Polityka bezpieczeństwa danych osobowych

„Polityka bezpieczeństwa danych osobowych” - zwana dalej „Polityką bezpieczeństwa” – przeznaczona jest dla osób przetwarzających dane osobowe w DRABEST Sp. z o.o. z siedzibą w Mnikowie – zwaną dalej „Spółką”
Polityka bezpieczeństwa opisuje reguły dotyczące bezpieczeństwa danych osobowych przetwarzanych w Spółce, w tym zawartych w jej systemach informatycznych, określa granice i zasady dopuszczalnego przetwarzania danych osobowych, zachowania osób dokonujących przetwarzania danych, wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, w tym w systemach informatycznych oraz konsekwencje, jakie mogą ponosić osoby przekraczające zasady przetwarzania danych osobowych oraz procedury postępowania w celu zapobiegania i minimalizowania skutków zagrożeń.

Podstawa prawna:
Polityka bezpieczeństwa została opracowana na podstawie przepisów:
- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
- ustawy z dnia 10 maja 2108r. o ochronie danych osobowych (Dz. U. z 2018r. poz. 1000)– zwanej dalej „ustawą o ochronie danych osobowych”,

§ 1
Słownik

Użyte w instrukcji określenia oznaczają:
1) **dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy;
2) **zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
3) **Administrator Danych Osobowych** – (zwany dalej „ADO”) DRABEST Sp. z o.o. z siedzibą w Mnikowie 281, 32-084 Morawica, wpisana do Krajowego Rejestru Sądowego pod nr KRS 0000282861, zwana dalej również „Spółką”;
4) **przetwarzanie danych** – operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, zarówno w systemach informatycznych, jaki i metodami tradycyjnymi (kartoteki, księgi, wykaz, itp);
5) **system informatyczny** –zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych przez ADO w celu przetwarzania danych;
6) **Administrator Systemu Informatycznego** – (zwany dalej „ASI”) informatyka lub osobę zajmującą się zarządzaniem całością lub wydzieloną częścią systemu informatycznego,

odpowiadający za jej sprawne działanie. Do zadań ASI należy nadzorowanie pracy serwerów, dodawanie i kasowanie kont ich użytkowników, konfiguracja komputerów, instalowanie oprogramowania, dbanie o bezpieczeństwo systemu informatycznego, nadzorowanie, eliminowanie nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalatorskich, konfiguracyjnych i naprawczych;

7) **użytkownik systemu informatycznego** – pracownik ADO lub inny podmiot przetwarzający posiadający odpowiednie upoważnienia;
8) **podmiot przetwarzający** – (zwany dalej „procesor") pracownika lub inną osobę, która przetwarza dane osobowe w imieniu ADO;
9) **kierownik komórki** – kierownik działu /wydziału lub innej komórki ADO, w której zatrudniony jest pracownik przetwarzający dane osobowe;
10) **odbiorcy danych** – rozumie się przez to każdy podmiot, któremu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- podmiotu lub osoby upoważnionej przez ADO lub procesora do przetwarzania danych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

11) **Inspektor Ochrony Danych Osobowych** – (zwany dalej „IODO") osoba wyznaczona przez ADO zgłoszona do Prezesa Urzędu Ochrony Danych Osobowych (zwanego dalej „PUODO"). Do obowiązków IODO należy w szczególności:
    - informowanie ADO, procesora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach związanych z ochroną danych osobowych i doradzanie im w tym zakresie;
    - monitorowanie przestrzegania przepisów o ochronie danych oraz polityk administratora lub procesora w zakresie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    - udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania;
    - współpraca z PUODO;
    - pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem danych osobowych oraz prowadzenie konsultacji w zakresie danych osobowych ;
12) **identyfikator użytkownika** – (zwany dalej „login") ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
13) **hasło** –ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
14) **autoryzacja** – proces, w którym sprawdzane jest czy dana osoba ma prawo dostępu do systemu informatycznego; odpowiednie uprawnienia są przypisane do konkretnej, zidentyfikowanej osoby, a autoryzacja jest zwykle poprzedzona uwierzytelnieniem (zidentyfikowaniem) osoby;
15) **uwierzytelnienie** – proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby, poprzez podanie odpowiedniego loginu i hasła;
16) **sieć publiczna** – sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004r. - Prawo telekomunikacyjne (Dz. U. z 2017r. poz. 1907 z późn. zm.);
17) **zapora ogniowa** – (ang. firewall – „ściana ogniowa") jeden ze sposobów zabezpieczania sieci i systemów informatycznych przed intruzami. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz tzn. sieci publicznych, Internetu oraz przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz;

