POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. CEL WPROWADZENIA POLITYKI

W związku z wejściem w życie ustawy z dnia 10 maja 2018 r. o Ochronie Danych Osobowych, Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r (RODO) oraz obowiązywaniem § 3, 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. Nr 100 poz. 1024) wprowadza się Politykę bezpieczeństwa ochrony danych osobowych w INQOO BUSINESS oraz Instrukcję zarządzania systemem informatycznym załącznik nr 1 do niniejszej Polityki.

Celem Polityki jest:

1) Wprowadzenie systemu ochrony danych osobowych,

2) Inicjowanie działań podnoszących efektywność i sprawność w zakresie ochrony danych osobowych w INQOO BUSINESS

3) Wskazanie działań, jakie należy wykonać oraz jakie ustanowić zasady i reguły postępowania, aby administrator danych mógł właściwie wykonywać zadania w zakresie ochrony danych osobowych.

2. ZAKRES STOSOWANIA

2.1. Dokument dotyczy pracowników i współpracowników (niezależnie od formy współpracy) INQOO BUSINESS przetwarzających dane osobowe, a także każdej osoby mającej dostęp do tychże danych osobowych.

2.2. Dokument może obejmować również przedsiębiorców, którzy zawrą umowę z INQOO BUSINESS na podstawie, której powierzone zostaną im dane osobowe na podstawie osobnych przepisów prawa powszechnie obowiązującego lub charakteru wyrażonej zgody.

3. DEFINICJE, TERMINOLOGIA I INFORMACJE DODATKOWE

Polityka bezpieczeństwa ochrony danych osobowych – zestaw wewnętrznych regulacji i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych (zwana dalej „Polityką").

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na jej imię i nazwisko albo jeden lub wszelkie inne czynniki umożliwiające identyfikację bez nadmiernego nakładu działań. Informacji nie uważa się za umożliwiającą określenie tożsamości, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Administrator danych osobowych (Administrator) – Przetwarzający albo podmiot, który zawarł z Przetwarzającym Umowę o powierzeniu przetwarzania danych osobowych.

Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Hasło użytkownika systemu informatycznego – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Upoważnienie – dokument upoważniający pracownika do przetwarzania danych osobowych.

Przetwarzający – INQOO BUSINESS

Pisemne przekazanie – każda udokumentowana forma dostarczenia informacji (mail, fax., list polecony, pismo za potwierdzeniem odbioru itp.).

Ustawa – Ustawa z dnia 10 maja 2018 r. o Ochronie Danych Osobowych.

Umowa – umowa, o której mowa w art. 31 ust. 1 Ustawy zawarta pomiędzy Administratorem Danych Osobowych i Przetwarzającym, mocą której przetwarzanie danych osobowych powierzone zostaje Przetwarzającemu.

4. ODPOWIEDZIALNOŚĆ ZA STOSOWANIE POLITYKI

4.1. Osoby odpowiedzialne za stosowanie polityki

4.1.1. Właściciel firmy – odpowiada za egzekwowanie stosowania postanowień Polityki i wyciąganie konsekwencji za jej naruszanie oraz nadzorowanie.

4.1.2. IOD, jeżeli został powołany, odpowiada za wskazanie standardów i nadzorowanie przestrzegania zasad ochrony danych osobowych w firmie oraz za zabezpieczenie danych osobowych w systemach informatycznych i danych utrwalonych w formie papierowej. W przypadku braku powołania IOD, jego funkcje wykonuje Właściciel INQOO BUSINESS lub osoba przez niego wskazana w formie pisemnej.

4.1.3. Pozostali pracownicy odpowiadają za przestrzeganie i praktyczne stosowanie Polityki.

4.1.4. W przypadku powołania IOD jest on zobowiązany również do:

- zapewniania przestrzegania przepisów o ochronie danych osobowych w sposób określony w Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r., poz. 745),
- prowadzenia rejestru zbiorów danych przetwarzanych przez administratora danych w sposób określony w Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r., poz. 719).

