POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

w przedsiębiorstwie QBL Wojciech Śliwka
Daszyńskiego 70c, 43-450 Ustroń

Administrator Danych Osobowych: Wojciech Śliwka

1. PODSTAWA PRAWNA

Niniejsza „Polityka bezpieczeństwa" stanowi wykonanie obowiązku, o którym mowa w w art. 24 ust. 1 i 2 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) zwane RODO.

2. CEL OPRACOWANIA DOKUMENTU

Celem opracowania niniejszego dokumentu jest wytyczenie zasad i wymagań w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez **QBL Wojciech Śliwka** zwaną dalej również jako „Firma" w części podejmowanej działalności gospodarczej polegającej na prowadzeniu wypożyczalni sprzętu sportowego oraz szkoły narciarsko-snowboardowej. Ponadto, celem niniejszej Polityki Bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez Firmę w ramach wypożyczalni i szkoły, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem. Wypracowane zasady i wymagania mają ukierunkować działania zmierzające do budowy systemu bezpieczeństwa, a potem jego utrzymywania podczas eksploatacji systemów informatycznych, na poziomie odpowiadającym potrzebom organizacji.

3. DEFINICJE

1) **administrator – QBL Wojciech Śliwka** (również jako: „Firma"),
2) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne),

3) **informatyczne nośniki danych** – materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych osobowych w postaci cyfrowej lub analogowej,

4) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

5) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,

6) **przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych,

7) **rozliczalność danych** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

8) **rozporządzenie** – 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) zwane RODO,

4. CEL POLITYKI BEZPIECZEŃSTWA

Celem Polityki bezpieczeństwa jest ochrona danych osobowych, przetwarzanych przez Firmę w zakresie określonym w pkt.2, w szczególności ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

5. ZAKRES STOSOWANIA POLITYKI BEZPIECZEŃSTWA

W ramach zabezpieczenia danych osobowych ochronie podlegają:

a) sprzęt komputerowy – serwer, komputery osobiste (w tym laptopy) i inne urządzenia zewnętrzne,
b) oprogramowanie,
c) dane osobowe zapisane na informatycznych nośnikach danych oraz dane przetwarzane w systemach informatycznych,
d) hasła użytkowników,
e) bazy danych i kopie zapasowe,

f) wydruki,

g) związana z przetwarzaniem danych dokumentacja papierowa.

Polityka bezpieczeństwa dotyczy przetwarzania wszystkich danych osobowych, przetwarzanych przez Firmę w zakresie funkcjonowania wypożyczalni w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, a także w systemach informatycznych będących w dyspozycji Firmy i zawiera następujące informacje:

A. wykaz pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych),

B. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych,

C. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi,

D. sposób przepływu danych pomiędzy poszczególnymi systemami,

E. środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,

Polityka bezpieczeństwa ma zastosowanie wobec wszystkich komórek organizacyjnych Firmy w zakresie określonym pkt.2.

A. Obszar przetwarzania danych osobowych

Przetwarzanie danych osobowych przez Firmę odbywa się zarówno przy wykorzystaniu systemów informatycznych jak i poza nimi, tj. w wersji papierowej. Obszar przetwarzania danych osobowych przez Firmę został określony w załączniku nr 1 do Polityki bezpieczeństwa pt.: „Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe w Wypożyczalni". Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności przetwarzania danych osobowych.

B. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych

Wykaz zbiorów danych osobowych przetwarzanych przez Firmę oraz programów zastosowanych do przetwarzania tych danych stanowi załącznik 2 do Polityki bezpieczeństwa pt.: „Wykaz zbiorów danych osobowych i systemów zastosowanych do ich przetwarzania".

C. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi

Pola informacyjne (rodzaje przetwarzanych danych osobowych) w odniesieniu do poszczególnych zbiorów danych zostały określone w dokumencie „Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania" stanowiącym załącznik nr 2 do Polityki bezpieczeństwa.

D. Sposób przepływu danych pomiędzy poszczególnymi systemami

W ramach procesów przetwarzania danych nie dochodzi do przepływu danych pomiędzy różnymi systemami informatycznymi.

E. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Do elementów zabezpieczenia danych osobowych przez Firmę zalicza się:

a) stosowane metody zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),
b) odpowiednie środki zabezpieczenia danych w systemach informatycznych (zabezpieczenia techniczne),
c) nadzór administratora danych nad wprowadzonymi zasadami i procedurami zabezpieczenia danych (zabezpieczenie organizacyjne),
d) bezpieczeństwo osobowe.

a) zabezpieczenia fizyczne obejmują:

- dostęp do pomieszczeń, w których przetwarzane są dane osobowe objęty jest systemem kontroli dostępu,
- samodzielny dostęp do pomieszczeń jest możliwy wyłącznie dla osób upoważnionych, wstęp osób postronnych jest możliwy jedynie podczas obecności osób upoważnionych,
- przechowywanie akt w wersji papierowej w zamykanych na klucz szafach,
- kopie zapasowe zbioru danych osobowych przechowywane są w sejfie w innym pomieszczeniu niż to, w którym znajduje się komputer, na którym dane osobowe przetwarzane są na bieżąco,

b) zabezpieczenia techniczne obejmują:

- systemy informatyczne zastosowane do przetwarzania danych osobowych są legalne certyfikowane i aktualizowane,
- w systemach informatycznych w Firmie obowiązują zabezpieczenia na poziomie wysokim,
- zastosowano mechanizmy kontroli dostępu do systemów informatycznych i ich zasobów; uprawnienia są różne dla różnych grup użytkowników,

- zastosowano odpowiednie i regularnie aktualizowane narzędzia ochronne, w tym oprogramowanie antywirusowe, które jest regularnie aktualizowane,
- system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
- Okresowo jest tworzona kopia zapasowa danych na odrębnym fizycznie nośniku danych przechowywanym w miejscu powszechnie niedostępnym według zaplanowanego harmonogramu.

c) zabezpieczenia organizacyjne obejmują:

- osobą odpowiedzialną za bezpieczeństwo danych osobowych jest Administrator danych, który opracowuje i aktualizuje Politykę bezpieczeństwa, załączniki do Polityki bezpieczeństwa
- pracownicy Firmy, którzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą, o zaobserwowanych nieprawidłowościach informują Administratora;
- Osoby upoważnione do przetwarzania danych osobowych mające dostęp do danych osobowych, które są w dyspozycji Firmy, zobowiązane są do utrzymywania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu z określonego stanowiska, a także po ustaniu zatrudnienia; w tym celu osoby te podpisują oświadczenie o utrzymywaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia,
- Przetwarzanie danych osobowych może być wykonywane wyłącznie przez osoby, które zostały upoważnione do przetwarzania danych osobowych.
- Osoby przetwarzające dane osobowe zostały upoważnione do przetwarzania danych osobowych poprzez udzielenie upoważnienia lub zawarcie umowy. Ewidencja osób upoważnionych do przetwarzania danych osobowych, stanowi załącznik 4 do Polityki bezpieczeństwa.

d) zabezpieczenie osobowe

- należy zawierać odrębne umowy o powierzenia danych lub wydawać upoważnienia;

- wprowadza się obowiązek raportowania do administratora danych wszelkich naruszeń (incydentów), zauważonych podatności i innych słabych punktów oraz przypadków błędnego działania sprzętu i oprogramowania,
- należy niezwłocznie dokonywać wszelkich aktualizacji wymaganych przez stosowane oprogramowanie.

6. ROZPOWSZECHNIANIE I ZARZĄDZANIE DOKUMENTEM POLITYKI

1. Niniejszy dokument zawiera informacje o zabezpieczeniach, dlatego też został objęty ochroną na zasadzie tajemnicy przedsiębiorstwa w myśl art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2018 r. poz. 419). Wybrane jego elementy mogą zostać udostępnione innym podmiotom po zawarciu stosownej umowy o zachowaniu poufności.
2. Za zarządzanie dokumentem Polityki Bezpieczeństwa, w tym jego rozpowszechnianiem, aktualizacją, utrzymywaniem spójności z innymi dokumentami, jest odpowiedzialny Administrator.
3. Z treścią niniejszego dokumentu powinny zostać zapoznane wszystkie osoby upoważnione do przetwarzania danych osobowych, które z racji wykonywanych obowiązków i czynności mają dostęp do danych osobowych.
4. Integralną część niniejszej Polityki Bezpieczeństwa stanowią następujące załączniki:

a) Załącznik nr 1 – Wykaz pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe;
b) Załącznik nr 2 – Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania;
c) Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych;
d) Załącznik nr 4 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.