P O L I T Y K A B E Z P I E C Z E Ń S T W A O C H R O N Y D A N Y C H

ZAKŁAD PRODUKCYJNO-USŁUGOWY „TONTOR” Tomasz Tontor

ul. Szczypiornicka 116-120

62-800 Kalisz

Kalisz 15.04.2018

WSTĘP

INFORMACJE OGÓLNE

Głównym celem wprowadzenia Polityki Ochrony Danych jest zapewnienie zgodności działania Administratora Danych z Ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi.

Dokument Polityki Ochrony Danych został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych :

1. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100, poz. 1024 z późn. zmianami)
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Rozporządzenie Ogólne o Danych Osobowych)
3. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych

WYJAŚNIENIA TERMINÓW UŻYWANYCH W DOKUMENTACH POLITYKI DANYCH OSOBOWYCH

ustawa – ustawa z dnia 10 maja 2018r. o ochronie danych osobowych , zwana dalej „Ustawą”,

dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

przetwarzanie danych – jakiekolwiek operacje wykonane na danych osobowych takie jak : zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,

Administrator Danych Osobowych – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W praktyce często stosowane jest określenie administratora danych osobowych jako ADO.
Inspektor Danych Osobowych – termin prawniczy, który w prawie polskim został wprowadzony przepisami ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych. Oznacza osobę nadzorującą z upoważnienia administratora danych osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną, zwanym dalej „IDO”

ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

Obszar przetwarzania danych obejmuje siedziby firmy ZPU TONTOR Sp. z o.o. tj.

- siedzibę główną firmy przy ul. Szczypiornickiej 116-120 w Kaliszu
- biura oddziału firmy :
  - ul. Warszawska 10 w Kaliszu
  - ul. Maratońska 111 w Łodzi
  - ul. Budowlanych 19 w Opolu
  - ul. Kliczkowska 60 w Świdnicy

Zbiory danych przetwarzane są w systemie informatycznym przez Zintegrowany System Informatyczny **enova365 ERP.** Enova365 ERP zbudowana jest z wielu modułów, które współpracują ze sobą w oparciu o jedną bazę danych tj. kadry i płace, księga handlowa, handel.
Każdy z modułów wykonuje pracę w wyspecjalizowanym obszarze. Moduły te składają się na system ERP. Elementy współdziałają ze sobą oraz z urządzeniami zewnętrznymi (m.in.: z drukarkami fiskalnymi, drukarkami etykiet, inwentaryzatorami).

Struktura danych wykorzystanych przez system enova365 ERP to :

Kartoteka pracowników : Imię Nazwisko, data i miejsce urodzenia, pesel, adres zamieszkania, wykształcenie, nr telefonu

Kartoteka klienta : Imię nazwisko, nazwa firmy, NIP, adres, imię i nazwisko osoby kontaktowej jej

nr. telefonu i adres e-mail.

Baza danych systemu znajduje się na serwerze. Serwer znajduje się w zamkniętym osobnym pomieszczeniu. Serwer posiada zainstalowanie oprogramowanie Windows Server Standard 2012 i wyposażony jest w zasilacz awaryjny. Serwer i komputery podłączone do niego pracują w środowisku domenowym, które zarządza uprawnieniami, użytkownikami. Każdy użytkownik ma dostęp do komputera dopiero po podaniu nazwy użytkownika i hasła. Użytkownicy znajdujący się poza siedzibą firmy mają dostęp do systemu enova365 poprzez zdalną konsolę lub stronę www, dostęp zabezpieczony jest hasłem. Na stacjach roboczych zainstalowane jest oprogramowanie Windows. Sieć pasywna wykonana jest w technologii w kategorii 5, wyposażona jest w urządzenia aktywne przełączniki

10/100/1000. Dostęp do Internetu realizowany poprzez router.
Systemy są zintegrowane i następuje pomiędzy nimi wymiana danych.

Zbiory danych przetwarzane są również w systemie informatycznym przez program kalkulacyjno - produkcyjny **WHokna**. Program wykorzystywany jest w szerokim pojęciu w sferze wycen, kalkulacji i optymalizacji produkcyjnej oraz magazynu. System na który oparty jest program WHokna w pełni komunikuje się innymi systemami przetwarzającymi dane osobowe.

