Załącznik nr 1

do Zarządzenia z dnia 18 maja 2018 roku

POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

FURMIS Tomasz Furmański

ul. Wojska Polskiego 9BA

39-300 Mielec

NIP: 8171139909

REGON: 831308401

WYŁĄCZNIE DO UŻYTKU WEWNĘTRZNEGO

SPIS TREŚCI

WSTĘP

Tworzy się niniejszą dokumentację przetwarzania danych osobowych celem realizacji obowiązków wynikających z powszechnie obowiązującego prawa, tj. art. 36 ust. 2 ustawy z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015. poz. 2135) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024)., a także 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)polegających na wdrożeniu przez administratora danych dokumentacji przetwarzania danych osobowych.

Celem wdrożenia niniejszej dokumentacji jest zapewnienie należytej ochrony danych osobowych będących w zasobach administratora danych, w szczególności odpowiedniej do zagrożeń i kategorii danych osobowych objętych ochroną.

Poprzez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.

Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie zbiory danych osobowych przetwarzane przez administratora danych, zarówno w formie elektronicznej, jak i papierowej, oraz dane osobowe przetwarzane poza zbiorami danych.

Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby, przy pomocy, których administrator danych wykonuje swoje czynności, mające dostęp do danych osobowych.

Dodatkowo, tworzy się Regulamin ochrony danych, jako wyciąg najważniejszych zasad i procedur bezpieczeństwa obowiązujący wszystkie osoby przetwarzające dane osobowe.

DEFINICJE

§1

Użyte w niniejszej dokumentacji przetwarzania danych osobowych definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą dokumentacją oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych. Ilekroć w niniejszej polityce bezpieczeństwa jest mowa o:

1. Inspektorze ochrony danych osobowych (lub „IODO") – rozumie się przez to osobę wyznaczoną przez Administratora, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami obowiązującego prawa. Wzór zarządzenia powołującej IODO stanowi Załącznik „zarządzenie właściciela firmy.doc" do niniejszej dokumentacji;
2. Administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych. W niniejszej dokumentacji przetwarzania danych osobowych przez Administratora danych rozumie się Właściciela marek furmis.pl, fratelli.pl, haftem.pl - Tomasza Furmańskiego, dalej zwaną „Administratorem";
3. Administratorze systemów informatycznych (lub „ASI") – rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy teleinformatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane ustawą i rozporządzeniem. Wzór powołania ASI stanowi Załącznik „zarządzenie właściciela firmy.doc" do niniejszej dokumentacji;
4. Danych osobowych (lub „dane") – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5. Dokumentacji przetwarzania danych osobowych – rozumie się przez to politykę bezpieczeństwa przetwarzania danych osobowych i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
6. Prezesie Urzędu Ochrony Danych Osobowych (PUODO). – Rozumie się przez to organ ochrony danych osobowych;
7. Identyfikatorze (loginie) użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8. Osobie fizycznej możliwej do zidentyfikowania – jest to osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
9. Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora upoważnienie do przetwarzania danych;
10. Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;
11. Rozporządzeniu – rozumie się przez to 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)

12. Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
13. Ustawie – rozumie się przez to ustawę z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015. poz. 2135);
14. Użytkownik uprzywilejowany – należy przez to rozumieć osobę upoważnioną, posiadającą nadane uprawnienia na poziomie administratora systemu informatycznego;
15. Użytkowniku systemu – rozumie się przez to osobę upoważnioną, która otrzymała dostęp do sieci LAN umożliwiający korzystanie z sieci Internet oraz login i hasło do systemu;
16. Załącznikach – należy przez to rozumieć wzory dokumentów; Administrator może przedmiotowe wzory zastąpić wydrukami z systemów komputerowych lub innymi dokumentami o treści zgodnej z przepisami powszechnie obowiązującego prawa;
17. Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§2

1. W celu zapewnienia ochrony przetwarzanych danych osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej Administrator wdraża niniejszą politykę bezpieczeństwa.
2. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była rozliczalność, integralność i poufność danych, gdzie przez:
   1) rozliczalność - rozumie się właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   2) integralność danych - rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) poufność danych - rozumie się właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.
3. Administrator deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a także prawidłowego zabezpieczenia systemu teleinformatycznego służącego do przetwarzania danych osobowych.
4. Administrator nadzoruje jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane.
5. Administrator na bieżąco dostosowuje systemy informatyczne służące do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w rozporządzeniu.