4.2. Oświadczenie potwierdzające cele i zasady bezpieczeństwa danych osobowych

4.2.1. Przetwarzający planuje podjęcie odpowiednich działań dla zapewnienia ochrony i bezpieczeństwa danych osobowych przed wszelkimi zagrożeniami, a w szczególności z zagrożeniami wynikającymi z przetwarzania danych w systemach informatycznych. Wyraża się to m.in. poprzez wynajem zewnętrznego serwera zgodnego z przepisami RODO, zapewnienie odpowiednich, zamykanych na klucz szaf, podnoszenie kwalifikacji pracowników w zakresie danych osobowych.

4.2.2. Poprzez zapewnienie bezpieczeństwa należy rozumieć stan uniemożliwiający bezprawne przetwarzanie, zmianę, utratę, uszkodzenie lub zniszczenie danych osobowych w firmie przez osoby postronne lub nieupoważnione.

4.2.3. Niniejszy dokument został przygotowany z myślą o zapewnieniu standardów bezpieczeństwa danych osobowych w firmie Przetwarzającego ze szczególnym uwzględnieniem zgodności z prawem.

5. PRACA Z DANYMI OSOBOWYMI

5.1. W firmie Przetwarzającego praca z danymi powinna być prowadzona wyłącznie przez osoby, którym wystawiono upoważnienie lub wynika to z przepisów lub charakteru świadczonej umowy. Osoby te mają obowiązek:

- przetwarzać dane osobowe zgodnie z przepisami prawa oraz niniejszą Polityka,
- chronić dane osobowe przed udostępnieniem osobom nieupoważnionym oraz przed zniszczeniem.

5.2. Upoważnienie zatwierdza Właściciel lub upoważniony przez niego pracownik, upoważnienie przekazywane jest do akt pracowniczych. Upoważnienie traci swą moc prawną w momencie ustania okresu na który zostało udzielone, lub w wypadku:

- ustania stosunku pracy,
- zakończenia wykonywania prac określonych umową zlecenia/umową o dzieło,
- zakończenia kontraktu z kontrahentem zewnętrznym.

5.3. Dane osobowe mogą być przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

5.4. Zbierane dane muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Rodzaj i treść danych nie może wykraczać poza potrzeby wynikające z celu ich zbierania.

5.5. Zabronione jest zbieranie danych nieistotnych, niemających znaczenia, danych o większym stopniu szczegółowości niż to wynika z określonego celu.

6. PRZETWARZANIE DANYCH OSOBOWYCH

6.1. Dane osobowe przetwarzane są w szczególności poprzez ich:

- utrwalanie,
- przechowywanie,
- opracowywanie,
- udostępnianie,
- usuwanie

w szczególności w systemie informatycznym i w formie papierowej.

6.2. W przypadku powierzenia przetwarzania danych osobowych podmiotom zewnętrznym w imieniu Przetwarzającego na podstawie Umowy, należy zawrzeć pisemną umowę zgodnie z wymogami ustawy i RODO. W przypadku powierzenia przetwarzania danych osobowych kopię stosownej umowy należy przekazać Właścicielowi. Przed podpisaniem Umowy należy zweryfikować, czy podmiot zewnętrzny spełnia ustawowe przesłanki dopuszczalności udostępnienia danych osobowych w drodze Umowy.

6.3. Przekazujący upoważnia pracowników do udostępniania danych osobowych osobie, której dane dotyczą. W przypadku wniosku osoby, której dane dotyczą odpowiedź musi nastąpić w terminie 30 dni od daty jego otrzymania. Odpowiedź musi zawierać następujące informacje:

- Jakie dane osobowe zawiera zbiór,
- W jaki sposób zebrano dane,
- W jakim celu i zakresie dane są przetwarzane,
- W jakim zakresie i komu dane zostały udostępnione,
- Inne informacje, o które prosi wnioskujący, o ile nie stanowią tajemnicy przedsiębiorstwa.

