POLITYKA BEZPIECZEŃSTWA INFORMACJI
w MS Sp. z o.o.
w Straszynie

SPIS TREŚCI

Rozdział 1.
Postanowienia ogólne

§ 1.
Podstawy prawne

1. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. 2016 r. poz. 922) (uodo);
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024);
3. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U., poz. 1934);
4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U., poz. 745);
5. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U., poz. 719);
6. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 r., poz. 113);
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)(Dz.Urz.UE L119 z 4 maja 2016 r.).

§ 2.
Słownik pojęć

1. **Administrator Danych Osobowych** (**ADO**) - organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych.

W tym przypadku Administratorem Danych Osobowych jest MS Sp. z o.o. w Straszynie reprezentowana przez Prezesa Zarządu;

2. **Administrator Bezpieczeństwa Informacji (ABI)** - osoba fizyczna powołana przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem rejestru zbiorów danych przetwarzanych przez administratora danych;
3. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
5. **Droga elektroniczna** – poczta elektroniczna lub elektroniczna skrzynka podawcza, o której mowa w art. 3 pkt 7 ustawy z dnia 17 lutego 2005 r. o informatyzacji dzialalności podmiotów realizujących zadania publiczne (t.j. Dz.U. 2017 r., poz. 570)**;**
6. **Działanie korygujące** - działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji;
7. **Działanie zapobiegawcze** - działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności/incydentu lub innej potencjalnej sytuacji niepożądanej;
8. **GIODO –** Generalny Inspektor Ochrony Danych Osobowych;
9. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
10. **Identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11. **Incydent -** pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego i zagrażają bezpieczeństwu informacji; naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
12. **Informacja stanowiąca tajemnicę służbową -** informacja uzyskana w związku z czynnościami służbowymi lub wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli, interesu publicznego lub MS Sp. z o.o. w Straszynie;
13. **Informatyk** – osoba fizyczna wyznaczona przez Administratora Danych Osobowych, zajmująca się sprawowaniem ogólnego nadzoru nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym danych osobowych przetwarzanych w systemie informatycznym stosowanym w MS Sp. z o.o. w Straszynie;
14. **IZSI –** Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w MS Sp. z o.o. w Straszynie;
15. **Korekcja** - działanie w celu wyeliminowania wykrytej niezgodności lub incydentu;
16. **Kontrola (Audyt)** - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań polityk i procedur**;**
17. **Niezgodność** - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe;

18. **Nośniki danych** – przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych;
19. **Odbiorca danych** – każdy, komu udostępniane są dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela administratora danych mającego siedzibę w państwie trzecim, przetwarzającego dane przy wykorzystaniu środków technicznych znajdujących się na terytorium RP, podmiotu który przetwarza dane na podstawie umowy powierzenia zawartej z administratorem, a także organów państwowych i organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem (art. 7 pkt 6 ustawy);
20. **Podatność** - luka (słabość), która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę;
21. **PBI / Polityka** – niniejszy dokument;
22. **Pracownik** – osoba fizyczna świadcząca na rzecz MS Sp. z o.o. w Straszynie pracę na podstawie stosunku pracy, powołania, mianowania, wykonująca zadania wyłącznie osobiście, w ramach prowadzonej działalności gospodarczej lub powierzone jej na podstawie umowy cywilnoprawnej, współpracująca w rozumieniu ustawy z dnia 13 października 1998 roku o systemie ubezpieczeń społecznych (Dz.U. 2016, poz. 963);
23. **Profilowanie** – automatyczny proces przetwarzania danych osobowych, dopuszczalny pod warunkiem spełnienia przesłanek określonych przepisami prawa;
24. **Przetwarzane danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;
25. **Słabość systemu** - zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu**;**
26. **Spółka** – MS Sp. z o.o. z siedzibą przy ul. Jowisza 1/4, 83-010 Straszyn;
27. **System informatyczny (system IT)** - zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
28. **System tradycyjny** - zespół procedur organizacyjnych, wyposażenia i środków trwałych związanych z mechanicznym przetwarzaniem informacji zawierających dane osobowe na nośnikach papierowych;
29. **Serwisant** – pracownik firmy zewnętrznej lub pracownik MS Sp. z o.o. w Straszynie w rozumieniu ust. 23 niniejszego paragrafu zajmujący się instalacją, naprawą i konserwacją sprzętu komputerowego;
30. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
31. **Sytuacja kryzysowa** - sytuacja wpływająca negatywnie na poziom bezpieczeństwa zasobów i infrastruktury technicznej, każde zdarzenie, zagrożenie lub domniemanie utraty poufności, integralności lub dostępności informacji wrażliwej przetwarzanej w systemie teleinformatycznym;
32. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
33. **Usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą;
34. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
35. **Użytkownik** – pracownik MS Sp. z o.o. w Straszynie bez względu na rodzaj stosunku pracy i wymiar etatu, stażysta, praktykant oraz każda inna osoba, która uzyskała

