POLITYKA OCHRONY DANYCH OSOBOWYCH

W

LABORATORIUM DROGOWYM SZCZECIN SP. Z O.O.
ul. Goleniowska 92, 70 – 830 Szczecin

zwana dalej ***Polityką***

sporządzona w oparciu o regulacje Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, w celu wykazania, że dane osobowe są gromadzone, przetwarzane i zabezpieczane zgodnie z wymogami prawa

Szczecin, dnia 25 maja 2018 r.

SPIS TREŚCI:

I. **Definicje**
II. **Postanowienia ogólne Polityki ochrony danych osobowych**
III. **Dane osobowe przetwarzane u administratora danych osobowych**
IV. **Obszar przetwarzania danych osobowych**
V. **Zapewnienie zgodności przetwarzania z prawem i zarządzanie bezpieczeństwem**
VI. **Środki techniczne i organizacyjne niezbędne dla zapewnienia ochrony danych osobowych**
VII. **Naruszenia zasad ochrony danych osobowych**
VIII. **Powierzenie przetwarzania danych osobowych**
IX. **Postanowienia końcowe**

I. DEFINICJE

- **Administrator danych** – Laboratorium Drogowe Szczecin Sp. z o.o.
-
- **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
- **Przetwarzanie danych** - wszelkie operacje, zarówno w formie tradycyjnej jak i elektronicznej, wykonywane na danych osobowych, takie jak gromadzenie, utrwalanie, przechowywanie, opracowywanie, zmienianie, przekazywanie, systematyzowanie, udostępnianie i usuwanie
- **Zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów
- **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. 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)
- **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych
- **Użytkownik** – osoba upoważniona przez Administratora danych do przetwarzania danych osobowych
- **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
- **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie

II. POSTANOWIENIA OGÓLNE POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka ma na celu zapewnienie bezpieczeństwa ochrony wszystkich danych osobowych przetwarzanych przez Administratora danych.
2. Polityka dotyczy wszystkich danych osobowych przetwarzanych przez Administratora danych, niezależnie od formy przetwarzania.
3. Wgląd do Polityki mają osoby upoważnione przez Administratora danych w celu zapoznania się z warunkami przestrzegania ochrony danych osobowych.
4. W celu realizacji Polityki Administrator danych zapewnia w odniesieniu do wszystkich, przetwarzanych danych:
   a) poufność danych - zapewnienie, iż dane osobowe nie będą udostępniane osobom nieupoważnionym,
   b) integralność danych - zapewnienie, iż dane osobowe nie będą zmieniane ani niszczone przez osoby nieupoważnione i w nieautoryzowany sposób; informacje i metody przetwarzania będą kompletne i dokładne,
   c) dostępność informacji - zapewnienie dostępu upoważnionym osobom do danych osobowych wtedy gdy jest to potrzebne,
   d) odporność i integralność systemu - zapewnienie osobom upoważnionym dostępu do danych w sytuacjach dużego obciążenia, a także zapewnienie komplementarności danych poprzez uniemożliwienie naruszenia systemu,
   e) analizę ryzyka - identyfikowanie, minimalizacja i eliminacja ryzyka związanego z bezpieczeństwem przetwarzanych danych osobowych

   Powyższe Administrator danych zapewnia poprzez wprowadzenie odpowiednich środków ochrony, w tym środków technicznych i organizacyjnych, nadzór nad przetwarzaniem danych, cykliczną analizę zastosowanych środków ochrony, które będą zgodne z niniejszą polityką oraz właściwymi przepisami prawa.

III. DANE OSOBOWE PRZETWARZANE U ADMINISTRATORA DANYCH OSOBOWYCH

1. Dane osobowe przetwarzane przez Administratora danych gromadzone są w zbiorach danych zarówno w formie tradycyjnej jak i elektronicznej.
2. Administrator danych nie podejmuje czynności przetwarzania wykazujących ryzyko dla praw i wolności osób.
3. Administrator danych prowadzi rejestr czynności przetwarzania dostępny w formie elektronicznej i tradycyjnej w siedzibie administratora danych (**Załącznik nr 1**).
4. Rejestr czynności przetwarzania obejmuje wszystkie procesy przetwarzania danych osobowych zachodzące u administratora danych.
5. Planowanie nowych czynności przetwarzania zostanie poprzedzone oceną skutków dla bezpieczeństwa i ochrony danych osobowych.

