Polityka Bezpieczeństwa Danych Osobowych
w Envirotech sp. z o.o.

Envirotech sp. z o.o. z siedzibą w Poznaniu przy ul. Kochanowskiego 7 (KRS: 0000138021), zwana dalej Podmiotem, świadoma wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych, a także regulacji prawnych wynikających z wejścia w życie 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, deklaruje:

1. zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych;
2. zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Podmiocie w zakresie problematyki bezpieczeństwa tych danych;
3. zamiar traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych, jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby;
4. zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

§ 1.
Postanowienia ogólne

1. Polityka bezpieczeństwa danych osobowych (zwana dalej „Polityką"), określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Ponadto Polityka określa także sposób przepływu danych pomiędzy poszczególnymi systemami, zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub w formie tradycyjnej, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.
2. Polityka jest zintegrowanym zbiorem ogólnych zasad, procedur, praw wewnętrznych i praktycznych doświadczeń regulujących sposób zarządzania, ochrony, użytkowania i przechowywania danych osobowych gromadzonych przez Podmiot w postaci elektronicznej oraz w dokumentach w wersji papierowej.
3. Integralną częścią Polityki oraz jej uszczegółowieniem jest „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych w Podmiocie" (zwana dalej „Instrukcją"), która zawiera wytyczne dotyczące bezpiecznego przetwarzania danych osobowych przy użyciu systemów informatycznych, stanowiąca **Załącznik nr 1** do Polityki.
4. Polityka obowiązująca w Podmiocie ma charakter obligatoryjny i dotyczy wszystkich osób, które przetwarzają dane osobowe w ramach współpracy z Podmiotem, tj. pracowników, współpracowników, współdziałających na podstawie umowy cywilnoprawnej, konsultantów i innych osób mających dostęp do danych osobowych.
5. Polityka została opracowana zgodnie z wymogami określonymi prawem powszechnie obowiązującym. Polityka w szczególności realizuje normy prawne wynikające 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 mającego zastosowanie do dnia 25 maja 2018 r.

6. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

§ 2.
Definicje

1. Na użytek Polityki:
   b. administrator danych – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
   c. dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna, to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
   d. zbiór danych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
   e. przetwarzanie danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie i ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
   f. system informatyczny – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur, przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   g. identyfikator użytkownika (login) – oznacza ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych
   w systemie informatycznym;
   h. hasło – oznacza ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
   i. uwierzytelnienie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
   j. podmiot tj. Envirotech sp. z o.o.;
   k. użytkownik – rozumie się przez to osobę wyznaczoną przez Podmiot lub osobę przez niego upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych zarówno w formie tradycyjnej jak i elektronicznej;
   l. organ nadzorczy – oznacza organ publiczny odpowiedzialny za monitorowanie stosowania przepisów prawa powszechnie obowiązującego dotyczącego ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej;

m. pomieszczenia – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń, określone przez Podmiot, tworzące obszar, w którym przetwarzane są dane osobowe zarówno w formie tradycyjnej i elektronicznej;
n. dostępność – oznacza gwarancję dostępu do danych osobowych tylko przez osoby uprawnione;
o. integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
p. poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
q. rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
r. integralność systemu – rozumie się przez to nienaruszalność systemu, niemożność jakiejkolwiek manipulacji;
s. podmiot przetwarzający – rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych, na podstawie pisemnej umowy zawartej z Administratorem Danych.