upoważnienie od ADO do przetwarzania danych osobowych w systemach IT, a także osoba upoważniona przez kierownika podmiotu, z którym została podpisana umowa powierzenia przetwarzania danych osobowych;

36. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
37. **Zagrożenie** - potencjalna możliwość wystąpienia incydentu;
38. **Zbiór danych osobowych** - posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
39. **Zdarzenie** - błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z zagrożeniem bezpieczeństwa danych osobowych.

§ 3.
Cel i zakres.

1. Polityka Bezpieczeństwa Informacji jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych w MS Sp. z o.o. w Straszynie;
2. Polityka Bezpieczeństwa Informacji została opracowana i wdrożona w celu uzyskania standardu przetwarzania informacji zawierających dane osobowe zgodnego z wymaganiami określonymi w przepisach prawa, o których mowa w § 1 ust. 1-7 niniejszego dokumentu, w szczególności danych osobowych przetwarzanych w celach określonych w art. 27 ust. 2 pkt 7 ustawy, danych osobowych przetwarzanych w systemie informatycznym wykorzystywanym w Spółce oraz pozostałych informacji podlegających ochronie;
3. Niniejszy dokument został wprowadzony Zarządzeniem Prezesa Zarządu oraz udostępniony każdej osobie mającej dostęp do danych osobowych przetwarzanych w Spółce. Potwierdzeniem zapoznania się z postanowieniami niniejszego dokumentu jest złożenie pisemnego oświadczenia, którego wzór stanowi załącznik nr 3 do Zarządzenia wymienionego w zdaniu pierwszym.

§ 4.

1. Polityka Bezpieczeństwa Informacji określa w szczególności:

    1) Prawa, obowiązki oraz granice dopuszczalnego zachowania osób przetwarzających dane osobowe w związku z działalnością Spółki, Użytkowników systemów IT i tradycyjnych, w których przetwarzane są dane osobowe oraz konsekwencje naruszenia przepisów o ochronie danych osobowych wymienionych w § 1 ust. 1-7,

    2) sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych, w tym podstawowe warunki jakim powinny odpowiadać urządzenia z wykorzystaniem których dane są przetwarzane,

    3) zasady prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych, w tym jawnego rejestru zbiorów danych osobowych zgłaszanych do GIODO,

    4) zasady prowadzenia wykazu zbiorów danych osobowych wraz ze wskazaniem

programów zastosowanych do przetwarzania tych danych, opisu struktury zbiorów danych wskazującej zawartość poszczególnych pól informacyjnych i powiązań między nimi oraz sposób przepływu informacji pomiędzy poszczególnymi systemami,

5) wymagania w zakresie odnotowywania udostępniania danych osobowych,

6) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych,

2. Zastosowane zabezpieczenia mają zapewnić:

   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom,

   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,

   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej,

   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

   6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.

Rozdział 2.
Administrator Danych Osobowych. Administrator Bezpieczeństwa Informacji. Informatyk.

§ 5.
Administrator Danych Osobowych (ADO)

1. Administrator Danych Osobowych podejmuje decyzje w zakresie realizacji celów i zapewnienia środków zapewniających bezpieczeństwo przy przetwarzaniu danych osobowych, zgodnie z wymogami i zaleceniami wynikającymi z przepisów prawa, w celu ochrony interesów osób, których dane dotyczą;
2. Administrator Danych Osobowych pełni funkcję kontrolną w zakresie poprawnego przetwarzania danych osobowych oraz nadzoruje przestrzeganie ustalonych zasad zawartych w PBI;
3. Administrator Danych Osobowych jest zobowiązany do zgłoszenia GIODO powołania (lub odwołania) ABI, wyłącznie przy użyciu formularzy zgłoszeń powołania i odwołania Administratora Bezpieczeństwa Informacji, których wzory stanowią

załączniki do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku (Dz.U., poz. 1934). W przypadku niepowołania ABI, funkcje mu przypisane ADO pełni w zakresie zgodnym z obowiązującymi przepisami;

