POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W Rezydencji„KORAB”

1. Wstęp

2. PBDO jest dokumentem, który określa podstawowe zasady bezpieczeństwa w zakresie danych osobowych, jest zbiorem podstawowych zasad (reguł) obowiązujących przy przetwarzaniu danych osobowych we wszystkich zbiorach.

3. Dyrekcja oraz pracownicy deklarują pełne zaangażowanie w proces bezpieczeństwa przetwarzania danych osobowych przetwarzanych zarówno w sposób zautomatyzowany i niezautomatyzowany,

4. Celem PBDO jest ochrona danych osobowych, przetwarzanych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem UODO, RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

5. Rezydencja „KORAB" przetwarza wyłącznie dane osobowe niezbędne do jego właściwego funkcjonowania i realizowania przez niego zadań określonych w statucie, regulaminie organizacyjnym oraz w przepisach odrębnych, przy uwzględnieniu zasady celowości, proporcjonalności (minimalizacja) oraz adekwatności przy przetwarzaniu danych osobowych.

6. Rezydencja „KORAB" przetwarza tylko takie dane osobowe o pracownikach, które mają bezpośredni i jednoznaczny związek ze stosunkiem pracy.

7. Rezydencja„KORAB" dokłada wszelkich starań w celu zapewnienia należytego bezpieczeństwa przetwarzanym danym osobowym jako informacjom podlegającym szczególnej ochronie.

8. Najważniejsze zagadnienia ochrony danych osobowych - RODO

1) Prezes Urzędu Ochrony Danych Osobowych

Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych, jest organem nadzorczym w rozumieniu rozporządzenia 2016/679, w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016,) oraz w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującego i uchylającego decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz. Urz. UE L 135 z 24.05.2016,).

2) Zgodność przetwarzania z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) 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;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

2. Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów niniejszego rozporządzenia w odniesieniu do przetwarzania służącego wypełnieniu warunków określonych w ust. 1 lit. c) i e); w tym celu mogą dokładniej określić szczegółowe wymogi przetwarzania i inne środki w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, także w innych szczególnych sytuacjach związanych z przetwarzaniem przewidzianych w rozdziale IX.

3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:

a) w prawie Unii; lub

b) w prawie państwa członkowskiego, któremu podlega administrator.

Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa

członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

4. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1 RODO, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;

b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;

c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 RODO lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10 RODO;

d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;

e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

3) Obowiązki informacyjne przy przetwarzaniu danych - Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą.

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

d) informacje o prawie wniesienia skargi do organu nadzorczego;

e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

4. Ust. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

1.

4) Rejestrowanie czynności przetwarzania

1. Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;

b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;

b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;

d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną.

4. Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego.

5. Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania tych operacji przetwarzania. Motyw (82) preambuły.

5) Powierzenie przetwarzania danych

Zasady dotyczące powierzenia przetwarzania danych osobowych podmiotom zewnętrznym zostały określone w Polityce Bezpieczeństwa Informacji.

6) Ewidencja osób upoważnionych

Wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi załącznik nr 2 do niniejszej Polityki. Upoważnienia do przetwarzania danych osobowych wydaje się na polecenie ADO zgodnie z art. 29 RODO.

7) Osoba upoważniona do przetwarzania danych osobowych /personel/

Art. 29 RODO, podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

9. Infrastruktura przetwarzania danych osobowych

1. Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych:

Obszar przetwarzania danych osobowych tworzy budynek REZYDENCJI „KORAB" Dąbrówki 3, 72-500 Międzyzdroje. Recepcja, pokój Manager'a.

Budynek jest monitorowany wewnątrz i na zewnątrz – parking.

Wejścia do budynku zabezpieczone są drzwiami zamykanymi na klucz.

2. **Rejestr czynności przetwarzania danych osobowych stanowi załącznik nr 8 do niniejszej Polityki.**

3. **Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych**

1) Bezpieczeństwo osobowe

- Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także na podstawie oświadczeń o nieposzlakowanej opinii. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
- Ryzyko utraty bezpieczeństwa danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych, jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.
- Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie pisemnych oświadczeń.

2) Szkolenia w zakresie ochrony danych osobowych

Administrator Danych Osobowych uwzględnia następujący plan szkoleń:

- szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
- szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
- przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania

danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

3) Zabezpieczenia we własnym zakresie /po stronie personelu/

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

- polityki „czystego ekranu”- w przypadku chwilowego opuszczenia stanowiska pracy pracownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane.
- polityki „czystego biurka” – w trakcie pracy pracownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy pracownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych;
- dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
- niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
- pilnego strzeżenia akt, płyt CD/DVD, pamięci;
- niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
- przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła.

- niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy.;
- niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej;
- zachowania tajemnicy danych, w tym także wobec najbliższych;
- zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
- zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

4) Polityka kluczy

Klucze do pomieszczeń biurowych gdzie są przetwarzane dane osobowe mają tylko osoby uprawnione. Niedopuszczalnym jest przekręcenie klucza i pozostawienie go w zamku drzwi.

5) Zabezpieczenie szaf

Wszystkie pomieszczenia w których są przechowywane dokumenty papierowe, zostały wyposażone w szafy zamykane na klucz,

10. Wykaz załączników

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych;

Załącznik nr 2 – Ewidencja osób upoważnionych do przetwarzania danych osobowych;

Załącznik nr 3 – Oświadczenie o przeszkoleniu i zapoznaniu się z przepisami

Załącznik nr 4 – Oświadczenie dla służb sprzątających.

Załącznik nr 5 – Rejestr naruszeń ochrony danych

Załącznik nr 6 – Upoważnienie do przetwarzania danych osobowych dla służb sprzątających

Załącznik nr 7 – Obowiązek Informacyjny – kontrahenci

Załącznik nr 7a – Obowiązek Informacyjny – pracownicy

Załącznik nr 8 - Rejestry czynności przetwarzania danych osobowych

Załącznik nr 9 – Raport naruszenia ochrony danych

Załącznik nr 10 - Rejestr naruszeń ochrony danych osobowych

Załącznik nr 11 - Wzór umowy powierzenia przetwarzania