§ 3.
Cele Polityki

1. Polityka została opracowana i wdrożona dla stworzenia i utrzymania wysokiego poziomu bezpieczeństwa zbioru danych osobowych w celu zapewnienia poufności danych, integralności danych i dostępności zasobów oraz zapewnienia rozliczalności podejmowanych działań.
2. Celem opracowania i wdrożenia Polityki jest:
   a. maksymalne ograniczenie ryzyka związanego z nieuprawnionym przetwarzaniem lub utratą danych osobowych;
   b. zagwarantowanie pełnej ochrony danych osobowych posiadanych przez Administratora Danych zbiorów bez względu na formę w jakiej zbiór jest przetwarzany;
   c. opracowanie zasad postępowania w sytuacjach kryzysowych;
   d. wdrożenie reguł, praw i procedur zapewniających odpowiedni poziom bezpieczeństwa zarządzania danymi osobowymi będącymi w posiadaniu Administratora Danych.
3. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników. Ponadto cele realizowane są poprzez:
   a. stałe doskonalenie oraz rozwijanie organizacyjnych i technicznych środków ochrony danych osobowych przetwarzanych zarówno w formie tradycyjnej jak i elektronicznej;
   b. podejmowanie wszelkich, dozwolonych prawem działań niezbędnych dla ochrony praw jednostki związanych z bezpieczeństwem ich danych osobowych;
   c. staranny dobór, ocenę i kwalifikację dostawców usług;
   d. stosowanie odpowiednich urządzeń i oprogramowania wykorzystywanych do przetwarzania i zabezpieczania danych osobowych.
4. Zastosowane zabezpieczenia gwarantują:
   a. poufność danych;
   b. integralność danych;
   c. rozliczalność;
   d. integralność systemu;
   e. uwierzytelnienie.

§ 4.

Zakres zastosowania Polityki

1. Polityka odnosi się do wszystkich danych osobowych przetwarzanych zarówno w sposób tradycyjny jak i w systemach informatycznych. Ochronie podlegają wszystkie dane osobowe przetwarzane przez Administratora Danych, również te, które Administrator Danych powierza do przetwarzania innym podmiotom.
2. Realizację celów określonych w § 3 Polityki, powinny zagwarantować następujące założenia:
   a. wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych;
   b. przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych;
   c. przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia;
   d. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
   e. opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;
   f. śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno – finansowych – wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5.

Zastosowane zabezpieczenia organizacyjne

1. Wdrożono niniejszą Politykę oraz Instrukcję;
2. W Podmiocie w celu szybkiego reagowania w przypadku naruszenia danych osobowych lub podejrzenia ich naruszenia wprowadzono:
   a. instrukcję postępowania w sytuacji naruszenia danych osobowych – **Załącznik nr 2** do Polityki;
   b. rejestr incydentów naruszających ochronę danych osobowych – **Załącznik nr 3** do Polityki;
   c. wzór zawiadomienia o naruszeniu danych osoby, której te dane dotyczą – **Załącznik nr 4** do Polityki;
   d. wzór zawiadomienia o naruszeniu danych organu nadzorczego – **Załącznik nr 5** do Polityki.
3. Dodatkowo Podmiot prowadzi:
   - ewidencję osób upoważnionych do przetwarzania danych osobowych – stanowiący **Załącznik nr 6** do Polityki;
   - ewidencję Podmiotów przetwarzających – stanowiący **Załącznik nr 7** do Polityki;
   - ewidencję zbiorów danych osobowych – stanowiący **Załącznik nr 8** do Polityki;
   - ewidencję sprzętu i nośników, na których znajdują się dane osobowe – stanowiący **Załącznik nr 9** do Polityki;
   - ewidencję licencjowanych programów komputerowych – stanowiący **Załącznik nr 10** do Polityk.
4. Wszystkie programy zainstalowane na stacjach roboczych pochodzą z legalnych źródeł, Podmiot posiada dokumenty potwierdzające legalność używanego w Podmiocie oprogramowania.
5. Każdy użytkownik – przed uzyskaniem dostępu do danych osobowych przetwarzanych w Podmiocie – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.