4. Zadania nałożone na Administratora Danych Osobowych ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych obejmują ponadto:
    1) wypełnianie obowiązku informacyjnego przy zbieraniu danych osobowych wynikającego z art. 24 i 25 ustawy, w tym udzielanie informacji o celu i zakresie przetwarzanych danych osobowych wynikające z art. 33 ustawy,
    2) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza wynikającej z art. 26 ustawy,
    3) obowiązek uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane wynikający z art. 35 ustawy,
    4) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną wynikające z art. 36 ustawy,
    5) nadawanie i anulowanie upoważnień do przetwarzania danych osobowych wynikające z art. 37 ustawy,
    6) obowiązek kontrolowania jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane wynikający z art. 38 ustawy,
    7) obowiązek prowadzenia wykazu osób upoważnionych do przetwarzania danych osobowych wynikający z art. 39 ustawy,
    8) nadzór nad zgłaszaniem przez ABI zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych wynikający z art. 40 ustawy.

§ 6.
Administrator Bezpieczeństwa Informacji.

ABI jest powoływany przez ADO drogą pisemnego upoważnienia. Wzór upoważnienia dla ABI stanowi załącznik nr 5 do PBI. ABI jest również zobowiązany do podpisania oświadczenia o zachowaniu poufności (załącznik nr 4 do PBI).

§ 7.

1. Do kompetencji ABI należy w szczególności:
    1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdań dla ADO,
    2) nadzorowanie przestrzegania zasad ochrony danych osobowych tj. środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, ze szczególnym uwzględnieniem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w tym nadzór nad obiegiem oraz przechowywaniem materiałów i dokumentów zawierających dane osobowe we współpracy z Informatykiem w zakresie dotyczącym systemu IT,

3) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych, środki ich ochrony oraz przestrzegania zasad w niej określonych,
4) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
5) wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych oraz pozostałych wniosków dotyczących bezpieczeństwa informacji, w tym danych osobowych, a także nadzór w zakresie realizacji tych wniosków,
6) nadzór nad fizycznym zabezpieczeniem pomieszczeń we współpracy z ADO, w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób,
7) zapewnienie przeciwdziałania incydentom oraz prowadzenie rejestru incydentów i zagrożeń (załącznik nr 10 do PBI),
8) w porozumieniu z Informatykiem, szkolenie osób upoważnionych do przetwarzania danych osobowych w zakresie przepisów o ochronie danych osobowych oraz zapewnienie bieżącej edukacji Użytkowników w zakresie polityki bezpieczeństwa, w tym wnioskowanie do ADO o organizację tych szkoleń.

§ 8.

1. ABI prowadzi jawny rejestr zbiorów danych osobowych (załącznik nr 14) przetwarzanych na potrzeby realizacji celów i zadań Spółki oraz wykaz zbiorów zawierający strukturę zbiorów, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi wraz z programami zastosowanymi do ich przetwarzania (załącznik nr 2). Kiedy jest to wymagane przez przepisy, ABI zgłasza te zbiory do rejestracji GIODO;
2. W ramach nadzoru nad przetwarzaniem danych, ABI sprawdza w szczególności cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia danych osobowych, w tym zabezpieczenia urządzeń mobilnych wykorzystywanych w działalności MS Sp. z o.o. w Straszynie;
2. ABI jest również zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym oraz tradycyjnym z uwzględnieniem specyfiki pracy wiążącej się z koniecznością przetwarzania danych osobowych poza siedzibą ADO z wykorzystaniem urządzeń mobilnych;
3. Ponadto ABI jest odpowiedzialny za prowadzenie i aktualizację wykazu budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1 do PBI), wykazu udostępnień danych osobowych innym podmiotom (załącznik nr 7 do PBI), wykazu podmiotów, którym powierzono dane osobowe do przetwarzania (załącznik nr 8 do PBI) oraz wykazu udostępnień danych osobowych osobom, których dane dotyczą (załącznik nr 9 do PBI).

§ 9.
Informatyk.