Struktura danych wykorzystanych przez system WH OKNA to :
Kartoteka klienta : Imię nazwisko, nazwa firmy, NIP, adres, imię i nazwisko osoby kontaktowej, jej nr. telefonu lub adres e-mail.

Baza danych systemu WH OKNA znajduje się na serwerze znajdującym się w dziale produkcji do którego spływają dane od każdego przedstawiciela handlowego, który ma system zainstalowany na indywidualnie przypisanych do osoby laptopach zabezpieczanych hasłem dostępu.

Systemy informatyczne zabezpieczone są hasłami i dostęp do nich mają upoważnione osoby.

W firmie stosuje się następujące zabezpieczenia fizyczne wszystkich pomieszczeń objętych przetwarzaniem danych:

- pomieszczenie biura jest zamykane i wyposażone w szafy i biurka zamykane na klucz
- obiekty w Kaliszu objęte są całodobowym nadzorem lub monitoringiem wizyjnym

W biurze zastosowano następujące środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych :

- został wyznaczony Inspektor Ochrony Danych
- dane osobowe są przetwarzane przez osoby posiadające upoważnienie
- przeprowadzane są okresowe szkolenia z zakresu ochrony danych osobowych
- zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi
- zbiory danych osobowych w formie papierowej są przechowywane w zamkniętej szafie na klucz
- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarki dokumentów

- osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych i zostały obowiązane do zachowania ich w tajemnicy
- zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej, która to jest przechowywana w osobnej szafie zamykanej na klucz
- zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. antywirusy na kluczowych jednostkach
- zainstalowano wygaszacze ekranów stanowiskowych na których przewarzane są dane osobowe

Dostęp do danych przetwarzanych w postaci elektronicznej możliwy jest po wielostopniowym uwierzytelnieniu użytkownika :

- dostęp do systemu operacyjnego wymaga pełnego uwierzytelnieniami u każdego z użytkowników - login i hasło
- dostęp do systemów w których przetwarzane są dane osobowe wymaga pełnego uwierzytelnienia i każdego użytkownika - login i hasło

OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

INFORMACJE OGÓLNE

Administrator danych – Zakład Produkcyjno-Handlowy TONTOR Tomasz Tontor

Inspektor Danych Osobowych – Aneta Kubiak

ADMINISTRATOR DANYCH

Uprawnienia i obowiązki Zakład Produkcyjno-Handlowy TONTOR Tomasz Tontor jako Administratora Danych :

- Jest zobowiązany do zapewnienia, aby przetwarzanie danych odbywało się zgodnie z prawem, wdraża wszystkie niezbędne środki organizacyjne i techniczne. Środki te muszą być aktualizowane. Zgodnie z zasadą rozliczalności jest zobowiązany do wykazania, które podjęte przez niego działania służą temu celowi
- Ma obowiązek wprowadzenia polityki ochrony danych, jeśli jest to proporcjonalne do czynności przewarzania
- Jest zobowiązany do działania zgonie z zasadą ochrony danych w fazie projektowania i permanentnej ochrony danych , poprzez określenie środków ochrony danych organizacyjnych i technicznych na etapie określania celów przetwarzania oraz domyślne przetwarzanie tylko tych danych osobowych, które są niezbędne dla osiągniecia celu przetwarzania
- Ma obowiązek zgłaszania organowi nadzorczemu przypadków naruszeń ochrony danych i jednocześnie dokumentuje i wprowadza działania zaradcze, o fakcie naruszenia ma także obowiązek powiadomić podmiot danych
- Dokonuje analizy ryzyka dla danych osobowych i dokonuje wszystkich lokalizacji oraz procesów, w ramach których dochodzi do przetwarzania Danych Osobowych, w szczególności poprzez analizę głównych procesów składających się na działalność Firmy
- Dokonuje oceny skutków dla ochrony danych i w razie potrzeby konsultuje się z organem nadzorczym. Ocena ma miejsce, gdy dany rodzaj przetwarzania powoduje potencjalne ryzyko

naruszenia praw i wolności osób fizycznych, stwierdzenie czy takie ryzyko istnieje pozostaje po stronie administratora – zasada rozliczalności

