczalność - właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

q) **Naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

r) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

s) **Zabezpieczanie danych w systemie informatycznym -** wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

C. Zdefiniowanie odpowiedzialności

Administratorem jest **Świerkot Spółką z ograniczoną odpowiedzialnością** z siedzibą w Studzionce (43-245) przy ulicy Powstańców Śląskich 113, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Katowice – Wschód w Katowicach Wydział VIII Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000469608, NIP: 6381808184.

Celem Polityki jest wskazanie działań, które należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki Administratora w zakresie zabezpieczenia danych osobowych.

Zakres przedmiotowy Polityki Bezpieczeństwa obejmuje wszystkie zbiory danych osobowych określone w **załączniku nr 3 – Wykaz zbiorów danych**.

Polityka obowiązuje wszystkich pracowników Administratora oraz osoby pracujące na rzecz Administratora na podstawie umów cywilnoprawnych oraz na podstawie prowadzonej działalności

gospodarczej.

Dane osobowe objęte Polityką Bezpieczeństwa oraz sposoby ich zabezpieczeń objęte są tajemnicą nieograniczoną w czasie.

Administrator zapewnia kontakt w sprawach ochrony danych osobowych poprzez:
http://swierkot.pl/sale-rodo

Kontakt: Paulina Świerkot - Spyra
e-mail: paulina@swierkot.pl
tel.: 600 918 939

Dane osobowe są przetwarzane na podstawie:

art. 6 ust. 1 lit. b RODO – realizacja umowy

art. 6 ust. 1 lit. c RODO – obowiązki prawne

art. 6 ust. 1 lit. f RODO – prawnie uzasadniony interes

art. 6 ust. 1 lit. a RODO – zgoda (jeśli dotyczy)

III. Polityka Bezpieczeństwa

A. Podstawowe zasady Polityki Bezpieczeństwa.

W celu zapewnienia ochrony danych osobowych przetwarzanych przez Administratora stosuje się następujące zasady:

a) ***„minimum przywilejów" - przydzielanie praw dostępu tylko w zakresie niezbędnym do wykonywania czynności służbowych,***

b) ***„separacja obowiązków" - zadania krytyczne z punktu widzenia bezpieczeństwa informacji nie mogą być realizowane przez jedną osobę,***

c) ***„domniemana odmowa" - przyjęcia, jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach.***

Realizacja Polityki Bezpieczeństwa przebiega według wymienionych poniżej zasad:

1) **Każda osoba biorąca udział w przetwarzaniu danych osobowych posiada pisemne, imienne upoważnienie do ich przetwarzania nadane przez Administratora stanowiące polecenie Administratora w rozumieniu art. 29 RODO oraz 32 ust. 4 RODO (załącznik nr 1)**. Upoważnienie to połączone jest z deklaracją pracownika o zachowaniu w tajemnicy danych osobowych, sposobów ich zabezpieczania jak również zapoznania się z treścią Polityki Bezpieczeństwa - procedura nadawania upoważnień jest opisana w punkcie VIII B.

   Wzór ewidencji osób upoważnionych stanowi **załącznik nr 2.**

2) Administrator wdrożył stosowne środki organizacyjne i techniczne mające na celu należyte zabezpieczenie danych osobowych.

3) Administrator zabezpiecza zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania poprzez stosowanie następujących zasad:

a) system informatyczny Administratora jest zabezpieczony przed nieupoważnionym dostępem, utratą, modyfikacją lub zniszczeniem danych poprzez stosowanie hasła (przechowywane w formie zaszyfrowanej przez specjalnie stosowany w tym celu algorytm kryptograficzny), szyfrowanie protokołem SSL. Sieć wewnętrzna jest zabezpieczona przed nieupoważnionym dostępem z zewnątrz.

b) każdy pracownik Administratora dysponuje indywidualnym identyfikatorem, za pośrednictwem którego może korzystać z udostępnianych zasobów i usług. Włączone w systemie informatycznym mechanizmy oraz procedury zapewniają rozliczalność użytkowników zarejestrowanych w systemie.

c) wszyscy pracownicy Administratora są uświadomieni w zakresie przyjętej Polityki.

d) pracownicy Administratora mają obowiązek informowania o wystąpieniu incydentu związanego z bezpieczeństwem informacji.