6. Podmiot nadaje upoważnienia do przetwarzania danych – wzór upoważnienia do przetwarzania danych osobowych stanowi **Załącznik nr 11** do Polityki.
7. Wszyscy użytkownicy podlegają szkoleniom, stosownie do potrzeb wynikających ze zmian systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmian wewnętrznych regulacji.
8. Za organizacje szkoleń odpowiedzialny jest Podmiot.
9. Każdy użytkownik zobowiązany jest do utrzymania właściwego poziomu bezpieczeństwa w zakresie swoich obowiązków i uprawnień.
10. Każdy użytkownik składa oświadczenie zgodnie ze wzorem określonym w **Załączniku nr 12** do Polityki, w którym potwierdza zapoznanie się z aktami prawnymi powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, Polityką oraz Instrukcją. Ponadto użytkownik zobowiązuje się do zapewnienia ochrony przetwarzanych przez niego danych osobowych. Oświadczenie to jest przechowywane przez Administratora Danych przez okres 10 lat licząc od daty zakończenia współpracy z użytkownikiem (np. od daty rozwiązania umowy o pracę).
11. Każdy użytkownik, zarówno w trakcie, jak i po ustaniu współpracy z Podmiotem ma obowiązek ochrony wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz sposobów zabezpieczenia danych.
12. Niedozwolone jest przetwarzanie danych osobowych w sposób inny niż opisany w niniejszej Polityce lub Instrukcji.
13. Użytkownicy zobowiązani są:
    a. przestrzegać procedury związane z otwieraniem i zamykaniem pomieszczeń, a także na wypadek wejścia do pomieszczeń gdzie przetwarzanie są dane osobowe przez osoby nieupoważnione do przetwarzania danych osobowych;
    b. informować Administratora Danych o wszelkich nietypowych zajściach mogących mieć wpływ na bezpieczeństwo przetwarzania danych:
    c. przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy a także po jej zakończeniu.
14. Przetwarzanie danych osobowych, bez względu na formę w jakiej są one przetwarzane, odbywa się wyłącznie w pomieszczeniach wyznaczonych przez Administratora Danych.
15. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza wyznaczonymi pomieszczeniami, o których mowa w § 5 ust. 14 Polityki, wyłącznie za zgodą Administratora Danych.
16. Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa **Załącznik nr 13** do Polityki.
17. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko osoby upoważnione.
18. W przypadku, gdy przebywanie w pomieszczeniach będących obszarami przetwarzania danych osobowych przez osoby nieupoważnianie do przetwarzania danych osobowych jest konieczne, wszelkie fizyczne dokumenty zawierające dane osobowe winny być zabezpieczone w zamkniętych na klucz szafach lub szufladach lub kasetach, a osoba taka nie może pozostawać sama w pomieszczeniu bez obecności osoby uprawnionej do przetwarzania danych osobowych.
19. Każdy użytkownik, który przetwarza dane osobowe w formie dokumentów fizycznych zobowiązany jest do zabezpieczenia ich przed osobami niemającymi upoważnienia do przetwarzania danych osobowych, w szczególności poprzez odpowiednie ich przechowywanie oraz należytą procedurę niszczenia;

20. Monitory użytkowników powinny zostać ustawione w taki sposób, że osoby postronne (nieuprawnione do przetwarzania danych osobowych) nie miały wglądu w treść wyświetlaną na ekranie;
21. Na stacjach roboczych, na których przetwarzane są dane osobowe zainstalowano automatyczne wygaszacze ekranu blokujące po 10 minutach bezczynności dostęp do stacji roboczej;
22. Niepotrzebne w danym momencie dokumenty w formie fizycznej i nośniki elektroniczne, należy bezwzględnie chować w zamykanych szafach. Pod żadnym pozorem dokumenty i nośniki nie powinny pozostać niezabezpieczone po zakończeniu pracy. Wszystkie niepotrzebne dokumenty niszczone są przy pomocy niszczarki do papieru. Niedopuszczalne jest pozostawienie wydruków zawierających dane osobowe w miejscach ogólnodostępnych – zasada „czystego biurka";
23. W razie naprawy sprzętu komputerowego zawierającego dane osobowe, dane te są wcześniej usuwane. W przypadku braku możliwości usunięcia danych – naprawa odbywa się pod nadzorem Administratora Danych lub osoby upoważnionej przez Administratora Danych;
24. Administrator Danych przewiduje możliwość powierzenia przetwarzania danych osobowych innemu podmiotowi. Administrator Danych zawiera, z każdym podmiotem, któremu zostanie powierzone przetwarzanie danych osobowych, umowę o powierzeniu przetwarzania danych osobowych, w której określony zostanie zakres przetwarzania, cel ich przetwarzania oraz wymagane zabezpieczenia danych osobowych gwarantowane przez te podmioty.