- Powołuje inspektora danych, lub przeprowadza ocenę, że powołanie go nie jest konieczne, zapewnia mu odpowiedni status i niezależność wewnątrz organizacji

Inspektor Danych Osobowych (IDO)

Uprawnienia i obowiązki IDO

- zapewnienie przestrzegania przepisów o ochronie danych osobowych w szczególności poprzez :

  - sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych

  - nadzorowanie opracowania i aktualizacji dokumentacji, o której mowa w art. 36 ust. 2 praz przestrzeganie zasad w niej określonych

  - zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Ochrony Danych oraz Instrukcji zarządzania systemem informatycznym.

Istotą powierzenia jest uprawnienie administratora innego podmiotu do przetwarzania danych osobowych w jego imieniu w drodze umowy. Podmiot przetwarzający nie może przetwarzać danych dla własnych celów. Podmiot przetwarzający staje się odpowiedzialny za przetwarzanie danych obok administratora.

Administrator i podmiot przetwarzający zawierają ze sobą osobną umowę powierzenia przetwarzania danych lub umieszczają klauzulę o powierzeniu danych jako integralną część innej umowy

Upoważnienie do przetwarzania danych osobowych są nadawane przez Administratora Danych Osobowych – na wniosek IDO. Upoważnienie jest wystawiane w formie pisemnej w dwóch egzemplarzach oraz odnotowanie w systemie informatycznym w formie elektronicznej.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Rozporządzenie RODO wprowadza katalog 6 zasad, które zobowiązany jest przestrzegać ADO jak i każda osoba upoważniona w firmie do przetwarzania danych osobowych

- **zasada zgodności z prawem, rzetelności i przejrzystości** – przetwarzanie danych zgodnie z prawem, rzetelnie, w sposób przejrzysty dla osób których te dane dotyczą
- zasada ograniczonego celu – dane osobowe zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach, nieprzetwarzane dalej niezgodnie z tymi celami, dopuszczone jest dalsze przetwarzanie do celów archiwalnych w interesie publicznym, naukowych, historycznych lub statystycznych
- **zasada minimalizacji** – gromadzenie danych osobowych adekwatnie i stosownie do celów przetwarzania
- **zasada prawidłowości** – obowiązek czuwania nad prawidłowością i aktualnością danych, podjęcie wszelkich rozsądnych działań dla niezwłocznego usunięcia, bądź sprostowania danych nieprawidłowych
- **zasada ograniczenia przechowywanie** – dane osobowe przechowywane w formie umożliwiającej identyfikację osoby przechowywane przez okres nie dłuższy niż jest to niezbędne dla celów przetwarzania,
- **zasada integralności i poufności** – przetwarzanie danych w sposób zapewniający odpowiedni stopień bezpieczeństwa, ochronę przed niedozwolonym i niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem danych, za pomocą odpowiednich środków organizacyjnych i technicznych

PODSTAWY PRAWNE PRZETWARZANIA DANYCH

Aby przetwarzanie danych było legalne niezbędne jest spełnienie co najmniej jednego z sześciu warunków, którymi są :

- uzyskanie zgody na przetwarzanie danych od osoby, której dane dotyczą
- przetwarzanie danych jest niezbędne do wykonanie umowy, której stroną jest podmiot danych, podjęcie przez ADO działań na żądanie takiej osoby jeszcze przed zawarciem umowy
- przetwarzanie jest niezbędne do wykonania obowiązku prawnego ciążącego na ADO
- Przetwarzanie jest niezbędne do ochrony żywotnych interesów podmiotu danych, lub innej osoby fizycznej
- przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach władzy publicznej powierzonej ADO
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów ADO lub strony trzeciej, z wyjątkiem sytuacji, gdy charakter nadrzędny mają interesy osoby, której dane dotyczą, w szczególności gdy ta jest dzieckiem

PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

1. **Prawo do bycie poinformowanych o operacjach przetwarzania** – wymaga ono by ADO podał osobie, której dotyczą dane wszelkie informacje o przeprowadzaniu operacji przetwarzania i jej celach.