4) W przypadku naruszenia ochrony danych osobowych, zgłoszenie go organowi nadzorczemu powinno:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5) Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

6) Administrator nie przeprowadził oceny skutków przetwarzania dla ochrony danych, gdyż charakter, zakres, kontekst i cele przetwarzania danych osobowych nie wskazują na duże prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

7) Administrator raz w roku podejmuje działania mające na celu testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania w postaci audytu sprawdzającego.

8) Administrator wdrożył środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego w postaci tworzenia kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym oraz programów i narzędzi służących do przetwarzania danych osobowych. Kopie tworzone są systematycznie przynajmniej raz w tygodniu na serwerach klastrowych w centrach danych oraz dodatkowo na trwałych nośnikach w postaci dysk zewnętrzny i przechowywane w innej lokalizacji niż siedziba Administratora.

9) Administrator prowadzi rejestr czynności przetwarzania .

Czynność	**Cel**	**Podstawa**	**Kategorie danych**	**Okres**

Obsługa klientów	realizacja umowy	art. 6 ust.1 b	dane kontaktowe	5 lat

Kadry	zatrudnienie	art. 6 ust.1 c	dane pracownicze	10 lat

B. Realizacja Polityki Bezpieczeństwa.

Szczególną uwagę Administrator zwraca na elementy zarządzania, które mają istotny wpływ na bezpieczeństwo danych rozumiane jako ochrona przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Dotyczy to nie tylko danych osobowych przechowywanych w bazach danych, dokumentacji papierowej, ale również tych danych, które przesyłane są w sieciach komputerowych.

W tym ostatnim przypadku chodzi głównie o zabezpieczenie danych podczas ich elektronicznego transportu, który występuje, gdy dane są przesyłane:

1) w wiadomościach e-mail: zbiorcze dane osobowe inne niż kontaktowe lub inne mogące negatywnie wpłynąć na podmiot danych muszą być przesyłane w zabezpieczonych załącznikach oraz nie mogą stanowić treści wiadomości – przez dane kontaktowe należy rozumieć dane (imię, nazwisko, stanowisko, telefon, adres poczty elektronicznej, miejsce pracy) wykorzystywane wyłącznie w celu skontaktowania się z daną osobą,
2) z baz danych do użytkowników,

W takim przypadku cały sprzęt komputerowy jest chroniony kryptograficznie, w szczególności komputery przenośne i inne nośniki danych.

Zasady bezpieczeństwa należy traktować w sposób kompleksowy. Przy realizacji Polityki Bezpieczeństwa ważne jest zaangażowanie wszystkich osób biorących udział w przetwarzaniu danych. Szczególnie ważna jest znajomość problematyki bezpieczeństwa oraz świadomość jej znaczenia.

Wszyscy pracownicy deklarują wolę ochrony przetwarzanych danych osobowych, której celem jest zapewnienie bezpieczeństwa tych danych, a w szczególności dbanie o ich:

a) Poufność,
b) Integralność,
c) Dostępność,
d) Rozliczalność.

Naruszenie ochrony danych zgłaszane jest do organu nadzorczego **w terminie 72 godzin**, o ile istnieje ryzyko naruszenia praw lub wolności osób fizycznych.

IV. Wykaz budynków i pomieszczeń przetwarzania danych osobowych

Administrator przetwarza dane osobowe w swojej siedzibie w Studzionce przy ul. Powstańców Śląskich 113 oraz w oddziałach w Pawłowicach przy ul. Grzybowej 35, w Większycach przy ul. Raciborskiej 22, w Mykanowie przy ul. Częstochowskiej 48.

Dostęp do danych osobowych przetwarzanych w systemach informatycznych poprzez sieć telekomunikacyjną mogą mieć wybrane osoby wyłącznie za zgodą Administratora.

V. Wykaz zbiorów danych osobowych

Administrator przetwarza dane osobowe osób fizycznych w systemach informatycznych oraz w postaci papierowej. Wszystkie dane osobowe przetwarzane przez Administratora są przetwarzane zgodnie z obowiązującymi przepisami prawa.

