

# Polityka Bezpieczeństwa

dla

**Organizacji LTD24 sp. z o.o. sp.k.**

wydana 13.08.2018

| Wersja dokumentu. | Osoba odpowiedzialna za utworzenie / aktualizację dokumentu. | Data         | Zakres aktualizacji                 |
|-------------------|--------------------------------------------------------------|--------------|-------------------------------------|
| 1.0               | Szymon Wiktorowicz                                           | 10.08.2018r. | Utworzenie Polityki Bezpieczeństwa. |

## SPIS TREŚCI

|                                                                                                                                                        |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1. Wprowadzenie.....                                                                                                                                   | 3 |
| 2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. ....                                  | 4 |
| 3. Wykaz zbiorów danych przetwarzanych w organizacji ze wskazaniem programów, w których dane są przetwarzane. ....                                     | 4 |
| 4. Opis struktury danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. ....                               | 5 |
| 5. Sposób przepływu danych pomiędzy poszczególnymi systemami. ....                                                                                     | 6 |
| 6. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. .... | 7 |
| 7. Zasady nadawania, zmiany i wygaśnięcia uprawnień do przetwarzania danych osobowych. ....                                                            | 8 |
| 8. Zasady udostępniania danych osobowych.....                                                                                                          | 8 |
| 9. Postępowanie w przypadku naruszenia ochrony danych osobowych.....                                                                                   | 8 |
| 10. Postanowienia końcowe .....                                                                                                                        | 9 |

## 1. Wprowadzenie

Polityka bezpieczeństwa jest zestawem praw, zasad i praktycznych rozwiązań regulujących przetwarzanie danych osobowych w organizacji i została przygotowana na podstawie przepisów<sup>1</sup>:

- Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922),
- Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 Nr 100, poz. 1024),

Nadrzędnym celem dokumentu jest wyznaczenie standardów bezpieczeństwa adekwatnych do funkcjonowania organizacji w obecnym czasie ( tj. w erze cyfrowej). Celem dokumentu jest stworzenie, w organizacji, prawnych gwarancji zapewnienia ochrony danych osobowych, przetwarzanych w celu usprawiedliwionym prowadzoną działalnością. Dokument

Polityka obowiązuje wszystkie osoby zatrudnione, w organizacji, na podstawie umowy o pracę oraz umów cywilnoprawnych, a także dostawców i podmioty współpracujące, które mają jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Przetwarzanie danych osobowych w organizacji odbywa się w wersji papierowej oraz z wykorzystaniem systemów informatycznych.

Administratorem danych osobowych (ADO) w organizacji jest – LTD24 sp. z o.o. sp. k.

Administrator danych osobowych pełni rolę administratora bezpieczeństwa informacji (ABI).

<sup>1</sup>• Od 25 maja 2018 w Polityce Bezpieczeństwa powinno się znaleźć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. Urz. UE L nr 119, str. 1).

Po zmianie przepisów prawa krajowego trzeba podać aktualne przepisy dot. ochrony danych osobowych.

## 2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Przetwarzanie danych osobowych odbywa się w siedzibie organizacji pod adresem ul. Sobieskiego 5/26 , 85-060 Bydgoszcz.

- Pomieszczenie zgodne z adresem siedziby

Dostęp do pomieszczeń i obszarów, w których przetwarzane są dane osobowe mają:

A. osoby reprezentujące organizację:

| Nazwa stanowiska | Dni tygodnia        | Godziny |
|------------------|---------------------|---------|
| Prezes zarządu   | poniedziałek-piątek | 8-18    |

## 3. Wykaz zbiorów danych przetwarzanych w organizacji ze wskazaniem programów, w których dane są przetwarzane.

W organizacji przetwarzane są następujące zbiory danych: pracownicy i klienci indywidualni.

| Nazwa zbioru | Podstawa prawna                                                                                                                                                                                              | Cel przetwarzania danych                                    | Kategoria osób                    | Program komputerowy zastosowany do przetwarzania danych w zbiorze |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------|
| Pracownicy   | Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz. U. z 1974 r. Nr 24, poz. 141.;<br><br>Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922, ze zm.). | Realizacja zadań pracodawcy wynikających z przepisów prawa. | Kandydaci do pracy.<br>Pracownicy |                                                                   |

| Nazwa zbioru         | Podstawa prawna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Cel przetwarzania danych      | Kategoria osób       | Program komputerowy zastosowany do przetwarzania danych w zbiorze |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------------------|-------------------------------------------------------------------|
| Klienci indywidualni | Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922, ze zm.);<br>Ustawa z dnia 27 lipca 2002 r. o szczególnych warunkach sprzedaży konsumenckiej oraz o zmianie Kodeksu cywilnego (Dz.U. 2002 nr 141 poz. 1176)<br>Ustawa z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny Dz.U. 2000 nr 22 poz. 271<br>Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204) | Realizacja zamówień klientów. | Klienci indywidualni |                                                                   |

#### 4. Opis struktury danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Dane osobowe ze zbioru „Pracownicy” przetwarzane są w formie papierowej i elektronicznej i obejmują następujący zakres:

- nazwisko i imię (imiona),
- datę i miejsce urodzenia,
- PESEL,

- serię i numer dowodu osobistego,
- numer rachunku bankowego,
- wykształcenie,
- przebieg dotychczasowego zatrudnienia,
- numer prawa jazdy
- imiona i nazwiska oraz daty urodzenia dzieci pracownika oraz współmałżonka, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,
- adres zameldowania, zamieszkania i adres do korespondencji,
- numer telefonu komórkowego,
- adres e-mail.
- adres do wysyłki,

## **5. Sposób przepływu danych pomiędzy poszczególnymi systemami.**

Organizacja posiada własny system informatyczny służący do przetwarzania danych osobowych o nazwie: wFirma

Dane osobowe przetwarzane są również przy użyciu edytora tekstu (MS Word, Pages), arkusza kalkulacyjnego (MS Excel, Numbers) oraz innych dostępnych programów do tworzenia baz danych.

