Polityka bezpieczeństwa przetwarzania danych osobowych w INWEBIT Sp. z o.o.

Rozdział 1
Postanowienia ogólne

§ 1
Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w Inwebit Sp. z o.o., zwanej dalej „Organizacją", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2
Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:
Rozporządzeniu 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 /Dz. Urz. UE.L nr 119, str.1/, dalej „RODO".

§ 3
Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4
Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Organizacji rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

- poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
- integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

- dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
- zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

Administratorem danych osobowych przetwarzanych w Organizacji jest Inwebit Sp. z o.o. z siedzibą w Poznaniu (61-888), przy ulicy Składowej 5B, nr KRS 0000587097, REGON: 363125111, NIP: 783-17-34-168.

Rozdział 2
Definicje

§ 6

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:
administrator danych osobowych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
RODO – 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 /Dz. Urz. UE.L nr 119, str. 1/,
dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
przetwarzane danych – operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,
system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
system tradycyjny – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

administrator systemu informatycznego – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 7
W Organizacji przetwarzane są dane osobowe pracowników, kandydatów do pracy, kontrahentów zebrane w zbiorach danych osobowych.
Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
Innymi dokumentami regulującymi ochronę danych osobowych w Organizacji są:
1) ewidencja osób upoważnionych do przetwarzania danych osobowych,
2) rejestr czynności przetwarzania danych osobowych,
3) procedura postępowania w przypadku naruszenia ochrony danych osobowych,

§ 8
Politykę bezpieczeństwa stosuje się w szczególności do:

- danych osobowych przetwarzanych w narzędziach developerskich, takich jak Jira wraz z dodatkami, Gitlab, Mantis, VPN czy narzędziach służących do organizacji pracy, takich jak Microsoft Office, oraz serwerze pocztowym jak i na stronie www.
- wszystkich informacji dotyczących danych pracowników, kontrahentów, odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia
- informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
- rejestru osób trzecich mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
- innych dokumentów zawierających dane osobowe.

§ 9

Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
- wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
- wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych osobowych

§ 10

Dane osobowe gromadzone są w:
Ewidencja osób upoważnionych do przetwarzania danych osobowych,
Akta osobowe pracowników,
Ewidencja czasu pracy, wejść/wyjść,
Rejestr delegacji służbowych,
Listy płac pracowników,
Deklaracje ubezpieczeniowe pracowników,
Deklaracje i kartoteki ZUS pracowników,
Deklaracje podatkowe pracowników,
Rejestr wypadków,
Umowy cywilno-prawne,
Umowy zawierane z kontrahentami,
Dokumenty archiwalne.

§ 11

Zbiory danych osobowych wymienione w § 10 podlegają przetwarzaniu w sposób tradycyjny, jak i w systemie informatycznym biura rachunkowego.

Rozdział 5
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 12

Zabezpieczenia organizacyjne

- opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
- stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
- opracowano i bieżąco prowadzi się rejestr czynności
- do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
- osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
- przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
- przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
- dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

Zabezpieczenia techniczne

- wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą dedykowanych urządzeń sieciowych (możliwość dostępu jest tylko poprzez VPN),
- komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne zmiany hasła,

Środki ochrony fizycznej:

- obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
- urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
- dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.