IV. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe przetwarzane przez Administratora danych znajdują się w siedzibie administratora danych, gdzie gromadzone są w formie tradycyjnej i elektronicznej.

2. Dane osobowe znajdują się i są przetwarzane na komputerach stacjonarnych oraz przenośnych, a także na innych urządzeniach mobilnych oraz nośnikach danych, którymi dysponuje administrator danych, i które są przeznaczone wyłącznie do użytku administratora danych i osób przez niego upoważnionych do przetwarzania danych osobowych.

V. ZAPEWNIENIE ZGODNOŚCI PRZETWARZANIA Z PRAWEM I ZARZĄDZANIE BEZPIECZEŃSTWEM

1. Administrator danych zapewnia, że przetwarzanie danych osobowych (przez Administratora danych jak i przez osoby upoważnione) odbywa się zgodnie z przepisami prawa, przy zastosowaniu środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzania danych.
2. Dane osobowe są przetwarzane w sposób przejrzysty, każdorazowo w oparciu o co najmniej jedną z podstaw przetwarzania określonych w art. 6 RODO.
3. Dane osobowe są przetwarzane w sposób odpowiadający celowi przetwarzania, tylko przez okres odpowiadający realizacji tego celu.
4. Administrator danych zapewnia zgodność przetwarzanych danych z rzeczywistością przez regularną ocenę aktualności przetwarzanych danych.
5. Administrator danych zapewnia anonimizację bądź usunięcie danych niezwłocznie po stwierdzeniu realizacji celu przetwarzania danych osobowych.
6. Administrator danych wypełnia obowiązek informacyjny wskazany w art. 13 i art. 14 RODO wobec osób, których dane dotyczą (**Załącznik nr 5 i 6**).
7. Wszystkie osoby upoważnione przez Administratora danych do przetwarzania danych są zobowiązane do zapoznania się i przestrzegania niniejszej Polityki oraz wewnętrznych procedur obowiązujących u Administratora danych, a związanych z przetwarzaniem danych osobowych.
8. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych będzie uważane w szczególności:
    a) udostępnienie bądź umożliwienie udostępnienia danych osobowych osobom nieupoważnionym,
    b) naruszenie integralności danych bądź zagrożenie wystąpienia takiego naruszenia,
    c) przetworzenie danych w sposób nieodpowiadającemu celowi przetwarzania,
    d) nieusunięcie danych osobowych niezwłocznie po zaistnieniu przesłanki do ich usunięcia,
    e) przetwarzanie danych bez podstawy prawnej,
    f) niekontrolowana utrata, zniszczenie, zmiana bądź kopiowanie danych osobowych.
9. W sytuacji stwierdzenia naruszenia zasad ochrony danych osobowych Administrator danych podejmie wszystkie niezbędne kroki w celu usunięcia naruszenia bądź zminimalizowania skutków jego wystąpienia.
10. W sytuacji zatrudniania pracowników bądź gdy istnieje pomiędzy administratorem danych a jego współpracownikiem stosunek cywilno-prawny, Administrator ma obowiązek zapewnić by wyznaczone do przetwarzania danych osoby posiadały upoważnienie do przetwarzania danych osobowych (**Załącznik nr 2**). Administrator

prowadzi w tym zakresie Ewidencję osób upoważnionych do przetwarzania danych osobowych (**Załącznik nr 3**).

11. W sytuacji zatrudniania pracowników bądź gdy istnieje pomiędzy Administratorem danych a jego współpracownikiem stosunek cywilno-prawny, Administrator zobowiązuje ww. do zachowania wszystkich przetwarzanych danych w tajemnicy i odpowiedniego ich zabezpieczenia (**Załącznik nr 4**).