Fakt udostępnienia danych osobowych odnotowuje się w rejestrze udostępnień danych osobowych.

6.4. Każdorazowe udostępnienie danych osobowych, na umotywowany wniosek upoważnionych instytucji i organów powinno być konsultowane z Właścicielem lub upoważnionym pracownikiem. Należy odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to:

- ujawnienie wiadomości stanowiących tajemnicę państwową,
- zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
- zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
- istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

Przed udostępnieniem danych osobowych na wniosek jakiejkolwiek instytucji, należy gruntownie przeanalizować, czy przedmiotowa instytucja posiada stosowną podstawę prawną do wnioskowania o udzielenie tego typu informacji.

6.5. Przetwarzanie danych osobowych w systemie informatycznym powinno odbywać się na poziomie wysokim.

6.6. Powierzenie przetwarzania danych osobowych osobom, które nie posiadają upoważnienia, a które to muszą dokonać prac serwisowych lub im podobnych możliwe jest wyłącznie:

- po podpisaniu przez taką osobę oświadczenia o zachowaniu poufności albo,
- gdy osoba taka wykonuje powierzone jej czynności pod nadzorem osoby posiadającej ww. upoważnienie,
- gdy wynika to z odrębnych przepisów lub charakteru świadczonej umowy.

6.7. W przypadku zbierania danych osobowych od osoby, której dane dotyczą, należy ją poinformować w przystępnej dla niej formie o:

- adresie swojej siedziby i pełnej nazwie,
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
- możliwości wycofania wcześniej udzielonej zgody

6.8. Celem zapewnienia prawidłowego przetwarzania danych osobowych w firmie prowadzone są również następujące rejestry i ewidencje:

- Rejestr osób upoważnionych do przetwarzania danych osobowych
- Rejestr podmiotów, którym powierzono przetwarzanie danych osobowych
- Rejestr zbiorów danych prowadzony przez Właściciela,
- Rejestr naruszeń polityki bezpieczeństwa ochrony danych osobowych.

7. TWORZENIE ZBIORÓW DANYCH OSOBOWYCH

7.1. Administrator może tworzyć zbiory danych osobowych

7.2. Opisy struktur zbiorów danych osobowych oraz powiązań między zbiorami jak również sposób przepływu danych pomiędzy poszczególnymi systemami prowadzi Właściciel. Zbiory danych muszą spełniać przepisy RODO.

7.3. W przypadku konieczności wprowadzenia istotnych zmian dotyczących struktury zbioru danych osobowych lub zasad przetwarzania danych w zbiorze pracownik powiadamia o tym powiadamia Właściciela. Zmiany mogą być wprowadzone po uzyskaniu zgody Właściciela.

7.4. Usuwanie danych osobowych przetwarzanych w systemach informatycznych wykonywane może być zgodnie z instrukcjami Właściciela oraz instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

8. INSTRUKCJA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

8.1. Incydenty naruszenia bezpieczeństwa

Przypadki mogące wskazywać na zaistnienie sytuacji kryzysowych:

- przekazanie osobie nieuprawnionej danych osobowych,
- uzyskanie sygnału o naruszeniu ochrony danych osobowych,
- niedopełnienie obowiązku ochrony danych osobowych,
- zaginięcie dokumentów lub nośnika zawierającego dane osobowe,
- ujawnienie indywidualnych haseł lub udostępnienie kluczy do pomieszczeń, w których przetwarzane są dane osobowe,
- próba lub naruszenie integralności danych oraz modyfikacje w dokumentach lub systemie przetwarzania danych,
- wykorzystywanie nielegalnych aplikacji lub elementów nielegalnego oprogramowania,
- wykonanie nieuprawnionych kopii danych osobowych.

