POLITYKA BEZPIECZEŃSTWA INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

w

ARGENTA Marcin Dziopa

ul. Warszawska 229

25-551 Kielce

I. POSTANOWIENIA OGÓLNE

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych
w zakresie ochrony danych osobowych, sposobu przetwarzania w ARGENTA Marcin Dziopa grupy informacji zawierającej dane osobowe.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
2. przetwarzanie danych osobowych – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza
   w systemach informatycznych,
3. użytkownik – osoba upoważniona do przetwarzania danych osobowych,
4. administrator systemu – osoba upoważniona do zarządzania systemem informatycznym,
5. system informatyczny – system przetwarzania danych w ARGENTA Marcin Dziopa wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
6. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

1. Utrzymanie bezpieczeństwa przetwarzanych przez ARGENTA Marcin Dziopa informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

4) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
   3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

1. W systemie informacyjnym firmy przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

Politykę Bezpieczeństwa stosuje się do:

1. danych osobowych kontrahentów i klientów przetwarzanych w systemie informatycznym,
2. wszystkich informacji dotyczących danych pracowników ARGENTA Marcin Dziopa, w tym danych osobowych pracowników i treści zawieranych umów o pracę,
3. wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
4. innych dokumentów zawierających dane osobowe.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do całego systemu informacyjnego firmy w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów i innych osób, w tym zatrudnionych na umowy cywilnoprawne oraz pracowników biura rachunkowego obsługującego firmę, mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci oraz inne osoby mające dostęp do informacji podlegających ochronie w tym osoby zatrudnione na umowy cywilnoprawne oraz pracownicy biura rachunkowego obsługującego firmę.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa składa się z:
   1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
   2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w firmie - załącznik nr 1,
   3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia- załącznik nr 2.

V. DOSTĘP DO INFORMACJI

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w firmie zasad ochrony danych osobowych.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

Osoba dopuszczona do przetwarzania danych osobowych zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych.

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, możliwe jest jeżeli w sposób wiarygodny podmioty te uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

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 dokonująca ich.

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.

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.

Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.

Dane osobowe udostępnia się na umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

Administratorem danych osobowych jest **ARGENTA Marcin Dziopa, 25-551 Kielce, ul. Warszawska 229, NIP: 959-147-38-28, REGON: 260658554**.

Administratorem Bezpieczeństwa Informacji jest **właściciel Marcin Dziopa**.

Osobą upoważnioną do przetwarzania danych osobowych jest **Monika Rudnicka**. Podstawę stanowi upoważnienie do przetwarzania danych osobowych

Dane osobowe powierza się do przetwarzania, na podstawie umowy powierzenia:

- **QBILO Sp. z o.o. ul. Sikorskiego 24d, 25-548 Kielce, NIP: 657-29-18-357,**.

- **M.K. SEKURA Obsługa i Szkolenie BHP i PPOŻ Marek Kulczycki, 26-060 Chęciny, Wolica, ul. Armii Krajowej 53, NIP: 959-116-87-20**,

- **Prywatny Gabinet Lekarski, Kielce, ul. Poleska 3. Dr n. med. Tadeusz Dudek – specjalista medycyny pracy, NIP: 959-003-03-94.**

VII. ZAKRESY ODPOWIEDZIALNOŚCI

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik firmy.

Administrator Bezpieczeństwa Informacji w Jednostce:

1. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolę przebywających w nich osób,
2. określa strategię zabezpieczania systemów informatycznych firmy,
3. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
4. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,

5. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych firmy,
6. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
7. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
8. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
9. odpowiada za realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji, w szczególności poprzez:
    - określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
    - określenie pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
    - zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
    - wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,
    - wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
    - działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
    - stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
    - odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
    - określanie, które osoby i na jakich prawach mają dostęp do danych informacji.

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje, konfiguracje i administrację oprogramowania systemowego, sieciowego zabezpieczającą dane przed nieupoważnionym dostępem
5. współpracę z dostawcami usług oraz sprzętu sieciowego,
6. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
7. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
8. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
9. prowadzenie profilaktyki antywirusowej.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych następuje w wyznaczonym pomieszczeniu przez wyznaczone do tego celu osoby.
2. 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.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć
   w stopniu uniemożliwiającym ich odczytanie np. z wykorzystaniem niszczarek
4. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

IX. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

W Jednostce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   - zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi,
   - zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat,
   - dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych,
   - zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie,
   - monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonym pomieszczeniu,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:

- osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Bezpieczeństwa Informacji (ABI),
- Administrator Bezpieczeństwa Informacji na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,

4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:

- przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie,

- w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,

- przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,

- w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,

- po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

X. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

Archiwizacja informacji zawierających dane osobowe odbywa w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonym pomieszczeniu, które jest zabezpieczone przed dostępem osób nieupoważnionych.