POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W PULS KAROLINA ŚLUSARSKA

Polityka bezpieczeństwa jest podstawowym dokumentem regulującym zasady zapewnienia bezpieczeństwa i ochronę osób fizycznych w związku z przetwarzaniem danych osobowych przez PULS Karolina Ślusarska.

Celem niniejszego dokumentu, jest zapewnienie kierunków działania i wsparcie administratora w celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych, oraz określenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w szczególności przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Niniejszy dokument opisuje procedury zapewnienia bezpieczeństwa przetwarzania danych osobowych zawartych w systemie informatycznym PULS Karolina Ślusarska oraz określa granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę w PULS Karolina Ślusarska.

Dokument zwraca uwagę jakie konsekwencje mogą ponosić osoby nieprzestrzegające procedur postępowania dla zapobiegania i minimalizowania skutków zagrożeń związanych z ochroną przetwarzania danych osobowych.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
- Ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 roku, poz. 1000).

I. Postawienia ogólne

Użyte w niniejszym opracowaniu określenia i skróty oznaczają:

- **RODO** – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
- **administrator** – PULS Karolina Ślusarska;
- **przetwarzanie** – wykonywanie jakichkolwiek operacji w sposób zautomatyzowany lub niezautomatyzowany takich jak zbieranie, utrwalanie, przechowywanie, pobieranie, przeglądanie, usuwanie lub niszczenie;

- **osoba upoważniona lub użytkownik** – osoba posiadająca upoważnienie wydane przez administratora do przetwarzania danych w sposób zautomatyzowany lub niezautomatyzowany w zakresie wskazanym w upoważnieniu;
- **osoba uprawniona** – osoba posiadająca uprawnienie wydane przez administratora, na mocy którego wykonuje w jego imieniu określone czynności;
- **identyfikator użytkownika (login) –** ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **hasło (password) –** ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie upoważnionej do pracy w systemie informatycznym;
- **zalogowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby;
- **odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
- **zbiór danych –** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficzni;
- **system informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- **zabezpieczenie danych – bezpieczeństwo systemu informatycznego** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych;
- **usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- **zgoda osoby, której dane dotyczą** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, gdzie osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
- **podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Celem Polityki Bezpieczeństwa jest zapewnienie bezpieczeństwa przetwarzania danych osobowych zgodnie z jej zasadami określonymi w art. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Polityka bezpieczeństwa jest zgodna z ogólnymi celami działania u Administratora. Celem opracowania i wdrożenia Polityki Bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych

Administratora jest utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów oraz określenie zasad ochrony, a w szczególności ochrony przed udostępnieniem osobom nieupoważnionym. Zabezpieczenie dotyczy danych osobowych przetwarzanych tradycyjnie (w formie papierowej) oraz w systemach informatycznych.

Na polecenie administratora niniejszy dokument może być zmieniany i aktualizowany w sposób, który nie będzie skutkował zmniejszeniem stopnia ochrony danych.

I. Obowiązki pracownicze wynikające z ochrony danych osobowych

- Obowiązek przestrzegania tajemnicy i poufności danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.
- Naruszenie zasad ochrony danych osobowych, w efekcie którego, nastąpiło udostępnienie danych osobie nie upoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych i przepisów RODO.
- Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez administratora, w zakresie indywidualnych obowiązków pracowniczych.
- Dane osobowe znajdujące się w posiadaniu Administratora mogą zostać udostępnione innym odbiorcom danych na zasadach określonych w RODO. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
  Osoba upoważniona przez administratora, jest zobowiązana do:

1. stosowania określonych procedur i środków, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
2. zachowania szczególnej staranności w trakcie wykonania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą;
3. podporządkowania się poleceniom przełożonego i przestrzegania ustalonych przez niego szczegółowych zasad i procedur.