8.2. Procedura postępowania w sytuacjach kryzysowych

8.2.1. W przypadku ujawnienia incydentu opisanego w pkt 8.1 pracownik powinien:

- powstrzymać się od podjęcia działań skutkujących zniszczeniem lub uszkodzeniem stosownych dowodów,
- zabezpieczyć dowody i zapobiec dalszym zagrożeniom,
- niezwłocznie powiadomić o zaistniałej sytuacji kierownika komórki organizacyjnej w obszarze swojego działania lub w przypadku jego nieobecności bezpośredniego przełożonego.

8.2.2. W przypadku zaistnienia incydentu naruszenia bezpieczeństwa pracownik właściwy do obsługi systemów informatycznych podejmuje działania w zakresie przywrócenia bezpieczeństwa systemu, przeprowadza niezbędne czynności w celu wyjaśnienia incydentu oraz sporządza informację, którą przekazuje Właścicielowi.

8.2.3. Właściciel lub osoba przez niego upoważniona sporządza na temat incydentu informację, którą przedstawia organowi zarządzającemu Przetwarzającego oraz poleca podjęcie działań niezbędnych do likwidacji incydentu. W przypadku, gdy incydent powstał w wyniku uchybienia przez pracownika ustalonej polityki mogą zostać podjęte kroki dyscyplinarne.

8.2.4. Po rozwiązaniu wszelkich komplikacji wynikających z incydentów naruszających bezpieczeństwo danych osobowych, należy niezwłocznie poinformować zainteresowane osoby, które dane udostępniły.

8.3. Zadania osób

8.3.1. Osobę, która ma zostać upoważniona do przetwarzania danych osobowych kierownik komórki organizacyjnej zapoznaje z:

- Ustawą z dnia 10 maja 2018 o Ochronie danych osobowych.
- Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. Nr 100, poz. 1024),
- Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r., poz. 719),

- Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r., poz. 745),
- niezbędną dokumentacją polityki bezpieczeństwa ochrony danych osobowych.

8.3.2. Po zapoznaniu się z wyżej wymienionymi dokumentami osoba kierująca komórką organizacyjną wnioskuje do Właściciela o wydanie upoważnienia.

8.3.3. Pracownikowi wydaje się upoważnienie.

8.4. Inne zagrożenia i ochrona przed nimi

8.4.1. Dokumenty oraz nośniki zawierające dane osobowe przechowywane są w wydzielonym pomieszczeniu, do którego dostęp mają wyłącznie osoby upoważnione, na należycie zabezpieczonych urządzeniach do przechowywania danych cyfrowych, takich jak serwery spełniające standardy RODO, w specjalistycznych szafach.

9. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

9.1. Dane osobowe przechowywane w systemach informatycznych nie są przetwarzane w sposób zautomatyzowany.

9.2. Zbiorami danych osobowych objęte są przede wszystkim dane osobowe pracowników oraz kontrahentów Administratorów Danych Osobowych przekazane do przetwarzania na mocy Umowy.

9.4. Zbiór danych osobowych przechowywany jest w siedzibie, tj. pod adresem: INQOO BUSINESS 40-082 Katowice, ul. Jana III Sobieskiego 2.

10. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

10.1. Celem zabezpieczenia zbiorów danych osobowych przed dostępem osób nieupoważnionych wprowadza się szczegółowe rozwiązania techniczne i organizacyjne przedstawione w niniejszej Polityce oraz Instrukcji zarządzania systemem informatycznym.

10.2. Dane osobowe zapisywane na nośniku elektronicznym należy szyfrować lub zabezpieczyć hasłem. Nośniki wykorzystywane do celów operacyjnych należy przechowywać, w czasie nieobecności w pomieszczeniu osoby upoważnionej, w zamykanych na klucz szafach lub sejfach. W przypadku, gdy zbiór danych osobowych był zapisany na nośniku w sposób trwały i nie będzie dalej wykorzystywany, należy go zniszczyć fizycznie po skopiowaniu danych na dysk twardy stacji roboczej (serwera), wprowadzeniu do systemu, aplikacji itp.