2. **Prawo dostępu do danych** – każda osoba fizyczna powinna mieć zapewniony dostęp do danych osobowych dotyczących tej osoby. Ma mieć świadomość przetwarzania i możliwość zweryfikowania legalności takiego przetwarzania.

3. **Prawo do sprostowania i uzupełnienia danych** – osoba której dane dotyczą ma prawo żądać od ADO sprostowania danych osobowych jej dotyczących, które są nieprawidłowe. Ma się to odbywać z uwzględnieniem celu, dla którego dane są przetwarzane

4. **Prawo do usunięcia danych** – podmioty danych mogą żądać od administratora niezwłocznego usunięcia danych dotyczących, natomiast ten ma obowiązek usunąć dane osobowe. Żądanie osoby, której dane dotyczą należy spełnić :

    - Kiedy dane nie są już potrzebne w związku z celem, dla którego zostały pierwotnie zebrane lub przetwarzane
    - W przypadku, gdy osoba fizyczna wycofa wyrażoną zgodę, a brak jest uzasadnienia przetwarzania
    - W przypadku przetwarzania opartego na prawnie uzasadnionym interesie – jeśli osoba wyrazi sprzeciw, a administrator danych nie będzie w stanie wykazać, że istnieją nadrzędne, ważne podstawy dla przetwarzania
    - W przypadku, gdy dane są w inny sposób przetwarzane niezgodnie z prawem
    - W przypadku, gdy dane muszą zostać usunięte na podstawie prawa unijnego lub krajowego, które ma zastosowanie do administratora danych

5. **Prawo bycia zapomnianym** – prawo osoby, której dotyczą do żądania usunięcia danych przez ADO, administrator, który upublicznił dane i do którego zostało skierowane żądanie ma obowiązek poinformowania kolejnych administratorów danych aby usunęli wszelkie łącza do tych danych, usunięciu mają także ulec dane z wszelkich kopiach danych

6. **Prawo do ograniczenia przetwarzania –** osoba, której dane dotyczą ma prawo żądania ograniczenia przetwarzania danych w przypadkach takich jak:

- Osoba, której dane dotyczą, kwestionuje prawidłowość jej danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych
- Osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania
- Dane potrzebne są do ustalenia, pochodzenia lub obrony roszczeń osoby, której one dotyczą, pomimo że administrator nie potrzebuje już tych danych osobowych do celów przetwarzania

7. **Prawo do przenoszenia danych -** dotyczy wyłącznie sytuacji, gdy przetwarzanie samych odbywa się na podstawie zgody podmiotu danych, w celu wykonania umowy. Istotą jest możliwość

otrzymania w ustrukturyzowanym powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych dostarczanych administratorowi, oraz przesyłania tych danych kolejnemu administratorowi

8. **Zakaz profilowania -** dotyczy sytuacji gdzie w oparciu o Pani/Pana dane osobowe Firma podejmuje wobec Pani/Pana decyzje w sposób automatyzowany, w tym decyzji będących wynikiem profilowania

UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH Z FIRMAMI ZEWNĘTRZNYMI

Umowy powierzenia przetwarzania danych osobowych wykonywane są przez następujące podmioty :

1. Zewnętrzna obsługa finansowo-ekonomiczna – Biuro ekonomiczno-finansowe Marian Borszyński, który korzysta ze zbiorów danych osobowych zawartych w systemie w celu sporządzania analiz finansowych i rachunku ekonomicznego firmy.
2. Zewnętrzna obsługa systemów informatycznych zarządzania przedsiębiorstwem enova365 – ARKomp Systemy Komputerowe Robert Dworczak, który korzysta ze zbiorów danych zawartych w systemie w celu prawidłowego funkcjonowania, aktualizowania systemów i nadzoru informatycznego
3. Zewnętrzna obsługa i administrowanie strony internetowej Firmy – MOVU – Przemysław Woźny, który korzysta ze zbiorów zatrudnionych pracowników w celu umieszczenia danych kontaktowych osób współpracujących z klientami na zewnątrz firmy.
4. Zewnętrzna służba BHP - Usługi BHP Andrzej Kordylas, która korzysta ze zbiorów zatrudnionych pracowników w celu przeprowadzenia szkoleń z zakresu BHP
5. Kancelaria Prawna - Three Consulting Group s.c. Janiak G., Lisok D. , która korzysta ze zbiorów klientów Administratora w celu prowadzenia spraw sadowych.