VI. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA OCHRONY DANYCH OSOBOWYCH

1. Administrator danych wdraża proporcjonalne i odpowiednie dla swojej działalności środki organizacyjne i techniczne dla ochrony danych osobowych
2. Administrator prowadzi zbiór danych oraz systemów zastosowanych do ich przetwarzania (**Załącznik nr 7**).
3. Zabezpieczenia organizacyjne obejmują:
   a) opracowanie i wdrożenie niniejszej Polityki,
   b) opracowanie procedury postępowania w przypadku naruszenia danych osobowych,
   c) zapewnienie dostępu do danych osobowych jedynie osobom upoważnionym przez Administratora danych,
   d) zapoznanie osób upoważnionych do przetwarzania danych z niniejszą Polityką,
   e) uniemożliwienie dostępu do pomieszczeń, w których przetwarzane są dane osobowe osobom nieupoważnionym; przebywanie takich osób w tych pomieszczeniach możliwe jest wyłącznie w obecności osoby upoważnionej,
   f) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu firewall.
4. Zabezpieczenia techniczne obejmują:
   a) przechowywanie danych osobowych w pomieszczeniach zamkniętych, w odpowiednio zabezpieczonych szafach, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,
   b) wykonywanie kopii zapasowych danych i odpowiednie ich zabezpieczenie,
   c) zabezpieczenie komputerów stacjonarnych oraz urządzeń mobilnych odpowiednimi hasłami dostępu, cyklicznie zmienianymi,
   d) zabezpieczenie komputerów stacjonarnych oraz urządzeń mobilnych przed niepożądanym oprogramowaniem (program antywirusowy),
   e) szyfrowanie danych w przypadku ich przesyłania,
   f) używanie niszczarki do trwałego usuwania danych osobowych.

VII. NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

1. W przypadku podejrzenia naruszenia ochrony danych osobowych administrator danych dokonuje oceny ryzyka dla praw lub wolności osób fizycznych (**Załącznik nr 10**).
2. W sytuacji stwierdzenia, że naruszenie niesie za sobą wysokie ryzyko dla praw lub wolności osób fizycznych administrator niezwłocznie powiadamia o tym fakcie organ nadzorczy, nie później jednak niż w przeciągu 3 dni od dnia ujawnienia naruszenia -

jeżeli jest to wykonalne pod względem technicznym i organizacyjnym (**Załącznik nr 11**).

VIII. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami określonymi w art. 28 RODO (**Załącznik nr 8**). Administrator prowadzi ewidencję podmiotów, z którymi zawarł umowę powiedzenia (**Załącznik nr 9**).
2. Administrator danych w miarę swoich możliwości przed powierzeniem przetwarzania danych sprawdza wybrany podmiot pod względem zapewnienia przez niego gwarancji wdrożenia procedur ochrony danych osobowych

IX. PRZEKAZYWANIE DANYCH DO PAŃSTWA TRZECIEGO

1. Administrator danych osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

X. POSTANOWIENIA KOŃCOWE

1. Polityka jest przechowywana w siedzibie administratora w formie papierowej i w wersji elektronicznej.
2. Za niedopełnienie obowiązków wynikających z niniejszej Polityki Ochrony Danych Osobowych pracownik ponosi odpowiedzialność na podstawie przepisów Kodeksu Pracy, przepisów o ochronie danych osobowych oraz RODO.
3. Integralną częścią Polityki stanowią następujące **załączniki:**

Załącznik 1 - Rejestr czynności przetwarzania danych osobowych przez Administratora
Załącznik 2 - Wzór upoważnienia dla osoby przetwarzającej dane osobowe
Załącznik 3 – Wzór Ewidencji osób upoważnionych do Przetwarzania danych osobowych
Załącznik 4 – Wzór oświadczenia o zachowaniu poufności
Załącznik 5 – Wzór informacji zgodnie z art. 13 RODO
Załącznik 6 – Wzór informacji zgodnie z art. 14 RODO
Załącznik 7 – Wzór zbioru danych i systemów do przetwarzania danych osobowych
Załącznik 8 – Wzór umowy powiedzenia
Załącznik 9 – Wzór Ewidencji umów powierzenia
Załącznik 10 – Wzór raportu z incydentu naruszenia danych osobowych
Załącznik 11 – Wzór zgłoszenia incydentu naruszenia ochrony danych osobowych.

Załączniki dostępne w siedzibie firmy