1. Do zadań Informatyka należy zapewnienie działania infrastruktury teleinformatycznej i oprogramowania w sposób zapewniający właściwy poziom bezpieczeństwa informacji wynikający z obowiązujących przepisów, PBI oraz zaleceń ABI;
2. Nadzorowanie przez Informatyka przestrzegania bezpieczeństwa danych osobowych gromadzonych i przetwarzanych w systemach IT ma na celu zabezpieczenie ich

przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

3. Do kompetencji Informatyka należy w szczególności:
   1) zapewnienie właściwego poziomu bezpieczeństwa systemu informatycznego, w tym danych osobowych w nich przetwarzanych,
   2) zapewnienie mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych,
   3) inicjatywa w zakresie zapewnienia alternatywnego, awaryjnego zasilania systemu informatycznego oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, w tym raportowanie do ABI stanu zabezpieczeń w zakresie centralnego awaryjnego zasilania budynku, w porozumieniu z administratorem budynku,
   4) podejmowanie działań zabezpieczających system informatyczny w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu, informacji o zmianach w sposobie działania systemu lub innych urządzeń wskazującej na naruszenie bezpieczeństwa danych,
   5) zapewnienie ochrony systemu teleinformatycznego oraz danych osobowych przesyłanych za pośrednictwem tych systemów,
   6) zapewnienie ochrony danych osobowych w związku z naprawą, konserwacją oraz likwidacją systemu informatycznego, w tym urządzeń komputerowych, na których zapisane są dane osobowe,
   7) wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych w systemie IT oraz realizacja tych czynności po akceptacji ADO,
   8) zapewnienie przeglądów, konserwacji oraz uaktualnień systemu służącego do przetwarzania danych osobowych, w tym w szczególności z uwzględnieniem specyfiki działalności Spółki,
   9) przestrzeganie przepisów bhp i ppoż. w przynależnych pomieszczeniach.

Rozdział 3.
Zasady przetwarzania danych osobowych. Profilowanie. Powierzenie. Udostępnianie. Obowiązek informacyjny. Zgoda. Zabezpieczenia. Sprawdzenia. Odpowiedzialność.

§ 10.

1. Zasady przetwarzania danych osobowych:
   1) dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Spółka może żądać podania jedynie tych danych, które są niezbędne do realizacji jej celów i zadań,
   2) zakres danych osobowych przetwarzanych przez jednego Użytkownika w systemie IT nie może być szerszy niż powierzony do przetwarzania w związku z wykonywanymi przez niego obowiązkami,
   3) po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą, zniszczone lub, w przypadku powierzenia, zwrócone podmiotowi, który dane powierzył;
2. Zasady ochrony danych osobowych określone przez PBI mają zastosowanie do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów przetwarzania informacji zawierających dane osobowe, w tym systemów IT,

2) informacji będących własnością Spółki oraz przetwarzanych przez nią w związku z prowadzoną działalnością,
3) wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
4) wszystkich osób świadczących pracę lub wykonujących czynności na rzecz Spółki mających dostęp do informacji podlegających ochronie,
5) wszystkich kontrahentów Spółki.

§ 11.

1. Przetwarzanie danych osobowych odbywa się z wykorzystaniem dokumentów, materiałów, przesyłek analogowych (nieelektronicznych), wniosków, pism, akt osobowych pracowników, dokumentów finansowo-księgowych, podań itp. oraz danych zawartych na nośnikach elektronicznych, magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych, a także danych przetwarzanych w systemie kadrowo-płacowym, systemie do obsługi dokumentów ubezpieczeniowych i wymianie informacji z ZUS, systemie teleinformatycznym administracji.

§ 12.

1. Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia lub części pomieszczeń w siedzibie Spółki znajdującej się przy ul. Jowisza 1/4 w Straszynie (załącznik nr 1 do PBI);
2. Pomieszczenia znajdujące się w budynku Spółki podzielone są na:
   1) strefę obejmującą pomieszczenia, gdzie kontrolowany jest ruch osobowy i materiałowy, do których dostęp posiadają pracownicy oraz pozostałe osoby przebywające w tej strefie w związku z wykonywanymi obowiązkami lub czynnościami,
   2) strefę obejmującą pomieszczenia objęte szczególną kontrolą wejścia i wyjścia oraz kontrolą przebywania, gdzie przebywać mogą wyłącznie upoważnieni pracownicy lub pozostałe osoby pod nadzorem upoważnionych pracowników.

§ 13.

Wszystkie osoby, które posiadają dostęp do danych osobowych w obszarze wymienionym w § 12 muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez ADO oraz podpisać oświadczenie o zachowaniu poufności. Wzór upoważnienia stanowi załącznik nr 3 do PBI. Wzór oświadczenia o zachowaniu poufności stanowi załącznik nr 4 do PBI.

§ 14.