Wszelkie zidentyfikowane ryzyka związane z dostarczaniem usług przez stronę trzecią są monitorowane. Umowy ze stronami trzecimi, dotyczące udostępniania, przetwarzania i zarządzania informacjami Firmy zawierane są z uwzględnieniem niezbędnych wymogów bezpieczeństwa oraz w formule wymaganej przepisami RODO. Administrator Danych korzysta wyłącznie z usług takich podmiotów przetwarzających dane , które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymogi i chroniło prawa osób, których dane dotyczą.

ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Przetwarzanie danych osobowych zwłaszcza w sposób zautomatyzowany, w systemach informatycznych zwiększa niebezpieczeństwo naruszeń.

Przykłady zagrożeń i sposobów na ich uniknięcie :

- Ataki na przeglądarki internetowe – korzystanie z konta z wyłączonymi prawami administracyjnymi
- Ataki na pocztę elektroniczną – nieotwieranie podejrzanych załączników do wiadomości
- Spam – nieodpowiadanie na spam, odpowiedź jest potwierdzeniem, że adres poczty użytkownika jest poprawny

Najpopularniejsze środki bezpieczeństwa :

- Hasła – stosowanie silnych haseł – wielkie małe litery, cyfry, znaki specjalne, częsta zmiana haseł
- Programy antywirusowe – aktualizacja programów i baz danych wirusów
- Wykonywanie kopii zapasowych systemu umieszczona na innym nośniku niż dysk twardy komputera
- Korzystanie wyłącznie z bezpiecznych wtyczek i przeglądarek internetowych

Środki fizycznego zabezpieczenia danych :

- Zasada „czystego biurka”
- Blokowanie dostępu do urządzenia w razie oddalenia się ze stanowiska pracy
- Właściwe utylizowanie urządzeń będących nośnikami danych np. stosowanie niszczarki

ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH OBOWIĄZUJĄCE W FIRMIE

- W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka" Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym
- Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści np. z wykorzystaniem niszczarek
- Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
  Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonując ich wyniesienia oraj jej bezpośredni przełożony
- Przebywanie osób nieuprawnionych w pomieszczeniu , w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

Dane osobowe będą przechowywane do momentu przedawnienia roszczeń z tytułu umowy lub do momentu wygaśnięcia obowiązku przechowywania danych wynikających z przepisów prawa, w szczególności obowiązku przechowywania dokumentów księgowych dotyczących umowy.

W momencie przedawnienia dane zostaną zarchiwizowane na nośniku elektronicznym, bądź zniszczone na prośbę osoby, której przetwarzanie danych dotyczy.

W przypadku złożenia zgody na przetwarzanie danych osobowych w zakresie i w celu wskazanym w treści zgody, dane osobowe osoby , której przetwarzanie danych dotyczy są przetwarzane przez okres wskazany w złożonym oświadczeniu o zgodzie na przetwarzanie danych osobowych, przy czym nie dłużej niż do czasu odwołania zgody.

Dokumenty i nośniki zawierające informacje o wysokim poziomie wrażliwości oraz nośniki kopii zapasowych serwerów są przechowywane w serwerowni na osobnych nośnikach elektronicznych. Nośniki kopii archiwalnych są przechowywane w serwerowni.

Niszczenie nośników papierowych wykonane jest poprzez niszczenie ich w niszczarkach, jak i odbywa się za po średniactwem profesjonalnych usług firmy zewnętrznej, z zachowaniem zabezpieczeń związanych z ochroną poufności niszczonych informacji. Nośniki elektroniczne (tj. płyty CD/DVD, DYSKI TWARDE, TASMY) podlegają składowaniu w serwerowni, a następnie fizycznemu zniszczeniu za pomocą odpowiednich środków przez firmy zewnętrzne.