§3

Wszelkie czynności, jakie na mocy niniejszej polityki bezpieczeństwa są wykonywane przez IODO lub ASI mogą być także wykonywane przez Administratora, z tym, że w przypadku niepowołania IODO Administrator nie ma obowiązku prowadzenia rejestru zbiorów danych osobowych, przygotowywania planu sprawdzeń ani opracowania sprawozdania ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

§4

1. Polityka bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody Administratora.
2. Dla codziennych potrzeb pracowników i współpracowników tworzy się Regulamin ochrony danych osobowych zawierający zasady przetwarzania danych osobowych obowiązujące u Administratora.
3. Regulamin jest jawny i udostępniany w sposób powszechnie przyjęty u Administratora wszystkim pracownikom i współpracownikom.

ADMINISTRATOR

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§5

1. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed: ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną.
2. Administrator w szczególności zapewnia:
   1) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
   2) system i sprzęt informatyczny umożliwiający bezpieczne przetwarzanie danych;
   3) że do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych;
   4) zapoznanie z przepisami o ochronie danych osobowych każdej osoby upoważnionej do przetwarzania danych osobowych;
   5) prowadzenie ewidencji osób upoważnionych;
   6) należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji w trybie art. 33 Ustawy;
   7) kontrolę nad tym, jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, ze zbiorów usunięte oraz komu i przez kogo przekazane.

§6

1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.
2. Administrator jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§7

1. Administrator może wyznaczyć Inspektora ochrony danych osobowych, który jest odpowiedzialny za przetwarzanie danych zgodnie z ustawą oraz rozporządzeniem.
2. Administrator może wyznaczyć, co najmniej jednego zastępcę IODO. Zastępca IODO musi spełniać wszystkie określone w rozporządzeniu wymagania
3. Zastępca IODO wykonuje wszystkie obowiązki należące do zakresu obowiązków IODO podczas jego nieobecności.

§8

1. W przypadku wyznaczenia IODO do zadań IODO należy:
   1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
      a) nie rzadziej niż raz w roku sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora;
      b) nadzorowanie opracowania i aktualizowania dokumentacji, ochrony danych osobowych oraz kontroli przestrzegania zasad w niej określonych;
      c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych i kierowanie osób do udziału w szkoleniach.
   2) Nadzorowanie rejestru zbiorów danych prowadzonych i przetwarzanych przez Administratora, z wyjątkiem zbiorów, wskazanych w jako zwolnione z obowiązku rejestracji, zawierającego w szczególności nazwę zbioru oraz spełniającego inne kryteria prawem przewidziane.
2. w celu sprawnej realizacji nałożonych zadań, IODO przysługują uprawnienia określone w rozporządzeniu.

§9

1. Inspektorem ochrony danych osobowych może być osoba, która:
   1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
   2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
   3) nie była karana za umyślne przestępstwo.
2. W dokumencie powołującym IODO osoba powołana do pełnienia funkcji IODO musi być wskazana z imienia i nazwiska.
3. Inspektor ochrony danych osobowych podlega bezpośrednio osobie fizycznej będącej Administratorem;
4. Administrator zapewnia środki i organizacyjną odrębność IODO niezbędne do niezależnego wykonywania przez niego zadań.

§10

1. Administrator może wyznaczyć Administratora Systemów Informatycznych.
2. ASI odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. ASI podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio Administratorowi.
4. W przypadku niewyznaczenia ASI za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych odpowiada Administrator.

PRZETWARZANIE DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI, osoby upoważnione.

§11

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
   1) osoba, której dane dotyczą wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych;
   2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
   3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
   4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
   5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektroniczne należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422) oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243), które przewidują dalej idącą ochronę.