Uprawnienia do przetwarzania danych osobowych w systemach IT nadawane są zgodnie z właściwą procedurą określoną w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w MS Sp. z o.o. w Straszynie (IZSI). Uprawnienia, o których mowa w zdaniu pierwszym, ważne są do dnia odwołania lub do chwili ustania zatrudnienia uprawnionego pracownika.

§ 15.

1. Ochrona dotyczy w szczególności:

1) danych osobowych gromadzonych i przetwarzanych w związku z działalnością Spółki, w tym danych osobowych kontrahentów i klientów w związku z zawieranymi umowami,
2) danych osobowych pracowników, w tym danych osobowych i treści zawieranych umów o pracę,
3) danych osobowych kandydatów do pracy zbieranych na etapie rekrutacji,
4) danych osobowych zawartych w dokumentach finansowo-księgowych,
5) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach IT, w których są przetwarzane dane osobowe,
6) rejestru osób dopuszczonych do przetwarzania danych osobowych,
7) danych osobowych zawartych w pozostałych dokumentach wytwarzanych w związku z działalnością Spółki.

2. Katalog zbiorów przetwarzanych danych osobowych może ulec rozszerzeniu, w zależności od zakresu bieżącej działalności Spółki.

§ 16.

1. W zbiorach danych gromadzonych w systemach IT zabrania się przetwarzania danych ujawniających stan zdrowia, pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, przynależność partyjną lub związkową, dane genetyczne, dane biometryczne, nałogi, preferencje seksualne, chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę;
2. Dane o skazaniach, w tym dane o niekaralności można przetwarzać wyłącznie w zakresie uregulowanym w art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz.U. 2017 poz. 678);

§ 17.
Profilowanie danych osobowych.

1. Do profilowania zabrania się używania danych wymienionych w § 16, chyba, że wymagają tego obowiązujące przepisy prawa, osoba, której dane dotyczą wyraziła na to zgodę lub jest to podyktowane ważnym interesem publicznym;
2. Przy profilowaniu Administrator Danych Osobowych obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą;
3. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą;
4. Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

§ 18.
Powierzenie przetwarzania danych osobowych.

1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy oraz pracownicy podmiotów współpracujących lub świadczących usługi na rzecz Spółki (procesorów, kontrahentów) w zakresie adekwatnym do celu powierzenia;
2. Powierzenie przetwarzania danych osobowych następuje na podstawie umowy powierzenia lub innego aktu prawnego, zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej (oświadczenie złożone drogą elektroniczną lub

zapisane na elektronicznym nośniku informacji, określona opcja internetowa). Wzór umowy powierzenia, zgodny z art. 31 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz art. 28 rozporządzenia ogólnego (RODO), stanowi załącznik nr 13 do PBI;

3. Umowa powierzenia danych osobowych określa przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy (administratora i procesora);

4. Podmiot, z którym zostaje zawarta umowa powierzenia jest zobowiązany do wdrożenia środków organizacyjnych i technicznych odpowiednich do ryzyk przetwarzania powierzonych danych, prowadzenia rejestru czynności przetwarzania, zgłaszania naruszeń ochrony danych do organu nadzorczego, czyli GIODO. Szczegółowy zakres praw i obowiązków procesorów określono w dokumencie o nazwie: Wymagania bezpieczeństwa informacji dla kontrahentów MS Sp. z o.o. w Straszynie;

5. Administrator Danych Osobowych zobowiązany jest do dokumentowania powierzania tych danych w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi. Wzór wykazu podmiotów, którym powierzono dane osobowe stanowi załącznik nr 8 do PBI;

6. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych), wymagana jest szczegółowa lub ogólna zgoda ADO na przekazanie powierzonych danych, wyrażona w formie pisemnej lub równoważnej jej formie elektronicznej.