§ 6.
Zastosowane zabezpieczenia techniczne

1. Przetwarzanie danych osobowych w Podmiocie odbywa się w ssiedzibie Podmiotu pod adresem: Poznań, ul. Kochanowskiego 7 (budynek z ochroną fizyczną, pomieszczenia zabezpieczone systemem alarmowych, zamykane na klucz, archiwum wyodrębnione, zamykane do którego dostęp posiada ograniczona liczba osób posiadających upoważnienie).
2. Do pomieszczeń w ssiedzibie Podmiotu określonej w ust. 1. powyżej dostęp mają wyłącznie osoby upoważnione do przetwarzania danych.
3. Siedziba Podmiotu określona w ust. 1. powyżej objęta jest całodobowym monitoringiem oraz ochroną fizyczną pracowników ochrony.
4. Pomieszczenia w siedzibie Podmiotu określonej w ust. 1. powyżej. wyposażone są w szafy zamykane na klucz do przechowywania danych w formie tradycyjnej.
5. Pomieszczenia, w których przetwarzane są dane są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolnostojącej gaśnicy.
6. Dokumenty fizyczne zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów lub poddane profesjonalnemu niszczeniu wyspecjalizowanej firmie zewnętrznej.
7. Zastosowano urządzenia typu UPS i wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
8. Dostęp do systemu operacyjnego komputera lub innego sprzętu, na którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
9. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
10. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
11. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu

służącego do przetwarzania danych.

§ 7.
Podmiot

1. Podmiot przetwarza dane osobowe z poszanowaniem następujących zasad:
   a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   b. rzetelnie i uczciwie (rzetelność);
   c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
   d. w konkretnych celach i nie „na zapas" (minimalizacja);
   e. nie więcej niż potrzeba (adekwatność);
   f. z dbałością o prawidłowość danych (prawidłowość);
   g. nie dłużej niż potrzeba (czasowość);
   h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).
2. Do najważniejszych obowiązków Podmiotu należy:
   a. zapewnienie środków organizacyjnych i technicznych zapewniających zabezpieczenie danych osobowych przed dostępem osób nieupoważnionych;
   b. zapewnienie przetwarzania danych zgodnie 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, ustawą o ochronie danych osobowych, uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi Podmiotu;
   c. informowanie organów uprawnionych do ścigania przestępstw w przypadku celowego naruszenia bezpieczeństwa przetwarzanych danych osobowych;
   d. zapewnienie właściwej konfiguracji systemu informatycznego zapewniającej bezpieczeństwo i ograniczenie dostępu do danych osobowych osób nieupoważnionych;
   e. przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych;
   f. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
   g. nadzór nad bezpieczeństwem danych osobowych;
   h. kontrola upoważnionych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
   i. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
3. Podmiot będzie również upoważniony i odpowiedzialny za prawidłowe funkcjonowanie sprzętu komputerowego, oprogramowania i jego konserwację.
4. Wykonanie obowiązków określonych w § 7. ust. 2. Administrator danych może przekazać powołanemu Inspektorowi Ochrony Danych.

§ 8.
Inspektor Ochrony Danych

1. Podmiot kierując się kryterium posiadania odpowiednich kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, wyznacza w Podmiocie Inspektora Ochrony Danych, do zadań którego należało będzie:
   a. informowanie Podmiotu (Administratora Danych, podmiotu przetwarzającego) oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów powszechnie obowiązujących dotyczących ochrony danych osobowych i doradzanie im w tej sprawie;
   b. monitorowanie przestrzegania prawa powszechnie obowiązującego dotyczącego ochrony danych osobowych, Polityki i Instrukcji, w tym podział obowiązków, działania

zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c. współpraca z organem nadzorczym;
d. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