§ 2
Zasady ogólne

1. Administratorem danych osobowych jest Drabest Sp. z o.o. Decyzje o celach, zasadach, sposobach i środkach przetwarzania danych osobowych podejmuje Prezes Zarządu Spółki, który wyznacza IODO. ASI w zakresie ochrony danych osobowych przetwarzanych przez systemy informatyczne ADO współpracuje z IODO.
2. Polityka bezpieczeństwa (zwana dalej „Polityką") określa zasady zabezpieczenia danych osobowych obowiązujące w ADO oraz tryb postępowania dla w przypadku, gdy stwierdzono naruszenie bezpieczeństwa danych osobowych.
3. Polityka bezpieczeństwa obowiązuje wszystkich pracowników ADO oraz wszystkie podmioty przetwarzające dane osobowe w jego imieniu, niezależnie od podstawy prawnej.
4. Wykonanie postanowień tego dokumentu ma zapewnić zachowanie poziomu bezpieczeństwa danych osobowych wynikającą z powszechnie obowiązujących przepisów w zakresie danych osobowych oraz właściwą reakcję, ocenę i udokumentowanie przypadków naruszania bezpieczeństwa danych, a także zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych przez ADO.
5. Polityka bezpieczeństwa zostało sporządzona na podstawie wyników przeprowadzonego przez ADO audytu przetwarzania danych osobowych.
6. Integralną cześć Polityki bezpieczeństwa stanowią następujące dokumenty:
   1) oświadczenie o wyznaczeniu IODO,
   2) ewidencja pomieszczeń tworzących obszar przetwarzania danych osobowych,
   3) rejestr czynności przetwarzania danych osobowych,
   4) opis struktury zbiorów danych osobowych,
   5) rejestr przypadków naruszenia bezpieczeństwa przetwarzania danych osobowych,
   6) rejestr osób upoważnionych do przetwarzania danych osobowych,
   7) rejestr podmiotów, którym powierzono przetwarzanie danych osobowych na podstawie umowy powierzenia przetwarzania,
   8) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   9) ewidencja korespondencji inspektora ochrony danych osobowych,
   10) polityka prywatności,
   11) wzory raportów IODO,
   12) klauzula informacyjna zamieszczana w stopce poczty elektronicznej i na fakturach,
   13) klauzula informacyjna o monitoringu,
   14) upoważnienie do przetwarzania danych osobowych,
   15) oświadczenie pracownika dotyczące przetwarzania danych osobowych i zachowania ich poufności,
   16) klauzula informacyjna dla pracowników,
   17) klauzula informacyjna na podstawie art. 14 RODO,
   18) umowa o powierzeniu przetwarzania danych osobowych,
   19) klauzula umowna informująca o przetwarzaniu danych osobowych do regulaminu sklepu internetowego,
   20) klauzula umowna o wzajemnym powierzeniu przetwarzania danych osobowych,