Organizacja korzysta w zakresie przetwarzania danych osobowych również z zewnętrznych systemów informatycznych:

- System „Płatnik” – będący aplikacją Zakładu Ubezpieczeń Społecznych przeznaczoną dla płatników składek i zapewniającą pełną obsługę dokumentów ubezpieczeniowych i wymianę informacji z ZUS.

Podmioty, do których przekazywane są dane to:

- Zakład Ubezpieczeń Społecznych
- Urząd Sakrbowy
- Banki
- Powiatowy Urząd Pracy
- Przychodnia Medycyny Pracy

Powyższe dane przekazywane są w formie papierowej lub za pośrednictwem Internetu.

## **6. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.**

Do zastosowanych w organizacji środków technicznych, służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należą:

- stosowanie zróżnicowanych poziomów uprawnień, określonych dla danego stanowiska pracy, do poszczególnych systemów informatycznych,
- stosowanie loginów i haseł uniemożliwiających korzystanie z komputerów osobom nieupoważnionym,
- okresowa zmiana haseł do komputerów,
- ustawienie monitorów komputerów w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

Do zastosowanych w organizacji środków organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należą:

- opracowanie i wdrożenie „Polityki Bezpieczeństwa”,
- nadanie przez ADO, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom upoważnień do przetwarzania danych osobowych,
- podpisanie umów powierzenia danych osobowych z podmiotami współpracującymi,
- wyznaczenie Administratora Systemu Informatycznego (ASI) przez ADO,
- sprawowanie przez ADO oraz ASI kontroli i nadzoru nad procesem wprowadzania danych osobowych do zbiorów oraz ich udostępniania.

Wydruki, kartoteki oraz dokumenty papierowe, na których znajdują się dane osobowe są przechowywane w zamykanych na klucz szafkach. Wydruki zawierające dane osobowe przeznaczone do usunięcia - niszczy się w niszczarce.

Pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz. Pracownicy zostali poinstruowani, że niedopuszczalne jest pozostawienie osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe w czasie nieobecności osób upoważnionych. W razie konieczności opuszczenia pomieszczenia przez osobę upoważnioną, dane osobowe należy zabezpieczyć w taki sposób, aby nie dostały się w niepowołane ręce.

## **7. Zasady nadawania, zmiany i wygaśnięcia uprawnień do przetwarzania danych osobowych.**

Przed przystąpieniem do przetwarzania danych osobowych w organizacji, każdy pracownik jest zobowiązany:

- uczestniczyć w szkoleniu w zakresie ochrony i przetwarzania danych osobowych,
- zapoznać się z dokumentami dotyczącymi przetwarzania danych osobowych i stosować się do ich postanowień,
- podpisać upoważnienie do przetwarzania danych osobowych – i przetwarzać dane tylko w zakresie objętym upoważnieniem, powyższe upoważnienia gromadzone są przez ADO w ewidencji upoważnień,
- zachować w tajemnicy przetwarzane dane osobowe oraz sposób ich zabezpieczenia także po ustaniu zatrudnienia.

W przypadku zmiany zakresu zadań na tym samym lub innym stanowisku, ADO zobowiązany jest do zweryfikowania zakresu upoważnienia do przetwarzania danych i jego aktualizacji. Aktualizacja może dotyczyć rozszerzenia uprawnień, ale także cofnięcia upoważnienia na przetwarzanie danych osobowych.

## **8. Zasady udostępniania danych osobowych.**

Dane osobowe w organizacji mogą być wydawane jedynie na pisemny wniosek, osobie której dotyczą lub osobie przez nią upoważnionej na piśmie.

## **9. Postępowanie w przypadku naruszenia ochrony danych osobowych.**

Każda osoba przetwarzająca dane osobowe w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym administratora danych osobowych lub inną upoważnioną osobę.

Do czasu przybycia na miejsce naruszenia danych osobowych ADO lub upoważnionej przez niego osoby należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych,
- udokumentować wstępnie zaistniałe naruszenie,

- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, ADO lub osoba przez niego upoważniona:

- zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji,
- może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji.

Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem / ujawnieniem ochrony danych osobowych, ADO zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych. ADO dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych,
- określenie czasu i miejsca: naruszenia / ujawnienia i powiadomienia o tym fakcie,
- określenie okoliczności towarzyszących i rodzaju naruszenia / ujawnienia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia / ujawnienia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego,
- wnioski co do ewentualnych przedsięwzięć: proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom / ujawnieniom w przyszłości.

## **10. Postanowienia końcowe**

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która po stwierdzeniu naruszenia / ujawnienia ochrony

danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie ADO.

Osoby, które zostały zapoznane z niniejszym dokumentem, zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt poprzez podpisanie oświadczenia.