POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH FIRMY ERBIS KRAJEWSKI-WIECZOREK SP. J.

Spis treści:

I PODZIAŁ OBOWIĄZKÓW

§ 1

1. Osoba prowadząca działalność gospodarczą, działając jako administrator danych osobowych (dalej jako „ADO") jest odpowiedzialna za realizację obowiązków wskazanych w niniejszej Polityce bezpieczeństwa danych.
2. Administratorem danych osobowych jest:

Firma Erbis Krajewski – Wieczorek sp. j.
ul. Jastrzębia 22
53-148 Wrocław

Tel/fax: +48 71 361 00 78
e-mail: biuro@erbis.pl

§ 2

ADO nadaje dostęp do przetwarzanych danych osobowych wyłącznie tym osobom, które zostały skutecznie zapoznane z wyciągiem z podstawowych zasad bezpieczeństwa danych osobowych (**załącznik nr 9**), zobowiązały się do jego przestrzegania w drodze odpowiednio złożonego oświadczenia oraz otrzymały upoważnienie (**wzór: załącznik nr 8**) ściśle precyzujące zakres czynności, które związane są z dostępem do danych osobowych.

§ 3

ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, wedle wzoru stanowiącego **załącznik nr 10**.

CZEŚĆ DRUGA – INWENTARYZACJA ZASOBÓW INFORMACYJNYCH

§ 1

ADO wykonuje i prowadzi na bieżąco inwentaryzację przetwarzanych informacji mogących stanowić dane osobowe.

§ 2

Inwentaryzacja zasobów informacyjnych polega ustaleniu w stopniu wyczerpującym i kompletnym:

a) jakie kategorie informacji są przetwarzane;
b) w jaki sposób;
c) w jakim celu;
d) na jakiej podstawie prawnej;
e) w jakim miejscu;
f) przez jaki okres czasu;
g) kto może mieć do nich dostęp.

§ 3

ADO może zawierać umowy powierzenia przetwarzania danych osobowych **(wzór: załącznik nr 11**). ADO prowadzi ewidencję wszystkich zawartych umów powierzenia przetwarzania na podstawie wzoru stanowiącego **załącznik nr 12.**

§ 4

Po uwzględnieniu wyboru zabezpieczeń dokonanego w ramach szacowania ryzyka, uzupełniany jest rejestr czynności przetwarzania, którego wzór stanowi **załącznik nr 2.**

§ 5

ADO sporządza wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych według wzoru stanowiącego **załącznik nr 3.**

CZEŚĆ TRZECIA – INWENTARYZACJA ZASOBÓW INFORMATYCZNYCH

§ 1

ADO wykonuje i prowadzi na bieżąco inwentaryzację sprzętu wykorzystywanego do przetwarzania informacji mogących stanowić dane osobowe (inwentaryzacja zasobów informatycznych) oraz oprogramowania.

§ 2

Inwentaryzacja zasobów informatycznych polega ustaleniu w stopniu wyczerpującym i kompletnym:

a) jakie urządzenia są wykorzystywane do przetwarzania danych osobowych;
b) jakie oprogramowanie jest wykorzystywane do przetwarzania danych osobowych;
c) kategorii informacji przetwarzanych na konkretnych, odnotowanych co do tożsamości urządzeniach;
d) miejscu ich przechowywania;
e) osobach, które mogą mieć dostęp do tych urządzeń.

§ 3

Inwentaryzacja zasobów informatycznych zapisywana jest w formie dokumentu, którego wzór stanowi **załącznik nr 14.**

§ 4

Infrastruktura zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowi **załącznik nr 4**. Ponadto, ADO stosuje i wprowadza:

a) politykę czystego biurka **(załącznik nr 5);**
b) politykę kluczy **(załącznik nr 6);**
c) politykę haseł **(załącznik nr 7).**

CZEŚĆ CZWARTA – SZACOWANIE RYZYKA I WYBÓR ZABEZPIECZEŃ

§ 1

ADO przeprowadza ogólne szacowanie ryzyka, która polega na przyporządkowaniu do wyników inwentaryzacji z części pierwszej i drugiej potencjalnych zagrożeń dla bezpieczeństwa danych osobowych wraz z zapisem i uzasadnieniem decyzji o konkretnych **działaniach związanych z zabezpieczeniem informacji**.

§ 2

ADO zobowiązany jest do uwzględnienia możliwości nieuprawnionego lub przypadkowego:

a) zniszczenia
b) utraty
c) zmodyfikowania
d) nieuprawnionego ujawnienia
e) nieuprawnionego dostępu

§ 3

Szacowanie ryzyka przeprowadzane jest z perspektywy potencjalnych negatywnych skutków **dla osób, których dane osobowe są przetwarzane** w ramach prowadzonej działalności.