Przeprowadzono szczegółową inwentaryzację danych osobowych przetwarzanych w formie papierowej jak i elektronicznej.

Wzór wykazu zbiorów danych osobowych oraz programów służących do ich przetwarzania wraz z ich strukturą znajduje się w **załączniku nr 3 – wykaz zbiorów danych osobowych.**

VI. Określenie środków niezbędnych do zachowania bezpieczeństwa danych

Administrator stosuje zróżnicowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

Stosowane środki organizacyjne i techniczne są wynikiem przeprowadzonego postępowania z ryzykiem obejmującego jego analizę oraz wybór sposobu postępowania.

A. Bezpieczeństwo fizyczne.

A 1.Kontrola wejścia.

Osobom odwiedzającym Administratora powinno się umożliwić dostęp wyłącznie w konkretnych, zatwierdzonych celach.

Bez specjalnego pozwolenia udzielonego przez Administratora nie wolno używać w jego siedzibie sprzętu fotograficznego, video i sprzętu nagrywającego.

A 2. Dostęp do pomieszczeń.

Dostęp do pomieszczeń Administratora, w których odbywa się przetwarzanie danych osobowych jest ograniczony jedynie do pracowników oraz innych osób upoważnionych przez Administratora. Osoby upoważnione do przebywania w obszarze przetwarzania danych osobowych mogą przebywać w nim wyłącznie w zakresie niezbędnym do wykonania czynności opisanych w upoważnieniu.

Pomieszczenia na czas nieobecności pracownika należy zamykać na klucz, a klucze po otwarciu drzwi nie pozostają w zamkach, w przypadku dostępu do pomieszczenia dla osób postronnych (współpracowników lub przedstawicieli Wykonawców) powinny one przebywać w pomieszczeniu wyłącznie w obecności upoważnionego pracownika lub za zgodą Administratora Danych. Każdorazowo wyznacza się pracownika do nadzoru personelu zewnętrznego.

A 3. Izolowane obszary przyjmowania gości.

Unika się przyjmowania gości przez pracowników Administratora w swoich biurach przy stanowiskach pracy. Może to prowadzić do przypadkowego wycieku informacji poprzez zapoznanie się z treścią otwartego dokumentu papierowego lub elektronicznego bądź przez podsłuchanie rozmowy pracowników.

A 4. Urządzenia systemu informatycznego.

Administrator nie posiada własnej serwerowni. W tym zakresie korzysta z usług podmiotów zewnętrznych w oparciu o stosowne zapisy umowne.

W działalności Administratora wykorzystywane są urządzenia przenośne: komputery przenośne, nośniki zewnętrzne, smartfony. Są one użytkowane ze szczególną ostrożnością poza obszarem przetwarzania danych, w szczególności:

a) stosowane są zabezpieczenia kryptograficzne;

b) stosowane są loginy i hasła do systemu informatycznego;

c) zabronione jest pozostawianie urządzeń bez nadzoru;

d) zabronione jest przekazywanie urządzeń do korzystania nieupoważnionym osobom;

e) zabronione jest korzystanie z sieci typu Hotspot;

f) wykonuje się kopie zapasowe danych;

g) hasła administracyjne dostępu do urządzeń aktywnych, systemów serwerowych, stacji roboczych oraz innych urządzeń wymagających logowania są przechowywane w bezpiecznym miejscu;

h) kopie zapasowe danych znajdują się w innym pomieszczeniu niż sam system przetwarzania tych informacji.

B. Ogólne środki bezpieczeństwa.

B 1. Upoważnienia do przetwarzania danych osobowych.

Każdy pracownik, przetwarzający dane osobowe musi posiadać upoważnienie do przetwarzania danych osobowych. Upoważnienie zawiera wszystkie wymagane prawem informacje oraz poziom dostępu do systemu informatycznego Administratora. Nadanie upoważnień do przetwarzania danych osobowych odbywa się na podstawie **załącznika nr 1.**

Najpóźniej w ostatnim dniu pracy anuluje się upoważnienie poprzez odnotowanie tego faktu w Ewidencji osób upoważnionych oraz dokonanie odpowiedniej adnotacji w dokumencie upoważnienia.

Upoważnienia przechowuje się w miejscu, w którym przechowywana jest dokumentacja kadrowa.