§ 9.
Administrator systemu informatycznego

1. Podmiot zgodnie z § 7. ust. 2. Polityki jest upoważniony i odpowiedzialny za prawidłowe funkcjonowanie sprzętu komputerowego, oprogramowania i jego konserwację. Tym samym pełni on funkcję Administratora systemu informatycznego, chyba że wyznaczy do tego inną upoważnioną osobę lub Inspektora Ochrony Danych.
2. Administrator systemu informatycznego odpowiedzialny jest za:
   a. nadawanie, zmianę i blokowanie uprawnień użytkowników do systemu informatycznego;
   b. właściwą konfigurację systemu informatycznego zapewniającą bezpieczeństwo i graniczenie dostępu do danych osobowych osób nieupoważnionych;
   c. monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych;
   d. nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, które zawierają dane osobowe;
   e. okresowe wykonywanie kopii bezpieczeństwa danych oraz nadzór nad ich zabezpieczeniem;
   f. podejmowanie działań w przypadku wykrycia naruszenia zabezpieczeń w systemie informatycznym lub podejrzenia takiego naruszenia (np. pojawienie się wirusa w systemie). Administrator, w takich sytuacjach, w szczególności zobowiązany jest do:
      - fizycznego odłączenia urządzeń, które umożliwiają nieautoryzowany dostęp do zbioru danych osobowych,
      - wylogowania użytkownika, który zgłosił podejrzenie lub naruszenie integralności zbioru danych osobowych,
      - podjęcie działań uniemożliwiających dalsze nielegalne przetwarzanie danych osobowych,
      - usunięcia skutków incydentu,
      - przywrócenie normalnego działania systemu (np. odtworzenie bazy danych z ostatniej kopii),
      - zmiany hasła użytkownika, który zgłosił naruszenie systemu informatycznego,
      - poinformowania o incydencie Administratora Danych, w tym sporządzenia notatki dotyczącej opisu, przyczyn i znanych skutków incydentu,
      - wyjaśnienia przyczyn wystąpienia incydentu i podjęcia działań zmierzających do ograniczenia ryzyka wystąpienia ponownego incydentu w przyszłości,
      - wydania zgody na ponowne rozpoczęcie przetwarzania danych osobowych,
      - przedstawienia Administratorowi Danych propozycji poprawy bezpieczeństwa przetwarzania danych osobowych,
      - w razie, gdy incydent wywołany był świadomie przez użytkownika – zabezpieczenia niezbędnych dowodów;
   g. okresowa analiza przyczyn i skutków sytuacji, które naruszały bezpieczeństwo danych oraz informowanie Administratora Danych o wynikach analizy;
   h. zabezpieczenie komputerów przenośnych poprzez:
      - ustawienie automatycznego wymuszenia zmiany hasła co 40 dni,

- ustawienie wymogu dotyczącego haseł zgodnie z wytycznymi Ustawy (odpowiednia ilość i rodzaj znaków),
- instalację oprogramowania antywirusowego,
- stosowanie środków ochrony kryptograficznej wobec przetwarzanych danych osobowych na komputerach przenośnych,

i. ograniczenie możliwości instalowania oprogramowania na stacjach roboczych przez osoby nieupoważnione.

§ 10.

Inwentaryzacja

1. Podmiot identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Podmiot postępuje zgodnie z przyjętymi zasadami w tym zakresie.
2. Podmiot identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
3. Podmiot identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W razie zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Podmiot postępuje zgodnie z przyjętymi zasadami w tym zakresie.
4. Podmiot identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

§11.