10.3. Dla zabezpieczenia zbiorów danych osobowych wprowadza się system uwierzytelniania użytkowników zabezpieczony, co najmniej 8-znakowym hasłem zawierającym małe i wielkie litery oraz cyfry i znaki specjalne.

10.4. Zarządzanie stacjami roboczymi i uprawnieniami użytkowników powinno odbywać się centralnie z wykorzystaniem dostępnych mechanizmów. Stacje robocze i serwery monitorowane są przez system ochrony antywirusowej oraz jednocześnie powinno się stosować system śledzenia, wykorzystania sprzętu i oprogramowania. Komunikacja pomiędzy stacjami roboczymi i serwerami odbywa się w oparciu o bezpieczne protokoły transmisji danych. Styk sieci lokalnej z siecią publiczną chroniony jest przez zastosowanie zapory ogniowej (firewall) oraz jej bieżący monitoring.

10.5. Komunikacja z siecią publiczną powinna odbywać się przez jeden punkt dostępu. Porty protokołu TCP/IP, które nie są wykorzystywane do transmisji danych są blokowane. Na urządzeniach sieciowych włączono logowania na podstawie kodu i hasła. Adresy protokołu TCP/IP powinny być nadawane centralnie i otrzymać je mogą wyłącznie urządzenia, których adresy fizyczne zarejestrowano w bazie danych MAC adresów.

10.6. Wprowadza się mechanizm domeny dla zarządzania stacjami i użytkownikami sieci. Każdy użytkownik sieci powinien posiadać własny identyfikator i hasło, którego zmianę wymusza system zarządzania siecią. Dla ewentualnych użytkowników korzystających z tych samych stacji roboczych wprowadza się mechanizm identyfikacji i autoryzacji. Wprowadza się powszechny system kontroli antywirusowej – zarządzany centralnie. Dostęp do danych w zbiorach danych osobowych przez użytkowników systemów możliwy jest wyłącznie za pośrednictwem aplikacji służących do przetwarzania tych zbiorów. W przypadku dłuższej nieaktywności użytkownika wprowadza się mechanizm blokady stacji roboczych.

10.7. Identyfikator użytkownika wprowadzającego dane oraz data wykonania operacji na danych są automatycznie rejestrowane. Wprowadza się różne poziomy uprawnień dostępu do danych. Wykonanie czynności administracyjnych na bazach danych jest możliwe wyłącznie z konsoli administracyjnej serwerów, a nie z poziomu stacji klienckich. Operacje wykonywane na danych mają charakter transakcyjny. Informacja o transakcjach wykonywanych na danych zapisywana jest na logach transakcyjnych.

10.8. Mechanizm zabezpieczania i uwierzytelniania użytkowników oraz procedury postępowania zostały szczegółowo opisane w Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji.

10.9. W sytuacji przetwarzania danych osobowych, przez pracowników na komputerach przenośnych lub dokumentach papierowych poza obszarem przetwarzania danych osobowych, są oni zobowiązani chronić nośnik oraz dane przed utratą i dostępem osób nieuprawnionych. W tym do dodatkowego zabezpieczenia hasłem plików lub folderów zawierających dane osobowe.

10.10. Głównym sposobem pracy w oparciu o dane osobowe przetwarzane w systemie informatycznym jest odmiejscowienie dostępu do zasobów.

10.11. Dokumenty papierowe zawierające dane osobowe powinny być chronione przed dostępem osób nieuprawnionych podczas ich przetwarzania. Dokumenty papierowe z danymi osobowymi, w czasie nieobecności w pomieszczeniu osoby upoważnionej do przetwarzania danych osobowych, muszą być przechowywane w zamykanych na klucz sprzętach biurowych.