Serwerownia jest osobnym pomieszczeniem, zamykanym jest na klucz.

INSTRUKCJA POSTEPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

- Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić IDO
- Do czasu przybycia na miejsce naruszenia ochrony danych osobowych IDO lub upoważnionej przez niego osoby, osoba powiadamiająca powinna :

  - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe ,

  - zaniechać dalszych planowanych przedsięwzięć, które mogą utrudnić jego udokumentowanie i analizę,

  - udokumentować wstępnie zaistniałe naruszenie

  - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IDO lub osoby upoważnionej.

KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

- Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych sprawuje IDO – w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetworzenia danych osobowych
- Czynności kontrolne przeprowadzane są nie rzadziej niż raz w roku
- Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności
- Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u IDO

ZAŁĄCZNIKI

Załącznik nr 1 - Ustanowienie Inspektora Danych Osobowych

Załącznik nr 2 – Upoważnienie IDO do nadawania upoważnień

Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

Załącznik nr 4 – Wzór oświadczenia o zobowiązaniu do zachowania poufności

Załącznik nr 5 – Wzór ustanowienia Administratora Systemów Informatycznych

Załącznik nr 6 - Wzór protokołu z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Załącznik nr 7 – Wzór zgody na przetwarzanie danych w celu zrealizowania zlecenia na wykonanie usługi

Załącznik nr 1 - Ustanowienie Inspektora Danych Osobowych

Niniejszym, zgodnie z dyspozycją Rozdziału 2 Polityki Ochrony Danych oraz reprezentują Administratora Danych – *NAZWA I ADRES ADMINISTRATORA DANYCH*

wyznaczam

Panią/Pana ……..

na stanowisko Inspektora Danych Osobowych (IDO) w *NAZWA ADMINISTRATORA DANYCH*

Zakres obowiązków oraz warunki pełnienia funkcji Inspektora Danych Osobowych określone są w Ustawą z dnia maja 2018 roku o ochronie danych osobowych oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia …/…/…… (dd/mm/rrrr) w *NAZWA ADMINISTRATORA DANYCH*

…… (DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO IDO)

…….. (DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH)

Załącznik nr 2 – Upoważnienie IDO do nadawania upoważnień

Niniejszym, zgodnie z dyspozycją Polityki Ochrony Danych oraz reprezentując Administratora Danych - *NAZWA I ADRES ADMINISTRATORA DANYCH*

Upoważniam

Panią/Pana ……

Inspektora |Danych Osobowych w *NAZWA ADMINISTRATORA DANYCH* do nadawania w imieniu Administratora Danych upoważnień do przetwarzania danych osobowych.

…… (DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO IDO)

…… (DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH)

Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszy, jako Inspektor Danych Osobowych w *NAZWA ADMINISTRATORA DANYCH,* Na podstawie art. 7 Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. 2002r. Nr 101, poz. 926 ze zm.),

upoważniam

Imię i nazwisko upoważnionego pracownika : ……..

Zbiory danych objęte zakresem upoważnienia: ……..

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełniania obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz przepisami Ustawy z dnia 10 maja 2018r. o ochronie danych i obowiązującymi w *NAZWA ADMINISTRATORA DANYCH* wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę trybie art.52 Kodeksu Pracy.

Upoważnienie ważne jest do odwołania.

…… ……

data i podpis upoważniającego data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w *NAZWA ADMINISTRATORA DANYCH* (w szczególności z Polityką Ochrony Danych oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuje się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanych stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....
data i podpis osoby upoważnionej

Załącznik nr 4 – Wzór oświadczenia o zobowiązaniu do zachowania poufności

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja, niżej podpisany …….zamieszkały w ……..

……zatrudniona/y na stanowisku ……..

……zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z Przetwarzaniem danych osobowych

Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia jak i po jego ustaniu.