II. Postępowanie podczas upoważnienia osób do przetwarzania danych osobowych

1. W przypadku przyjęcia do pracy nowego pracownika lub zmiany obowiązków pracownika już zatrudnionego, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, bezpośredni przełożony pracownika zobowiązany jest wystąpić do administratora z wnioskiem o wydanie upoważnienia do przetwarzania danych osobowych.
2. Pracownik, któremu administrator ma udzielić upoważnienia do przetwarzania danych osobowych, po przeprowadzeniu szkolenia z zakresu RODO jest zobowiązany do złożenia oświadczenia, o zapoznaniu się z przepisami RODO, ustawy o ochronie danych osobowych, „Polityki Bezpieczeństwa" oraz „Instrukcją zarządzania systemem informatycznym" i zobowiązuje się do stosowania zasad zawartych w tych dokumentach.
3. Na podstawie złożonego przez pracownika oświadczenia, administrator upoważnia pracownika do przetwarzania danych osobowych.

4. W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, bezpośredni przełożony pracownika zobowiązany jest bezzwłocznie skierować wniosek do administratora o wydanie lub cofnięcie upoważnienia do przetwarzania danych osobowych.
5. Zakończenie stosunku pracy jest równoznaczne z cofnięciem upoważnienia administratora do przetwarzania danych osobowych.

Administrator prowadzi i uaktualnia na bieżąco Ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów.

III. Postępowanie w przypadku utworzenia nowego zbioru danych osobowych

W przypadku zaistnienia konieczności utworzenia zbioru danych, wynikających z wypełniania obowiązków służbowych nałożonych przepisami bądź nowymi zasadami, pracownik Administratora zobowiązany jest niezwłocznie poinformować o tym fakcie administratora.

1. W zbiorach danych gromadzonych w systemie informatycznym zabrania się przetwarzania szczególnych kategorii danych ujawniających:
2. pochodzenie rasowe lub etniczne,
3. poglądy polityczne,
4. przekonania religijne lub światopoglądowe,
5. przynależność wyznaniową,
6. przynależność do związków zawodowych,
7. dane genetyczne,
8. dane biometryczne,
9. preferencje seksualne,

chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła wyraźną zgodę.

3. Zabrania się profilowania bez wyraźnej zgody, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych.

IV. Ochrona danych osobowych

Zagrożenia naruszenia ochrony danych osobowych powstają wskutek podjętych czynności:

1. zamierzonych – świadomie podjęte działania mające na celu naruszenie systemu ochrony danych osobowych spowodowanych działaniem lub zaniechanym działaniem przez pracownika,
2. wewnętrznych – niezamierzone błędy pracowników, awarie sprzętu komputerowego, oprogramowania itp.,
3. zewnętrznych – spowodowanych czynnikami zewnętrznymi, na które nie ma wpływu spółka, np.: wyładowania atmosferyczne, opady atmosferyczne, klęski żywiołowe itp.

Skuteczność ochrony danych osobowych uzależniona jest od współdziałania pracowników w czasie wprowadzania i utrzymania systemu bezpieczeństwa danych osobowych na każdym poziomie organizacyjnym. Szkolenia pracowników Administratora zarówno w czasie wprowadzania systemu ochrony jak i po jego wprowadzeniu mają na celu uniknięcie nieświadomego ujawnienia danych osobowych poprzez wynoszenie nieaktualnych lub źle wypełnionych dokumentów zawierających dane osobowe np.: brudnopisy i notatki w nich zawarte. Wprowadzenie do stosowania nowych rozwiązań technologicznych o charakterze zautomatyzowanym bądź zapisów regulaminowych i prawnych wymaga ciągłego aktualizowania systemu ochrony danych osobowych.

V. Obszar przetwarzania danych osobowych

1. Dane osobowe w systemie informatycznym przetwarzane są w obiektach wykonywania działalności przez Administratora. Pomieszczenia, w których przetwarzane są dane osobowe winny być zamykane na czas nieobecności w nich zatrudnionych osób, w sposób uniemożliwiający dostęp do nich osobom trzecim. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych osobowych jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych.
2. Obszar przetwarzania danych osobowych stanowią pomieszczenia lub części pomieszczeń, w których przechowywane są i przetwarzane dane osobowe z użyciem sprzętu komputerowego lub w formie kartotek, skorowidzów, ksiąg i wykazów oraz innych zbiorów ewidencyjnych. Szczegółowy wykaz miejsc, w których przetwarzane są dane osobowe określa załącznik nr 5 do Polityki Bezpieczeństwa.

