

1. Cel i zakres Polityki

Niniejsza Polityka ma na celu ustanowienie ogólnych zasad postępowania z danymi osobowymi przetwarzanymi przez Bioset Sp. z o.o. Wojnowo 7, 86-014 Wojnowo, NIP: 5542941256, zwaną dalej „Administratorem” lub „Spółką”, w zgodzie z wymogami wynikającymi z przepisów rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016r. 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 osobowych osób fizycznych), zwanego dalej „RODO” lub „Rozporządzeniem”.

Niniejsza Polityka ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w inny sposób niż zautomatyzowany danych osobowych przetwarzanych przez Spółkę.

Zapisy w niniejszej Polityce znajdują zastosowanie do wszystkich operacji przetwarzania danych osobowych prowadzonych przez Spółkę niezależnie od tego, czy występuje ono jako administrator danych, czy podmiot przetwarzający.

Niniejsza Polityka bezpieczeństwa danych nie stanowi zbioru wszystkich przepisów Rozporządzenia mogących mieć zastosowanie w Spółce natomiast jest praktycznym przewodnikiem po najważniejszych obowiązkach wynikających z ww. aktu.

2. Definicje

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 tj.: 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.

Szczególne kategorie danych – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania, danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, tj.: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikację, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnienie, dopasowanie lub łączenie, ograniczanie lub niszczenie.

Administrator Danych Osobowych (ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych

Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Naruszenie ochrony danych – przez to pojęcie należy rozumieć „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” (art. 4 pkt 12 RODO).

Ograniczenie przetwarzania – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

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.

Odbiorca – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie do celów przetwarzania.

Strona trzecia – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

Zgoda osoby, której dane dotyczą - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Dane genetyczne – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalną informację o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej od tej osoby fizycznej.

Dane dotyczące zdrowia – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

Dane biometryczne – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

3. Przesłanki do przetwarzania danych osobowych przez Bio-Set Sp. z o.o.

Spółka jako Administrator posiada co najmniej jedną z podstaw przetwarzania danych osobowych, o których mowa w art. 6 lub 9 Rozporządzenia:

- a) Przetwarzanie na podstawie art. 6 ust. 1 lit. A – zgoda osoby, której dane dotyczą ma zastosowanie podczas przetwarzania wizerunku osób fizycznych oraz w przypadku przesyłania zamówionych informacji o treści handlowej.
- b) Przetwarzanie na podstawie art. 6 ust. 1 lit. B RODO – 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. Przesłanka

ta ma zastosowanie do przetwarzania danych osobowych kandydatów do pracy, pracowników i kontrahentów.

- c) Przetwarzanie na podstawie art. 6 ust 1 lit. C RODO – przetwarzanie jest niezbędne do wykonania obowiązku prawnego ciążącego na administratorze
- d) Przetwarzanie na podstawie art. 9 ust. 2 lit. H – przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny 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 warunków i zabezpieczeń. Ta przesłanka ma zastosowanie do przetwarzania orzeczeń lekarskich pracowników.

- 4. Przetwarzanie danych osobowych przez Bio-Set Sp. z o.o. jako podmiot przetwarzający

W przypadku przetwarzania danych osobowych w charakterze podmiotu przetwarzającego Spółka posiada umowę powierzenia przetwarzania danych osobowych z administratorem danych, który zleca operację przetwarzania, zawierającą wszystkie elementy wymienione w art. 28 RODO oraz ściśle się do niej stosuje.

- 5. Zasady jakimi kieruje się Spółka w trakcie przetwarzania danych osobowych

Zasada legalności – oznacza spełnienie wszystkich wymogów prawa, w tym w szczególności posiadanie jednej z przesłanek przetwarzania, o których mowa w rozporządzeniu art. 6 ust. 1;

Zasada rzetelności – oznacza przejrzystość i zgodność z prawem na każdym na każdym etapie przetwarzania;

Zasada ograniczonego celu – oznacza, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawem uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami;

Zasada ograniczonego czasu przechowywania (retencji danych) – nakazuje aby dane osobowe były przetwarzane jedynie tak długo jak jest to niezbędne dla osiągnięcia celu;

Zasada prawidłowości – zgodnie z którą dane osobowe muszą być prawidłowe tj.. odpowiadać stanowi faktycznemu oraz w miarę potrzeb aktualizowane;

Zasada przejrzystości – charakter operacji przetwarzania wykonywanych przez Podmiot musi być jasny dla osób, których dane dotyczą;

Zasada poufności oraz integralności – tj.. zapewnienie aby dane nie zostały ujawnione stronie trzeciej;

Zasada rozliczalności – ma na celu przypisanie wszystkich działań dokonywanych na danych osobowych konkretnym osobom. Zgodnie z tą zasadą Administrator musi być w stanie wykazać spełnienie przez siebie wymogów wynikających z przepisów dotyczących ochrony danych osobowych;

- 6. Środki techniczne i organizacyjne zastosowane przez Administratora w celu ochrony danych osobowych.

- Każda osoba zatrudniona, posiadająca dostęp do danych osobowych posiada pisemne upoważnienie do przetwarzania, w którym wskazano których operacji przetwarzania ono dotyczy. Wraz z upoważnieniem pracownicy podpisują zobowiązanie do

zachowania w poufności wszelkich danych osobowych w trakcie zatrudnienia jak i po jego zakończeniu

- Prowadzony jest rejestr czynności przetwarzania danych osobowych który obejmuje informacje wskazane w pkt. 30 ust. 5 rozporządzenia.
- Administrator nie przekazuje danych osobowych, osób fizycznych będących pacjentami, pracownikami i kontrahentami do państwa trzeciego tj. nienależącego do Europejskiego Obszaru Gospodarczego i organizacjom międzynarodowym.

7. Obowiązki pracowników w związku z ochroną danych osobowych

- Każdy pracownik ma obowiązek zapoznać się z niniejszą Polityką Ochrony Danych oraz przestrzegać jej zapisów.
- Każdy pracownik ma obowiązek uczestniczenia w szkoleniach organizowanych przez Administratora z zakresu ochrony danych osobowych.
- Każdy pracownik posiadający pisemne upoważnienie do przetwarzania danych osobowych zobowiązany jest przestrzegać zachowania w poufności informacji i danych, do których ma dostęp zarówno w trakcie trwania współpracy jak i po jej ustaniu.
- W przypadku gdy pracownik wykorzystuje do przetwarzania danych osobowych sprzęt komputerowy i narzędzia dostarczone przez Administratora, posiada on indywidualny login i hasło. Pracownik nie podaje swoich haseł innym osobom.
- Niedopuszczalne jest wykorzystywanie prywatnych urządzeń pracowników do przetwarzania danych osobowych, których Administratorem jest Spółka, chyba że na podstawie odrębnie przyjętych zasad regulujących postępowanie z danymi osobowymi w takiej sytuacji.
- W przypadku przetwarzania danych osobowych w formie papierowej pracownik przechowuje je w formie uniemożliwiającej do nich dostęp osobom nieupoważnionym, w szczególności zamyka je na klucz w przypadku gdy opuszcza swoje stanowisko pracy.