Rejestr czynności przetwarzania danych

1. Rejestr czynności przetwarzania danych stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2. Podmiot prowadzi Rejestr Czynności Przetwarzania Danych jako Administrator Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe, który stanowi **Załącznik nr 14** do Polityki.
3. Podmiot prowadzi Rejestr Czynności Przetwarzania Danych jako Podmiot Przetwarzający, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe, który stanowi **Załącznik nr 15** do Polityki.
4. Rejestry są jednym z podstawowych narzędzi umożliwiających Podmiotowi rozliczanie większości obowiązków ochrony danych.
5. W Rejestrach dla każdej czynności przetwarzania danych, którą Podmiot uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej:
   a. nazwę czynności,
   b. cel przetwarzania,
   c. opis kategorii osób,
   d. opis kategorii danych,
   e. podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Podmiotu, jeśli podstawą jest uzasadniony interes,
   f. sposób zbierania danych,
   g. opis kategorii odbiorców danych (w tym przetwarzających),
   h. informację o przekazaniu poza EU/EOG;
   i. ogólny opis technicznych i organizacyjnych środków ochrony danych.

§ 12

Podstawy przetwarzania

1. Podmiot dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel), Podmiot dookreśla podstawę i cel w precyzyjny i czytelny sposób, gdy jest to potrzebne.
3. Podmiot wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu.

§ 13.

Sposób obsługi praw jednostki i obowiązków informacyjnych Podmiotu jako Administratora Danych

1. Podmiot dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. Podmiot ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym m.in.: zamieszczenie na stronie internetowej Podmiotu informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.
3. Podmiot dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
4. Podmiot wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
5. W celu realizacji praw jednostki Podmiot zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Podmiot, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
6. Podmiot dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.
7. Podmiot określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
8. Podmiot informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
9. Podmiot informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
10. Podmiot informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
11. Podmiot określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
12. Podmiot informuje osobę o planowanej zmianie celu przetwarzania danych.
13. Podmiot informuje osobę przed uchyleniem ograniczenia przetwarzania.
14. Podmiot informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
15. Podmiot informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
16. Podmiot bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

§14.

Żądania osób

1. Realizując prawa osób, których dane dotyczą, Podmiot jako Administrator danych

wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Podmiot może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

2. Podmiot informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. Podmiot informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. Na żądanie osoby dotyczące dostępu do jej danych Podmiot informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15. RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Podmiot nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
5. Na żądanie Podmiot wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Podmiot wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.
6. Podmiot dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Podmiot ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.
7. Podmiot uzupełnia i aktualizuje dane na żądanie osoby. Podmiot ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Podmiot nie musi przetwarzać danych, które są zbędne). Podmiot może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. Na żądanie osoby Podmiot usuwa dane, gdy:
   a. dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
   b. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
   c. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   d. dane były przetwarzane niezgodnie z prawem,
   e. konieczność usunięcia wynika z obowiązku prawnego,
   f. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).
9. Podmiot określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.
10. Jeżeli dane podlegające usunięciu zostały upublicznione Podmiot podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.

11. W przypadku usunięcia danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.
12. Podmiot prowadzi Rejestr żądań osób, których dane Podmiot przetwarza – wzór Rejestru stanowi **Załącznik nr 16** do Polityki.

§15.

Ograniczenie przetwarzania

1. Podmiot dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
   a. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
   b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   c. nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   d. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją, do czasu stwierdzenia, czy po stronie Podmiotu zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
2. W trakcie ograniczenia przetwarzania Podmiot przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
3. W przypadku ograniczenia przetwarzania danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.

§ 16.

Przenoszenie danych

Na żądanie osoby Podmiot wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Podmiotowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Podmiotu.

§ 17.

Sprzeciw w szczególnej sytuacji

1. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Podmiot w oparciu o uzasadniony interes lub o powierzone zadanie w interesie publicznym, Podmiot uwzględni sprzeciw, o ile nie zachodzą po stronie Podmiotu ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
2. Jeżeli Podmiot prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Podmiot uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym – sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych.
3. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Podmiot na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Podmiot uwzględni sprzeciw i zaprzestanie takiego przetwarzania – sprzeciw względem marketingu bezpośredniego.

§18.

Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu

1. Jeżeli Podmiot przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę**,** Administrator zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Podmiotu, chyba że taka automatyczna decyzja:
   a. jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Podmiotu,
   b. jest wprost dozwolona przepisami prawa,
   c. opiera się na wyraźnej zgodzie odwołującej osoby.