§12

1. Zgoda na przetwarzanie danych osobowych, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
2. Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
3. Zgoda na przetwarzanie danych osobowych może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator obowiązany jest usunąć wszystkie dane osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie.
4. Zgody należy odbierać w postaci możliwej do późniejszego udowodnienia, najlepiej pisemnie lub:
   - w ramach systemu informatycznego po zastosowaniu metody dwustopniowego uwiarygodniania,
   - jako nagranie przeprowadzonej rozmowy telefonicznej - po poinformowaniu rozmówcy o prowadzonej rejestracji

   - rejestru odbiorców wysłanych wiadomości

   - potwierdzenia przesłania wiadomości drogą teleinformatyczną

§13

1. W przypadku powzięcia jakichkolwiek wątpliwości, co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IODO z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez IODO odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotycz należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

POWIERZENIE PRZETWARZANIA DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§14

1. Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
2. Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.
3. Podmiot, któremu powierzono przetwarzanie danych obowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające przetwarzanie danych, o których mowa w ustawie oraz w rozporządzeniu.
4. Wzór umowy powierzenia stanowi załącznik „Umowa powierzenia” do polityki bezpieczeństwa.

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

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§15

1. Administrator prowadzi wykaz zbiorów danych osobowych, które posiada.
2. Przy opisie każdego ze zbiorów wskazuje się programy zastosowane do przetwarzania danych.
3. Zbiory danych osobowych posiadane przez Administratora wraz z programami zastosowanymi do przetwarzania zawartych w nich danych wymienione zostały w załączniku „Wykazy - obszary, zbiory i przepływy" do polityki bezpieczeństwa.

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA POMIĘDZY NIMI

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§16

Struktura zbiorów danych osobowych wraz ze wskazaniem poszczególnych pól informacyjnych i powiązania pomiędzy nimi wskazane zostały w załączniku „Wykazy - obszary, zbiory i przepływy" do polityki bezpieczeństwa.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§17

Sposób przepływu danych pomiędzy poszczególnymi systemami wskazany został w załączniku „Wykazy - obszary, zbiory i przepływy" do polityki bezpieczeństwa.

PLAN SPRAWDZEŃ ORAZ DOKONYWANIE SPRAWDZEŃ

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§18

1. Inspektor ochrony danych osobowych, sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdanie w tym zakresie.
2. Sprawdzenie jest dokonywane dla Administratora lub Prezesa Urzędu Ochrony Danych osobowych. Sprawdzenie może być doraźne, planowe lub na żądanie PUODO.

§19

1. IODO zawiadamia Administratora o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia na żądanie PUODO przed podjęciem pierwszej czynności.
2. Administrator zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o możliwości przeprowadzenia czynności przez IODO.
3. Zawiadomienia nie przekazuje się w przypadku:
   1) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;
   2) sprawdzenia, o którego dokonanie zwrócił się PUODO, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin;
   3) jeżeli kierownik jednostki organizacyjnej objętej sprawdzeniem posiada informacje, o zakresie planowanych czynności.
4. Jeżeli IODO nie został wyznaczony Administrator nie ma obowiązku tworzenia planu sprawdzeń ani przygotowywania sprawozdania ze sprawdzenia.

§20

1. IODO przygotowuje plan sprawdzenia planowego.
2. Plan sprawdzeń zawiera przedmiot, zakres, termin sprawdzeń oraz sposób i zakres ich dokumentowania.
3. Plan sprawdzeń przygotowywany jest na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany Administratorowi nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje, co najmniej jedno sprawdzenie.
4. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych podlegają sprawdzeniu nie rzadziej niż raz na pięć lat.

§21

1. Po zakończeniu sprawdzenia IODO przygotowuje sprawozdanie.
2. Sprawozdanie jest sporządzane w postaci elektronicznej i przekazywane w postaci papierowej.
3. Inspektor Ochrony Danych Osobowych przekazuje Administratorowi sprawozdanie:
   1) ze sprawdzenia planowego - nie później niż w terminie 30 dni od zakończenia sprawdzenia;
   2) ze sprawdzenia doraźnego - niezwłocznie po zakończeniu sprawdzenia;

3) ze sprawdzenia, o którego dokonanie zwrócił się PUODO - zachowując termin wskazany przez Prezesa Urzędu.