B 2. Zasada czystego biurka i czystego ekranu

Informacje pozostawione na biurkach mogą ulec zniszczeniu lub uszkodzeniu, lub też mogą zostać ujawnione poprzez wgląd osób postronnych, dlatego też wprowadzono zasady:

1) dokumenty papierowe oraz inne nośniki informacji powinny być przechowywane w zamykanych na klucz szafach i/lub w innych bezpiecznych miejscach, zwłaszcza poza godzinami pracy,
2) wszystkie dokumenty papierowe muszą być niszczone przy pomocy niszczarki,
3) dokumenty zawierające wrażliwe lub krytyczne informacje powinny być zamykane w szafkach z zamkiem, pieczątki powinny być zamykane w szufladach z zamkiem,
4) nie wolno pozostawić zalogowanych komputerów bez nadzoru,
5) monitory powinny być tak ustawione by uniemożliwić podgląd informacji na ekranie osobom postronnym,
6) poza godzinami pracy urządzenia kopiujące powinny być chronione przed użyciem przez nieuprawnione osoby,
7) informacje poufne/wrażliwe należy natychmiast po wydrukowaniu wyjąć z drukarki.

C. Powierzenie przetwarzania danych.

Administrator przekazuje dane osobowe innym podmiotom. Dochodzi wówczas do powierzenia przetwarzania danych osobowych. W takim przypadku Administrator podejmuje następujące działania:

1) uwzględnia powierzenie przetwarzania danych osobowych w **wykazie zbiorów danych – złącznik nr 3**;
2) umieszcza w umowach zapisy dotyczące powierzenia przetwarzania danych osobowych.

Zapisy umowne dotyczące powierzenia przetwarzania danych muszą zawierać zapisy o tym, że podmiot przetwarzający:

1) przetwarza dane osobowe wyłącznie w celu i zakresie określonym w umowie, a także wyłącznie na udokumentowane polecenie administratora;

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

3) w miarę potrzeb podejmuje wszelkie środki wymagane w celu zabezpieczenia danych osobowych, w szczególności pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.;

4) przekazuje powierzone dane osobowe innym podmiotom do przetwarzania tylko po uzyskaniu wyraźnej zgody administratora;

5) pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;

6) pomaga administratorowi wywiązać się z obowiązków dotyczących zgłaszania naruszeń ochrony danych osobowych oraz w zakresie oceny skutków przetwarzania dla danych osobowych;

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

8) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Administrator przetwarza dane również w związku z korzystaniem ze strony internetowej, w tym poprzez pliki cookies – szczegóły określa odrębna Polityka Cookies.

D. Postępowanie z informacją

D 1. Kontrola dostępu do informacji

Pracownicy nie mogą, bez upoważnienia Administratora, udzielać następujących informacji:

- o danych osobowych oraz innych informacji o charakterze poufnym,
- o zabezpieczeniach, w tym o zabezpieczeniach systemu informatycznego.

D 2. Formy wymiany informacji

Ochronie podlega także informacja głosowa, faksowa oraz wizualna. Dla zabezpieczenia przekazywanej informacji wprowadza się następujące wymogi:

1) zachowanie szczególnej ostrożności podczas prowadzenia rozmów telefonicznych, a w szczególności zakaz przekazywania informacji poufnych i danych osobowych drogą telefoniczną.

2) zakaz prowadzenia poufnych rozmów w miejscach publicznych (restauracje, publiczne środki transportu, itp.), szeroko dostępnych biurach, pomieszczeniach o cienkich ścianach.

3) nie pozostawianie wiadomości zawierających treści poufne na „sekretarkach automatycznych".

D 3. Bezpieczeństwo teleinformatyczne

Stosuje się oprogramowanie antywirusowe oraz inne urządzenia oraz programy kontrolujące przepływ informacji pomiędzy siecią publiczną a systemem informatycznym ADO.

VII.Postanowienia końcowe

Polityka wchodzi w życie z dniem 24 maja 2018 roku.

VIII.Wykaz zmian w dokumencie:

POLITYKA BEZPIECZEŃSTWA		
Data:	Rodzaj modyfikacji:	Osoba odpowiedzialna:
2022-05-24	Powstanie dokumentu.	