Polityka bezpieczeństwa przetwarzania danych osobowych w PROTEKTOR-POLSKA Sp. z o.o.

I. Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych w firmie PROTEKTOR-POLSKA Sp. z o. o. (zwanej dalej **POLITYKĄ BEZPIECZEŃSTWA**) 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 m.in. w:
a) 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/**,
b) Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (**Dz. U. z 2018 r., poz. 1000**).

§ 3

Ochrona danych osobowych realizowana jest przez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników, proporcjonalnie i adekwatnie do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w firmie PROTEKTOR-POLSKA Sp. z o. o. rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
a) poufność danych – dane nie są udostępniane osobom nieupoważnionym,
b) integralność danych – danych osobowych nie zmienia się ani nie niszczy w sposób nieautoryzowany,
c) rozliczalność danych – działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
d) integralność systemu – nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,
e) dostępność informacji – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów, gdy jest to potrzebne,
f) zarządzanie ryzykiem – 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 PROTEKTOR-POLSKA Sp. z o. o. jest Sebastian Piórkowski.

II. Definicje

§ 6

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:
a) 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,
b) ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000),
c) 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/**,
d) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
e) zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
f) 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.
g) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
h) system tradycyjny – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
i) zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
j) administrator systemu informatycznego – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
k) odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o **umowę powierzenia**,
l) 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,
m) identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
n) hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

III. Zakres stosowania

§ 7

1. W firmie PROTEKTOR-POLSKA Sp. z o. o. zebrane w zbiorach danych osobowych i przetwarzane są dane osobowe:
a) pracowników,
b) kandydatów do pracy,
c) klientów,
d) kontrahentów.
Powyższe informacje są przetwarzane w postaci dokumentacji tradycyjnej, jak i elektronicznej.

2. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

3. Firma PROTEKTOR-POLSKA Sp. z o. o. prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, również rejestr czynności przetwarzania danych osobowych i procedur postępowania w przypadku naruszenia danych osobowych.

§ 8

Politykę Bezpieczeństwa stosuje się w szczególności do:
a) danych osobowych przetwarzanych w systemie: Faktura iBiznes, Open Office, Symfonia, Płatnik,
b) wszystkich informacji dotyczących danych pracowników, kandydatów do pracy, klientów i kontrahentów,
c) odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o **umowy powierzenia**, np. biuro rachunkowe, kancelaria prawna, informatyk,
d) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
e) rejestru osób trzecich, np. pracowników, firm zewnętrznych, biur rachunkowych, mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
f) innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez Politykę Bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:
a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
b) wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
c) wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

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

IV. Wykaz zbiorów danych osobowych

§ 10

Dane osobowe gromadzone są w zbiorach:
1. Ewidencja osób upoważnionych do przetwarzania danych osobowych,
2. Akta osobowe pracowników,
3. Ewidencja zwolnień lekarskich,
4. Skierowania na badania okresowe, specjalistyczne,
5. Ewidencja urlopów, czasu pracy, wyjść,
6. Rejestr delegacji służbowych,
7. Listy płac pracowników,
8. Deklaracje ubezpieczeniowe pracowników,
9. Deklaracje i kartoteki ZUS pracowników,
10. Deklaracje podatkowe pracowników,
11. Rejestr wypadków,
l2. Umowy cywilnoprawne,
13. Umowy zawierane z kontrahentami,
14. Rejestr klientów,
15. Dokumenty archiwalne.
Wymienione zbiory danych osobowych podlegają przetwarzaniu w sposób tradycyjny oraz przy użyciu systemu informatycznego.

V. Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

§ 11

Dane osobowe przetwarzane są w budynkach mieszczących się w Bydgoszczy 85-079 ul.Kościuszki 27/ 610, w Żninie 88-400 ul.Dworcowa 45 oraz w Wągrowcu 62-100 ul.Gnieźnieńska 45.

VI. Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 12

1. Zabezpieczenia organizacyjne:
a) opracowano i wdrożono **politykę bezpieczeństwa przetwarzania danych osobowych**,
b) sporządzono i wdrożono **instrukcję zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych w Organizacji – stanowiącą załącznik numer 1,
c) stworzono **procedurę postępowania w sytuacji naruszenia ochrony danych osobowych** – stanowiącą załącznik numer 2,
d) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych osobowych bądź osobę przez niego upoważnioną,
e) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz przepisami w zakresie zabezpieczeń systemu informatycznego,
f) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
g) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
h) 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,

i) 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.

2. Zabezpieczenia techniczne:
a) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
b) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,

3. Środki ochrony fizycznej:
a) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
b) obszar, na którym przetwarzane są dane osobowe objęty jest całodobową fizyczną ochroną budynku,
c) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
d) dokumenty zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

VII. Zadania administratora danych osobowych

§ 14

1. Do najważniejszych obowiązków administratora danych osobowych należy:
a) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami **RODO** i **ustawy o ochronie danych osobowych**,
b) zapewnienie przetwarzania danych zgodnie z **uregulowaniami polityki bezpieczeństwa** i innymi dokumentami wewnętrznymi,
c) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
d) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
e) nadzór nad bezpieczeństwem danych osobowych,
f) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

2. Administrator danych osobowych odpowiedzialny jest za:
a) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
b) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
c) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
d) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
e) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
f) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
g) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
h) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
i) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
j) przyznawanie ściśle określonych praw dostępu do informacji w danym systemie,
k) wprowadzanie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
l) zarządzanie licencjami, procedurami ich dotyczącymi,
m) prowadzenie profilaktyki antywirusowej.

VIII. Powierzenie przetwarzania danych osobowych

§ 15

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w **art. 28 RODO**.

2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach osoby której powierzono przetwarzanie danych dotyczące zabezpieczenia danych osobowych.

IX. Postanowienia końcowe

§ 16

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

2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych.

3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,

4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.