§ 2 Obszar i czynności przetwarzania danych osobowych i ich rodzaje

1. Dane osobowe są przetwarzane przez ADO wyłącznie z pomieszczeniach lub przestrzeniach tworzących obszar przetwarzania danych osobowych. Opis obszaru przetwarzania danych osobowych, w tym ewidencja pomieszczeń stanowi załącznik nr 3 do Polityki.
2. Dane osobowe są przetwarzane przez ADO wyłącznie w celach i w zakresie określonym w rejestrze czynności przetwarzania stanowiącym załącznik nr 4 do Polityki.
3. Dane osobowe powierzone ADO do przetwarzania przez innych administratorów danych są przetwarzane wyłącznie w celach i w zakresie określonym w rejestrze kategorii czynności przetwarzania stanowiącym załącznik nr 4a do Polityki.
4. ADO przetwarza dane osobowe zwykłe lub szczególnych kategorii w rozumieniu art. 9 RODO (wrażliwe). Szczegółowy wykaz rodzajów przetwarzanych danych osobowych zawiera opis struktury zbiorów danych osobowych wraz z opisem sposobu przepływu danych między systemami informatycznymi stanowiący załącznik nr 5 do Polityki.

§ 3 Zabezpieczenie danych osobowych

1. Dane osobowe przetwarzane przez ADO, w tym za pomocą systemów informatycznych, są chronione za pomocą środków technicznych, informatycznych i organizacyjnych, które mają zabezpieczyć przetwarzane dane przed:
   1) udostępnieniem osobom nieupoważnionym;
   2) zabraniem przez osobę nieuprawnioną;
   3) przetwarzaniem z naruszeniem obowiązujących przepisów oraz ich zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Do środków technicznych należą:
   1) zastosowanie ochrony bezpośredniej i monitoringu wizyjnego przy wejściu do siedziby ADO oraz monitoringu wizyjnego przy wejściu do obszaru przetwarzania danych osobowych;
   2) zabezpieczenie antywłamaniowe wejścia do siedziby ADO oraz do pomieszczeń tworzących obszaru przetwarzania danych osobowych;
   3) zastosowanie systemu kontroli dostępu do obszaru przetwarzania danych osobowych;
   4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa przechowywanej w nich dokumentacji.
3. Do środków informatycznych należą środki opisane w Instrukcji zarządzania systemem informatycznym.
4. Do środków organizacyjnych należą:
   1) dokonywanie przetwarzania danych osobowych wyłącznie przez osoby, którym ADO udzielił upoważnienia lub podmioty, w którymi ADO zawarł umowę powierzenia przetwarzania danych. Wykazy tych osób i podmiotów stanowią odpowiednio załączniki nr 7 i nr 8;
   2) przeszkolenie każdej osoby przed dopuszczeniem jej do przetwarzania danych osobowych w zakresie przepisów dot. ochrony danych osobowych, oraz bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych osobowych;
   3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę;
   4) zapewnienie dostępu do obszaru przetwarzania danych osobowych wyłącznie osobom uprawnionym;
   5) osoby nieuprawnione mogą przebywać w obszarze przetwarzania danych osobowych wyłącznie w obecności osoby uprawnionej;
   6) zapewnienie w pomieszczeniach obszaru przetwarzania danych osobowych właściwych parametrów środowiskowych dla sprzętu komputerowego oraz wyposażenia ppoż;

7) stosowanie tzw. polityki czystego biurka

5. W ramach polityki czystego biurka pracownicy ADO są zobowiązani do:
   1) przechowywania na biurku tylko tych dokumentów, które są potrzebne do wykonywania w danym momencie pracy;
   2) nie przetrzymywania na biurku jedzenia oraz picia;
   3) zabezpieczenia po zakończonej pracy dokumentów w zamykanej na klucz szafie;
   4) niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.
6. Niezależnie od zasad określonych w Polityce, w zakresie bezpieczeństwa danych osobowych stosuje się wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informatycznych.