……
Podpis

Załącznik nr 5 – Wzór ustanowienia Administratora Systemów Informatycznych

Niniejszym, zgodnie z dyspozycja Rozdziału 2 Polityki Ochrony Danych oraz reprezentując Administratora Danych - *NAZWA I ADRES ADMINISTRATORA DANYCH*

wyznaczam

Panią/Pana …….

na stanowisko Administratora Systemów Informatycznych (ASI) w *NAZWA ADMINISTRATORA DANYCH*

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone Ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia …/…/……. (dd/mm/rrrr) w *NAZWA ADMINISTRATORA DANYCH*

…….	…….
(DATA I PODPIS OSOBY WYZNACZONEJ NA STANOWISKO IDO)	(DATA I PODPIS OSOBY REPREZENTUJĄCEJ ADMINISTRATORA DANYCH)

Załącznik nr 6 - Wzór protokołu z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

PROTOKÓŁ

Z KONTROLI /CZYNNOŚCI SPRAWDZAJACYCH

w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej : .....
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli : ……..
3. Data wykonania czynności kontrolnych : ……
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne :……
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej : ……..
6. Ustalenia dokonane w trakcie czynności kontrolnych :…….
7. Wnioski i zalecenia pokontrolne : ……

…….. ……..

data i podpis osoby wykonującej czynności kontrolujące data i podpis kierownika kontrolowanej kom. organizacyjnej

Załącznik nr 7 – Informacje dotyczące przetwarzania danych osobowych

(dla klienta)

Administratorem danych jest

ZAKŁAD PRODUKCYJNO USLUGOWY TONTOR TOMASZ TONTOR z siedzibą w Kaliszu przy ul. Szczypiornickiej 116-120

Z Administratorem danych można się skontaktować poprzez adres email : dane.osobowe@tontor.com lub pisemnie na adres siedziby administratora we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz z korzystania z praw związanych z przetwarzaniem danych.

ZPU TONTOR Tomasz Tontor przetwarza następujące kategorie danych osobowych : dane identyfikacyjne klientów tj. imię i nazwisko , dane adresowe, nr telefonu lub adres email

Pani/Pana dane mogą być przetwarzane w celu realizacji przez Administratora zadań ustawowych i umownych.

Przysługuje Pani/Panu prawo dostępu do Pani/Pana danych oraz prawo żądania ich sprostowania, ich usunięcia lub ograniczenia ich przetwarzania.

W zakresie, w jakim podstawą przetwarzania Państwa danych osobowych jest przesłanka prawnie uzasadnionego interesu administratora, przysługuje Pani/panu prawo wniesienia sprzeciwu wobec przetwarzania Pani/pana danych osobowych. W szczególności przysługuje Pani/Panu prawo sprzeciwu wobec przetwarzania danych na potrzeby marketingu bezpośredniego.

W zakresie w jakim podstawą przetwarzania Pani/Pana danych osobowych jest zgoda, ma Pani/Pan prawo wycofania zgody. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

W zakresie, w jakim Pani/Pana dane są przetwarzane w celu zawarcia i wykonywania umowy przysługuje Pani/Panu prawo do przenoszenia danych osobowych, tj. do otrzymania od administratora Pani/Pana danych osobowych, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Dane te można przesłać innemu administratorowi

W oparciu o Pani/Pana dane osobowe Firma nie podejmuje wobec Pani/Pana decyzji w sposób automatyzowany, w tym decyzji będących wynikiem profilowania

Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych

Pani/Pana dane osobowe będą przechowywane do momentu przedawnienia roszczeń z tytułu umowy lub do momentu wygaśnięcia obowiązku przechowywania danych wynikających z przepisów prawa, w szczególności obowiązku przechowywania dokumentów księgowych dotyczących umowy.

Podanie danych osobowych w związku z zawieraną umową jest dobrowolne, ale konieczne do zawarcia umowy i wykonania usługi. Brak podania danych osobowych jest jednoznaczny z rezygnacją podpisania umowy.

……	……
data i podpis klienta upoważniające do przetwarzania danych	data i podpis osoby upoważnionej do przetwarzania danych