CZĘŚĆ PIĄTA – REALIZOWANIE OBOWIĄZKÓW INFORMACYJNYCH

§ 1

1. ADO przekazuje każdej osobie, której dane są przetwarzane odpowiednie klauzule informacyjne, chyba że przepis ustawy przewiduje zwolnienie z tego obowiązku.
2. ADO stosuje następujące klauzule informacyjne:
   a) klauzulę informacyjną dla osób rekrutowanych (**załącznik nr 19**);
   b) klauzulę informacyjną dla pracowników (**załącznik nr 21**);
   c) klauzulę informacyjną dla kontrahentów i klientów (**załącznik nr 24**);
   d) obwieszczenie pracodawcy oraz klauzulę informacyjną w zakresie stosowania monitoringu wizyjnego (**załącznik nr 15**).

CZĘŚĆ SZÓSTA – GOTOWOŚĆ DO REALIZACJI UPRAWNIEŃ OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

§ 1

ADO zapewnia możliwość dostępu do treści przetwarzanych danych osobowych – w formie udostępnienia bezpłatnej kopii danych osobowych (w formie elektronicznej lub papierowej), chyba że przepis ustawy zwalnia ją z tego obowiązku lub żądanie osoby, której dane są przetwarzane jest **ewidentnie nieuzasadnione** lub **nadmierne.**

§ 2

W przypadku uznania żądania za ewidentnie nieuzasadnione lub nadmierne należy uzasadnić odmowę realizacji żądania wskazując powody przemawiające za przyjęciem takiej kwalifikacji i w formie pisemnej przekazać uzasadnienie osobie wnoszącej żądanie informując, o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§ 3

W przypadku tych informacji, które są przetwarzane przy użyciu środków elektronicznych na podstawie zgody lub umowy, ADO przetwarza je w **formie pozwalającej na przekazanie i odczyt przez** innego administratora – jeżeli osoba, której dane dotyczą skorzysta z uprawnienia do przeniesienia dostarczonych przez nią danych.

CZĘŚĆ SIÓDMA – POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

W przypadku konieczności przekazania danych osobowych - zarówno w formie papierowej jak i elektronicznej – do podmiotu, który ma realizować cele wskazane przez ADO, uprzednio zawiera się umowę powierzenia przetwarzania.

CZĘŚĆ ÓSMA – NARUSZENIA OCHRONY DANYCH

§ 1

W przypadku pozyskania informacji z jakiegokolwiek źródła o potencjalnym naruszeniu ochrony danych, ADO natychmiast podejmuje niezbędne środki w celu ustalenia, czy konkretne zdarzenie miało miejsce, a następnie, czy stanowiło ono naruszenie ochrony danych osobowych. Na tyle, na ile jest to możliwe należy podjąć działania, które ograniczą rozmiar i dotkliwość naruszenia dla osób, których danych ono dotyczyło.

§ 2

Z chwilą stwierdzenia naruszenia, ADO niezwłocznie dokonuje klasyfikacji naruszenia.

§ 3

Każde stwierdzone naruszenie musi zostać odnotowane w wewnętrznym rejestrze naruszeń (**załącznik nr 13**), a te naruszenia, które zostały zaklasyfikowane jako chrakteryzujące się większym niż NISKI stopień powagi naruszenia muszą zostać zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych niezwłocznie – nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. Naruszenia, które zostały zaklasyfikowane jako chrakteryzujące się WYSOKIM lub BARDZO WYSOKIM stopniem powagi naruszenia muszą zostać natychmiastowo zakomunikowane osobom, których danych one dotyczyły.

CZĘŚĆ DZIEWIĄTA – MONITOROWANIE I SPRAWDZANIE

§ 1

ADO dokonuje okresowych sprawdzeń przestrzegania przepisów i procedur ochrony danych osobowych.

§ 2

W przypadku dokonywania aktualizacji należy sprawdzić, czy zachodzi konieczność dokonania ponownego szacowania ryzyka. W przypadku wątpliwości co do odpowiedniości zastosowanych środków bezpieczeństwa należy dokonać ponownej oceny ryzyka.

CZĘŚC DZIESIĄTA – POSTANOWIENIA KOŃCOWE

§ 1

W sprawach nieuregulowanych niniejszym dokumentem znajdują zastosowanie odpowiadające w konkretnej sprawie postanowienia zawarte w wytycznych, opiniach oraz decyzjach grupy roboczej art. 29, Europejskiej Rady Ochrony Danych, Urzędu Ochrony Danych Osobowych, Komisji Europejskiej oraz zatwierdzonych przez Urząd Ochrony Danych mechanizmach certyfikacyjnych lub kodeksach postępowania.

§ 2

Załącznik do niniejszej Polityki Bezpieczeństwa danych osobowych stanowi wykaz dokumentacji RODO **(załącznik nr 25)**

§ 3

Niniejszy dokument wchodzi w życie z dniem 3 sierpnia 2018 r.