§ 4 Opis ryzyka zdarzeń naruszających ochronę danych osobowych

1. Niebezpieczeństwem dla danych osobowych i ich ochrony są następujące rodzaje zagrożeń:
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych;
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki, awarie sprzętowe, błędy oprogramowania) – których występowanie może prowadzić do zniszczenia danych, może zostać zakłócona ciągłość pracy systemów oraz nastąpić naruszenie poufności danych;
   3) zagrożenia zamierzone, świadome i celowe – stanowią najpoważniejsze zagrożenia naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te można podzielić na:
      - nieuprawniony dostęp do systemów z zewnątrz (włamanie do systemu),
      - nieuprawniony dostęp do systemów z jego wnętrza,
      - nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemów.
2. Przypadkami uznanymi jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe, stanowią:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemów - np.: wybuch, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, uszkodzenia w czasie remontu;
   2) niewłaściwe parametry środowiska - np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, w tym pozostawienie serwisantów bez nadzoru;
   4) odpowiedni komunikat alarmowy od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
   5) nieprawidłowa jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
   6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
   7) próba lub modyfikacja danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

8) niedopuszczalna manipulacja danymi osobowymi w systemie;
9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
10) praca w systemie informatycznym wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w systemie osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
11) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.;
12) podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub skopiowanie danych osobowych;
13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji – np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, praca na danych osobowych w celach prywatnych;
14) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych - np. otwarte szafy, biurka, regały oraz inne - na nośnikach papierowych na lub na nośnikach elektronicznych, w formie niezabezpieczonej.

§ 5 Kontrola przestrzegania zasad ochrony danych osobowych

1 IODO sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z obowiązujących przepisów oraz zasad ustanowionych w Polityce, a także dokonuje okresowych ocen stanu bezpieczeństwa danych osobowych, z których sporządza sprawozdanie.

2 W przypadku stwierdzeniu naruszenia lub ujawnienia ochrony danych osobowych IODO:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy ADO;
2) żąda dokładnej informacji od osoby powiadamiającej oraz od innych osób, posiadających informacje związane z naruszeniem;

3. IODO dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób udzielających informacji o naruszeniu;
2) określenie czasu i miejsca naruszenia i powiadomienia;
3) określenie okoliczności towarzyszących i rodzaju naruszenia;
4) wyszczególnienie przesłanek wyboru metody postępowania i opis podjętego działania;
5) wstępną ocenę przyczyn wystąpienia naruszenia;
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

4. IODO składa w okresach półrocznych ADO informacje o stanie bezpieczeństwa danych osobowych, oraz niezwłocznie o każdorazowym stwierdzonym przypadkach naruszania bezpieczeństwa danych osobowych oraz podjętych niezbędnych środkach doraźnych.

5. ADO po uzyskaniu informacji, o których mowa w ust. 3 lub 4, zasięga niezbędnych opinii i wprowadza postępowanie naprawcze, w tym podejmuje decyzję o ewentualnym odtworzeniu danych z zabezpieczeń, terminie wznowienia przetwarzania danych oraz podejmuje przedsięwzięcia proceduralne, organizacyjne i techniczne, które powinny zapobiec podobnym

naruszeniom w przyszłości.

§ 6 Opis postępowania w przypadku naruszenia ochrony danych osobowych

Opis postępowania w przypadku naruszenia ochrony danych osobowych jest zawarty w Instrukcji zarządzania systemem informatycznym, stanowiącej załącznik nr 9 do Polityki.

§ 7 Monitorowanie zabezpieczeń

1. Prawo do monitorowania systemu zabezpieczeń posiadają zgodnie z zakresem czynności:
   1) Prezes Zarządu;
   2) IODO;
   3) Administrator Systemu – w zakresie systemów informatycznych.
2. W ramach kontroli należy zwracać szczególną uwagę na:
   1) okresowe sprawdzanie kopii zapasowych (bezpieczeństwa) pod względem przydatności do możliwości odtwarzania danych;
   2) kontrolę ewidencji nośników danych;
   3) kontrolę właściwej częstotliwości zmiany haseł;
   4) kontrolę zabezpieczeń technicznych pomieszczeń i miejsc, w których są przetwarzane lub przechowywane dane osobowe;
   5) kontrolę stosowania procedur związanych z ochroną danych osobowych.
3. Wszystkie osoby dopuszczone do przetwarzania danych osobowych mają obowiązek brać udział w szkoleniach z zakresu ochrony danych osobowych.
4. Szkolenie powinno dotyczyć:
   1) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach różnego rodzaju;
   2) zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy;