10.12. Dokumenty lub nośniki danych zawierające dane osobowe powinny być komisyjnie archiwizowane lub niszczone w sposób gwarantujący brak możliwości odczytania danych osobowych zawartych w dokumentach lub nośnikach elektronicznych.

10.13. Monitorowanie ochrony danych osobowych powinno być prowadzone na bieżąco przez pracowników, podczas audytów wewnętrznych oraz w innej formie określonej przez Właściciel, osobę kierującą obszarem informatyki.

10.14. Nadzór nad właściwym funkcjonowaniem systemu informatycznego, w którym przetwarzane są dane osobowe prowadzony jest przez osobę kierującą obszarem informatyki w firmie lub ASI. W przypadku wystąpienia nieprawidłowości ASI niezwłocznie informuje osobę kierującą obszarem informatyki w firmie, który uruchamia działania zmierzające do usunięcia nieprawidłowości,

11. ODPOWIEDZIALNOŚĆ DYSCYPLINARNA I KARNA

Za naruszenie wymogów niniejszej Polityki pracownik podlega odpowiedzialności dyscyplinarnej.

Niezależnie od tego, zgodnie z ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych, naruszenie jej przepisów jest zagrożone odpowiedzialnością karną i odpowiedzialnością administracyjną.

12. UWAGI KOŃCOWE

12.1. Wątpliwości, dotyczące interpretacji lub zastosowania przepisów Polityki wyjaśnia Właściciel lub wyznaczony przez niego pracownik.

12.2. Tekst Polityki powinien zostać udostępniony użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia. Jednocześnie tekst Polityki stanowi tajemnicę Przetwarzającego w rozumieniu tajemnicy przedsiębiorstwa zgodnie z ustawą z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji.

13. AKTY PRAWNE I DOKUMENTY ZWIĄZANE

13.1. Konstytucja Rzeczypospolitej Polskiej.

13.2. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku, Nr 101, poz. 926 ze zm.).

13.3. Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204 ze zm.).

13.4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. Nr 100, poz. 1024).

13.5. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 r., poz. 719),

13.6. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r., poz. 745).

Załącznik Nr 1 – Instrukcja zarządzania systemem informatycznym.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją Zarządzania" wprowadza się w oparciu o wymogi bezpieczeństwa informacji określone w rozporządzeniu 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. Nr 100, poz. 1024).

System, na którym pracują użytkownicy, jest zbiorem samodzielnych lub połączonych zależnościami podsystemów informatycznych, w których ma miejsce przetwarzanie danych osobowych.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

- 1

- Użytkownikowi zostaje przyznany unikalny w konkretnym podsystemie identyfikator wraz z poufnym hasłem, który proponuje Administrator Informacji występując z wnioskiem o przyznanie użytkownikowi uprawnień do przetwarzania danych w podsystemie. Hasło wymaga uzgodnienia z Administratorem.
- O przyznaniu identyfikatora decyduje Administrator Danych, co jest tożsame z przyznaniem użytkownikowi prawa do przetwarzania danych osobowych w systemie informatycznym.
- Identyfikator wraz z prawidłowym hasłem umożliwia użytkownikowi dostęp do podsystemu przetwarzania danych osobowych.
- Każdy z użytkowników przed dopuszczeniem do podsystemu podpisuje klauzulę o ochronie danych osobowych, zapoznaje się z Instrukcją Zarządzania i Polityką Bezpieczeństwa oraz zostaje pouczony o wdrożonych procedurach bezpieczeństwa.
- Administratorowi przysługuje prawo do zablokowania konta użytkownika w każdym czasie.
- Po zakończeniu operacji w systemie informatycznym, użytkownik zobowiązany jest wylogować się z podsystemu.
- W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych – każdy użytkownik zobowiązany jest do niezwłocznego powiadomienia Administratora Danych lub Administratora.
- Użytkownikom przyznaje się równe uprawnienia w dostępie do podsystemu (poziom podstawowy) chyba, że specyfika systemu wymaga innego podejścia.
- Administratorowi przysługuje prawo dostępu do podsystemu na poziomie wyższym (Administratora Systemu).