§19.
Minimalizacja

1. Podmiot dba o minimalizację przetwarzania danych pod kątem:
   a. adekwatności danych do celów (ilości danych i zakresu przetwarzania) – Podmiot zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Podmiot dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. Podmiot przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).
   b. dostępu do danych – Podmiot stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Podmiot stosuje kontrolę dostępu fizycznego. Podmiot dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających. Podmiot dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Podmiot.
   c. czasu przechowywania danych – Podmiot wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów produkcyjnych Podmiot, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Podmiot. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§20.
Bezpieczeństwo

1. Podmiot zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Podmiot.
2. Podmiot przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a. zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
   b. kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

c. przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.
d. analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
e. ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście, jak:
   - pseudonimizacja,
   - szyfrowanie danych osobowych,
   - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   - środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

3. Podmiot dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
4. Podmiot stosuje metodykę oceny skutków przyjętą w przedsiębiorstwie.
5. Podmiot stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
6. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w przedsiębiorstwie i są bliżej opisane w procedurach przyjętych przez Podmiot dla tych obszarów.
7. Podmiot stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

§21.

Powierzenie danych przez podmiot jako Administratora danych

1. Zgromadzone u Administratora danych dane osobowe przekazywane są uprawnionym podmiotom na mocy obowiązujących przepisów prawa. Administrator sprawuje nadzór nad tym jakie dane i w jakim zakresie, a także komu zostały udostępnione.
2. Administrator przekazuje dane podmiotom przetwarzającym, które dają wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Podmiocie.
3. Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych osobowych stanowiące **Załącznik nr 17** do Polityki – „Umowa powierzenia przetwarzania danych”.
4. Administrator rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Umowy powierzenia przetwarzania danych.

§22.

Powierzenie danych podmiotowi jako Podmiotowi przetwarzającemu

1. Podmiot, jako podmiot przetwarzający, dokonuje w imieniu Administrator danych przetwarzania danych, zapewniając wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi istniejące tj. 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 i chroniło prawa osób, których dane dotyczą.

2. Podmiot, jako podmiot przetwarzający może korzystać z usług innego podmiotu przetwarzającego po udzieleniu mu przez Administratora pisemnej zgody. Podmiot przekazuje dane Podprzetwarzającemuu, który daje wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Podmiocie. Podmiot nie ponosi odpowiedzialności za uchybienia Podprzetwarzającego.
3. Podmiot przechowuje dane udostępnione przez Administratora danych do momentu przedawnienia roszczeń wynikających z umowy powierzenia. Następnie dane zostają przez Podmiot mechanicznie usunięte lub zwrócone Administratorowi danych.

§23.

Eksport danych

1. Podmiot rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Liechtenstein i Norwegia).
2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Podmiot okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

§24.

Projektowanie prywatności

1. Podmiot zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
2. W tym celu zasady prowadzenia projektów i inwestycji przez Podmiot odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

§25.

Analiza ryzyka i ocena skutków

1. W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem Podmiot szacuje ryzyko właściwe dla przetwarzania danych.
2. Podmiot wdrożył Procedurę określającą zasady szacowania ryzyka – **Załącznik nr 18** do Polityki, oraz wzór analizy ryzyka – **Załącznik nr 19** do Polityki.
3. W razie, gdy operacje przetwarzania wiążą się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać Podmiot do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka.
4. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.
5. Podmiot, jako Podmiot przetwarzający, jest obowiązany dokonać oceny skutków dla ochrony danych, które przetwarza w imieniu Administratora danych.

§26.

Postanowienia końcowe

1. Polityka jest dokumentem wewnętrznym w Podmiocie i nie może być udostępniania osobom nieupoważnionym w jakiejkolwiek formie.
2. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy prawa powszechnie obowiązującego.
3. Wszelkie załączniki do niniejszej Polityki stanowią jej integralną część.
4. Osoby upoważnione zobowiązane są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.