§ 8 Niszczenie nośników danych osobowych

1. Nośniki wszelkiego rodzaju wykorzystywane w systemach informatycznych, które zostają przekazane na zewnątrz, powinny być pozbawione zapisów zawierających dane osobowe. Poprawność przygotowania nośnika do przekazania na zewnątrz powinna być sprawdzona przez ASI.
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika, o ile jest to możliwe. W przeciwnym wypadku niszczenie zapisów następuje poprzez fizyczne zniszczenie nośnika.
3. Uszkodzone nośniki wykorzystywane w systemach informatycznych, przed ich utylizacją lub przekazaniem na zewnątrz, należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
4. Uszkodzone komputery przed ich przekazaniem do naprawy lub utylizacji są pozbawiane nośników danych (dysków).
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

§ 9 Archiwizacja danych

Tworzenie kopii zapasowych danych osobowych następuje na zasadach określonych w Instrukcji zarządzania systemem informatycznym, stanowiącej załącznik nr 9 do Polityki.

§ 10 POSTANOWIENIA KOŃCOWE

1. Wobec pracownika ADO, która w przypadku naruszenia ochrony danych osobowych nie podjął działania określonego w Polityce, w szczegó1ności nie powiadomił odpowiedniej osoby zgodnie z obowiązującymi procedurami, wszczyna się postępowanie dyscyplinarne.
2. Przypadki nieuzasadnionego zaniechania obowiązków określonych w Polityce mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez pracownika, który w przypadku naruszenia ochrony danych osobowych nie powiadomił o tym IODO lub ASI. Orzeczona wobec pracownika kara dyscyplinarna nie wyklucza jego odpowiedzialności karnej zgodnie z ustawą o ochronie danych osobowych oraz możliwości wniesienia przez ADO przeciwko niemu pozwu o odszkodowanie.
3. Postanowienia ust. 2 stosuje się odpowiednio do osób zatrudnionych na podstawie innych umów niż umowa o pracę. W tym przypadku zaniechania obowiązków wynikających z Polityki uznaje się za rażące naruszenie umowy.
4. W sprawach nie uregulowanych w Polityce stosuje się przepisy obowiązujące w zakresie ochrony danych osobowych.
5. Polityka bezpieczeństwa wchodzi w życie z dniem …….

Załączniki:

1) oświadczenie o wyznaczeniu IODO,
2) ewidencja pomieszczeń tworzących obszar przetwarzania danych osobowych,
3) rejestr czynności przetwarzania danych osobowych,
4) opis struktury zbiorów danych osobowych,
5) rejestr przypadków naruszenia bezpieczeństwa przetwarzania danych osobowych,
6) rejestr osób upoważnionych do przetwarzania danych osobowych,
7) rejestr podmiotów, którym powierzono przetwarzanie danych osobowych na podstawie umowy powierzenia przetwarzania,
8) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
9) ewidencja korespondencji inspektora ochrony danych osobowych,
10) polityka prywatności,
11) wzory raportów IODO,
12) klauzula informacyjna zamieszczana w stopce poczty elektronicznej i na fakturach,
13) klauzula informacyjna o monitoringu,
14) upoważnienie do przetwarzania danych osobowych,
15) oświadczenie pracownika dotyczące przetwarzania danych osobowych i zachowania ich poufności,
16) klauzula informacyjna dla pracowników,
17) klauzula informacyjna na podstawie art. 14 RODO,
18) umowa o powierzeniu przetwarzania danych osobowych,
19) klauzula umowna informująca o przetwarzaniu danych osobowych do regulaminu sklepu internetowego,
20) klauzula umowna o wzajemnym powierzeniu przetwarzania danych osobowych,