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

- 2

- Użytkownicy którym przyznano dostęp do podsystemu przetwarzania danych osobowych
  (w tym identyfikator dostępu do systemu) ustalają hasło dostępu z Administratorem.
- Hasło jest informacją o poufnym charakterze i należy zachować je w tajemnicy.
- Obowiązuje ścisły zakaz ujawniania hasła osobom trzecim, w tym innym użytkownikom.
- Hasła do wszystkich podsystemów użytkowanych w Zakładzie/Dziale należy przechowywać
  w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem lub w zabezpieczonym pliku.
- Osobą odpowiedzialną za bezpieczne przechowywanie listy identyfikatorów wraz z hasłami wymienionymi w pkt. 4 jest Administrator Informacji.
- Dostęp do listy identyfikatorów i haseł użytkowników wszystkich podsystemów użytkowanych w Zakładzie/Dziale posiada Administrator Informacji. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie Administratorowi Informacji lub bezpośrednio Administratorowi, który ustali nowe hasło.

- 3

- Hasło składa się z ciągu co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
- Hasła są różne dla każdego z użytkowników.
- Hasła są przechowywane w podsystemie w postaci zaszyfrowanej.
- Para „identyfikator i hasło” przyznane jednemu użytkownikowi nie może zostać powtórnie wykorzystane.
- Hasła są zmieniane nie rzadziej niż co 30 dni.
- System wymusza zmianę hasła.
- Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej.
- Jeżeli system informatyczny środkami technicznymi nie wymusza podjęcia czynności określonych w pkt 1-6, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i ustanowieniu nowego, spełniającego wymogi określone w niniejszym paragrafie.

- 4

Osobą odpowiedzialną za ustalanie poprawności haseł jest Administrator. Jeśli użytkownik podsystemu odpowiedzialny za zmianę hasła nie jest pewien jego poprawności, zobowiązany jest do konsultacji z osobą odpowiedzialną za ustalanie poprawności bezpiecznych haseł.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

- 5

- W celu uruchomienia podsystemu informatycznego użytkownik powinien:

- uruchomić komputer,
- wybrać odpowiednią opcję umożliwiającą logowanie do podsystemu,
- zalogować się do podsystemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.

- Użytkownik podczas logowania do podsystemu nie może ujawniać hasła osobom trzecim, w tym innym administratorom oraz pozostawiać zapisanego hasła w pobliżu stanowiska pracy i innych pracowników.
- Użytkownik zobligowany jest do skutecznego wylogowania się z podsystemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego na jak długo ma zamiar odejść od komputera.
- Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.
- Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych.
- W przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu, użytkownik niezwłocznie zawiadamia o zaistniałym fakcie Administratora Informacji lub bezpośrednio Administratora.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

- 6

- Kopie zapasowe zbiorów danych osobowych tworzone są codziennie po zakończonym dniu pracy ze zbiorem, chyba że danego dnia nie dokonano żadnych zmian w zbiorze.
- Za tworzenie kopii zapasowych odpowiedzialny jest Opiekun Zbioru.
- Opiekun Zbioru dokonuje zapisu kopii zbiorów danych osobowych na nośnikach CD, DVD, Pendrive lub innych nośnikach informacji przynajmniej co 14 dni lub częściej jeśli zmian na zbiorze jest dostatecznie wiele lub gdy uważa to za stosowne.
- Opiekun Zbioru oznacza i przechowuje kopie zbiorów danych w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
- Poprawność procesu tworzenia i przechowywania kopii zapasowych – nadzoruje Administrator Informacji.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

- 7

- Elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamkniętych szafkach z zabezpieczeniem dostępu osób trzecich lub serwerach spełniających wymagania RODO.
- Kopie bezpieczeństwa są niezwłocznie zniszczone po ustaniu użyteczności danych osobowych tam zawartych.
- Zniszczenia kopii dokonuje się w sposób uniemożliwiający późniejsze odtworzenie danych, poprzez fizyczne zniszczenie nośników danych lub jeśli to niemożliwe, poprzez trwałe usunięcie danych przy pomocy specjalistycznego oprogramowania służącego do tego celu. W przypadku wątpliwości, należy zwrócić się do Administratora.