REJESTR ZBIORÓW DANYCH OSOBOWYCH PROWADZONY PRZEZ INSPEKTORA OCHRONY DANYCH OSOBOWYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§22

1. IODO prowadzi rejestr zbiorów danych przetwarzanych przez Administratora.
2. W rejestrze nie ujawnia się zbiorów danych osobowych podlegających wyłączeniu od obowiązku rejestracji, zgodnie z art. 43 Ustawy.
3. Rejestr jest jawny, każdy ma prawo do przeglądania rejestru.
4. Wzór rejestru stanowi załącznik „Rejestr zbiorów danych osobowych" do niniejszej polityki bezpieczeństwa.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§23

1. Administrator obowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona.
2. Upoważnienie powinno zwierać w szczególności:
   1) Imię i nazwisko osoby upoważnionej
   2) datę z którą zostało nadane;
   3) datę z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony;
   4) zakres upoważnienia.
3. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.
4. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba, że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.
5. Wzór upoważnienia do przetwarzania danych stanowi załącznik „Upoważnienie i oświadczenie" do niniejszej polityki bezpieczeństwa.

EWIDENCJA OSÓB UPOWAŻNIONYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§24

1. Administrator obowiązany jest do prowadzenia ewidencji osób upoważnionych.
2. Ewidencja jest prowadzona w wersji papierowej.
3. Ewidencja zawiera:
   1) imię i nazwisko osoby upoważnionej;
   2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
   3) Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
4. Wzór ewidencji stanowi załącznik „Ewidencja osób upoważnionych”.

SZKOLENIA

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§25

1. Administrator organizuje szkolenie dla osób upoważnionych do przetwarzania danych osobowych w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych.
2. Szkolenie w miarę możliwości jest przeprowadzane przed dopuszczeniem osoby upoważnionej do czynności przetwarzania danych oraz przed nadaniem upoważnienia.
3. Szkolenia prowadzi Administrator, IODO lub osoba posiadająca wiadomości specjalne z zakresu ochrony danych.
4. Przeprowadzenie szkolenia musi być dokumentowane stosownymi zaświadczeniami.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI.
Do wiadomości: Osoby upoważnione.

§26

1. Administrator przetwarza dane jedynie w pomieszczeniach do tego przeznaczonych w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.

2. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe zawarty został w załączniku „Wykazy - obszary, zbiory i przepływy" do polityki bezpieczeństwa.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH ORGANIZACYJNYCH NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI, osoby upoważnione.

§27

1. Każdy, kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe, do których posiada dostęp, sposoby zabezpieczania danych jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.
4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.

§28

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba, która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność Administratorowi i IODO.
4. Administrator podejmuje wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.
5. Administrator reguluje przepływ danych wśród osób upoważnionych.
6. Szczegółowy wykaz środków technicznych i organizacyjnych stosowanych przez Administratora celem zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zawarty został w załączniku „Wykazy - obszary, zbiory i przepływy" do polityki bezpieczeństwa.

§29

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.

2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia (zaleca się, aby niszczarka spełniała wymogi normy DIN 66399, klasa bezpieczeństwa nie niższa niż 3) lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie w sposób ustalony w niniejszym dokumencie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.
6. Szczegółowy opis środków bezpieczeństwa zastosowanych przez Administratora wskazany został w załączniku „Wykazy - obszary, zbiory i przepływy" do polityki bezpieczeństwa.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, IODO, ASI, osoby upoważnione.

§30

1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić IODO.
2. W przypadku opisanym w ust. 1 IODO przeprowadza sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.
3. Przy dokonywaniu sprawdzenia IODO przysługują uprawnienia wskazane w rozporządzeniu w szczególności IODO przysługuje prawo:
   1) utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
   2) odebrania wyjaśnień osoby, której czynności objęto sprawdzeniem;
   3) sporządzeniu kopii otrzymanego dokumentu;
   4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych
   5) dokonywania dokumentacji fotograficznej

POSTANOWIENIA KOŃCOWE

§31

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.
2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany Dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.
3. Każdy, kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Dokumentacji przetwarzania danych osobowych.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą, jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
5. W sprawach nieuregulowanych w niniejszej polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy o ochronie danych osobowych.

ADMINISTRATOR DANYCH OSOBOWYCH:

Imię i nazwisko: **Tomasz Furmański**

Adres e-mail: furmis@furmis.pl

Telefon komórkowy: +48 731 502 502

Administrator systemu informatycznego:

Imię i nazwisko: **Bogusław Bańka**

Adres e-mail: bogdan@furmis.pl

Telefon komórkowy: 666 313 919

Inspektor ochrony danych osobowych:

Imię i nazwisko: **Marcin Barbarzak**

Adres e-mail: barbarzak@bhpskorpion.pl

Telefon stacjonarny: 531217990

http://**furmis.pl**/pl/