VI. Wykaz zbiorów danych osobowych oraz ich struktura i powiązania między nimi

Wykaz oraz struktura zbiorów danych osobowych wskazujące zawartość poszczególnych pól informacyjnych i powiązania między nimi wraz z wskazaniem programów zastosowanych do ich przetwarzania określa załącznik nr 6 do Polityki Bezpieczeństwa.

VII. Środki techniczne i organizacyjne niezbędne dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych

Wykorzystane środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych określa załącznik nr 7 do Polityki Bezpieczeństwa.

Środki techniczne ochrony danych osobowych stosowane przez Administratora to:

1. Środki ochrony fizycznej.

2. Środki organizacyjne.
3. Środki ochrony technicznej.

W skład środków ochrony fizycznej przetwarzanych danych osobowych wchodzą:

1. wszelkiego rodzaju urządzenia służące do przetwarzania danych osobowych,
2. zamki drzwi wejściowych do pomieszczeń, w których przetwarzane są dane osobowe posiada administrator bądź uprawnieni pracownicy,
3. organizacja pracy obiektu – ustawienie ekranów komputerów w określony sposób, czyli w stronę, która nie daje możliwości dostępu do ich widoczności przy wejściu do pomieszczenia,
4. wszystkie zbiory w postaci kartotek, skorowidzów, spisów, wykazów itp. znajdują się w pomieszczeniach, które można zamknąć przed dostępem osób nieuprawnionych,
5. odseparowanie urządzeń Administratora od sieci internetowej poprzez fizyczne rozłączenie lub poprzez zastosowanie zapory sieciowej,
6. ochrona komputerów oprogramowaniem antywirusowym,
7. dokumenty papierowe zawierające dane osobowe niszczone są przy pomocy niszczarki o wysokim poziomie utajenia.

W skład środków organizacyjnych chroniących dane osobowe znajdujące wchodzą:

1. przeszkolenie pracowników Administratora przystępujących do przetwarzania danych osobowych zgodnie z zakresem obowiązków z zakresu przepisów prawa w zakresie ochrony danych osobowych i upoważnieniu ich przez administratora do przetwarzania danych osobowych,
2. sporządzanie sprawdzeń i przestrzeganie wszystkich wymaganych prawem czynności opisanych w niniejszym dokumencie,
3. prowadzenie rejestru podmiotów, którym powierzono przetwarzanie danych osobowych oraz podmiotów, które udostępniły dane osobowe,
4. wprowadzenie do stosowania w firmie Instrukcji zarządzania systemem informatycznym,
5. wprowadzenie i przestrzeganie zasady zabezpieczenia materiałów zawierających dane osobowe, a nie używanych w danym momencie, tzw. zasada czystego biurka,
6. dokonywania systematycznych kontroli przez osoby upoważnione przez administratora na okoliczność przestrzegania zasad ochrony danych osobowych,
7. ustawienia ekranów komputerów w sposób uniemożliwiający wgląd w dane przez osoby nieupoważnione do przetwarzania danych osobowych.

Zgodnie z art. 33 RODO, administrator danych bez zbędnej zwłoki, ale nie później niż w ciągu 72 godzin od stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych jest zobowiązany zgłosić ten fakt Prezesowi Urzędu Ochrony Danych Osobowych.

IX. Postanowienia końcowe

Wszyscy pracownicy zatrudnieni przez Administratora zobowiązani są zapoznać się z dokumentem Polityka Bezpieczeństwa danych osobowych oraz przestrzegania i stosowania reguł i trybów postępowania opisanych w tym dokumencie poprzez sporządzenie oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Wzór oświadczenia stanowi załącznik nr 1 do Polityki Bezpieczeństwa.

W sprawach nieuregulowanych niniejszym dokumentem zastosowanie mają przepisy określone rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 roku, poz. 1000).