- Fakt zniszczenia kopii zapasowych wymaga sporządzenia na tę okoliczność protokołu opatrzonego podpisem Administratora i osoby sporządzającej ten dokument.
- Kopie zapasowe przechowuje się przez okres 2 lat o ile przepisy nie stanowią inaczej, lub gdy użyteczność danych osobowych ustała przed upływem 2 lat licząc od dnia utworzenia kopii zapasowej, na której te dane są utrwalone.

- 8

- System informatyczny jest zabezpieczony przed atakami z zewnątrz sieci za pomocą oprogramowania typu firewall. Dodatkowo na serwerze pocztowym program antywirusowy chroni system przed przedostaniem się do wewnątrz sieci złośliwego oprogramowania.
- Komponenty serwerowe chronione są przed zakłóceniami w sieci zasilającej przy pomocy urządzeń typu UPS, podtrzymujących zasilanie.
- Każdy podsystem w którym ma miejsce przetwarzanie danych osobowych, podlega ochronie przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym aktualizowanym na bieżąco.
- W celu przeciwdziałania atakom zainfekowanych plików, podsystem musi być skanowany przynajmniej raz dziennie pod kątem obecności w systemie wirusów i innych zagrożeń. Za proces ten odpowiedzialny jest Opiekun Zbioru.
- W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadamia Administratora.
- Wszystkie komputery, na których uruchomione są podsystemy przetwarzające dane osobowe muszą być zaopatrzone w urządzenia typu UPS, podtrzymujące zasilanie, a tym samym zabezpieczające podsystem przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
- W przypadku stwierdzenia braku zasilania należy dokonać natychmiastowego zapisu danych osobowych oraz przeprowadzić procedurę opuszczenia podsystemu.

- 9

- Podsystemy informatyczne nie służące do przetwarzania danych osobowych, a ograniczone wyłącznie do edycji tekstu w celu udostępnienia go na piśmie, zapewniają odnotowanie:

- informacji o odbiorcach, którym dane osobowe zostały udostępnione,
- dacie i zakresie tego udostępnienia.

- Odnotowanie następuje przez automatyczny zapisek okoliczności w podsystemie.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

- 10

- Przeglądów oraz konserwacji systemu dokonuje Administrator.
- W przypadku przekazania innym podmiotom elementów systemu w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte. Proces ten nadzoruje Administrator.
- Dane osobowe muszą być zabezpieczone przed dostępem osób trzecich zanim nośnik lub element systemu zostanie przekazany podmiotowi innemu niż Administrator Informacji.

Uwagi końcowe

- 11

- Dopuszcza się możliwość wprowadzania w Instrukcji Zarządzania procedur uzupełniających, jeśli wymagać będzie tego specyfika komórki organizacyjnej.

Zmiany i udostępnienie tekstu Instrukcji Zarządzania

- 12

- Dopuszcza się możliwość dokonywania zmian w Instrukcji Zarządzania.
- Tekst Instrukcji Zarządzania jest udostępniany użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia.

……

Administrator Danych

Załącznik Nr 3 – Struktura zbiorów danych osobowych.

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

- Imię
- Nazwisko,
- Telefon kontaktowy
- Adres poczty elektronicznej
- Data urodzenia
- PESEL
- NIP
- Numer konta
- Adres zamieszkania /ulica, numer lokalu, miejscowość/

- Adres do korespondencji /ulica, numer lokalu, miejscowość/
- Miejsce pracy /ulica, numer lokalu, miejscowość/