§ 19.
Udostępnianie danych osobowych

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności;
2. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych;
3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych;
4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 20.
Obowiązek informacyjny.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany poinformować tę osobę o:
    1) adresie swojej siedziby i pełnej nazwie,
    2) celu i zakresie zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
    3) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej i konsekwencjach niepodania danych,
    4) Administratorze Bezpieczeństwa Informacji,
    5) prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywać się będzie przetwarzanie danych,
    6) okresie, przez który dane osobowe będą przechowywane lub o kryteriach tego okresu,
    7) profilowaniu danych,
    8) prawach osoby, której dane dotyczą tj. prawie do usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych);
2. W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, ADO jest zobowiązany poinformować tę osobę, oprócz wymienionych w ust. 1 pkt 1-8, o źródle pozyskania danych oraz uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 ustawy o ochronie danych osobowych;
3. Obowiązek poinformowania wymieniony w ust. 1 niniejszego paragrafu powinien być wykonany w momencie zbierania danych z wyjątkiem sytuacji, w której przepis innej ustawy zezwala na przetwarzanie danych osobowych lub osoba, której dane dotyczą, posiada już informacje, których udzielenia wymaga art. 24 ust. 1 ustawy o ochronie danych osobowych;
4. Obowiązek poinformowania wymieniony w ust. 2 niniejszego paragrafu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie z wyjątkiem sytuacji opisanych w art. 25 ust. 2 ustawy o ochronie danych osobowych.

§ 21.
Zgoda na przetwarzanie danych osobowych.

1. Zgodnie z art. 7 pkt 5 ustawy o ochronie danych osobowych oraz art. 4 ust. 11 RODO, zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
2. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana ani wynikać z oświadczenia woli o innej treści, tzn. zgoda nie może być zawarta np. w regulaminie, którego zaakceptowanie wiąże się ze zgodą na warunki w nim zawarte;
3. Zgodnie z ust. 32 preambuły RODO, w przypadku pozyskania zgody w formie innej niż pisemna, na ADO ciąży obowiązek udowodnienia, że została ona pozyskana, a nie dorozumiana – „*Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny oznaczać zgody*”;
4. Zgoda na przetwarzanie danych osobowych powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, należy pozyskać odrębną zgodę na każdy cel;
5. Zgodnie z ust. 32 preambuły RODO, elektroniczne pytanie o zgodę musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy;

6. Zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie w sposób tak samo prosty i przystępny, w jaki została pozyskana.

§ 22.

1. Zgoda na przetwarzanie danych osobowych nie jest wymagana w przypadku, gdy dane będą przetwarzane:
   1) w związku z zawarciem umowy z osobą, której dane dotyczą,
   2) na podstawie przepisu prawa,
   3) w interesie publicznym,
   4) w prawnie usprawiedliwionym celu administratora danych,
   5) w przypadku żywotnego interesu osoby, której dane dotyczą, gdy pozyskanie zgody jest konieczne, ale niemożliwe.

§ 23.
Zabezpieczenia danych osobowych.

W celu zapewnienia należytej ochrony przetwarzania danych osobowych, w Spółce zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych.

§ 24.
Zabezpieczenia techniczne.

1. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w zabezpieczonych pomieszczeniach (zamki na klucz, karty zbliżeniowe);
2. Pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w system ostrzegania alarmowego, w tym dźwiękowego;
3. Pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczone przed skutkami pożaru za pomocą instalacji przeciwpożarowej;
4. Dostęp do pomieszczeń kontrolowany jest przez system całodobowego monitoringu wizyjnego;
5. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce;
6. Zastosowano specjalistyczne urządzenia chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
7. Do ochrony dostępu do sieci komputerowej stosuje się zaporę sieciową Firewall;
8. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
9. Stosowany system informatyczny posiada mechanizm wymuszający okresową zmianę haseł dostępu;
10. Dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (Ms Word), arkuszach kalkulacyjnych (Ms Excel) lub programach równorzędnych (np. Open Office) i innych programach do tworzenia baz danych oraz w systemach informatycznych, np. Płatnik, system bankowości elektronicznej itp. stosuje się środki ochrony przed szkodliwym oprogramowaniem: robaki, wirusy, konie trojańskie itp.;
11. W przypadku wystąpienia konieczności dostępu do zbioru danych osobowych w czasie nieobecności pracownika upoważnionego do przetwarzania danych w tym zbiorze, ABI, w porozumieniu z Informatykiem w zakresie dostępu do systemu informatycznego, może udostępnić ten zbiór innemu pracownikowi w celu dokonania

niezbędnych czynności służbowych. Po powrocie nieobecny pracownik otrzymuje nowe indywidualne hasło dostępu;
12. Z każdego zdarzenia opisanego w ust. 10 niniejszego paragrafu, ABI sporządza protokół, w którym podaje: imiona i nazwiska osób zastępujących nieobecnego pracownika;
13. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
14. Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych;
15. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 25.
Zabezpieczenia organizacyjne.

1. Opracowano i wdrożono Politykę Bezpieczeństwa Informacji oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w MS Sp. z o.o. w Straszynie;
2. Powołano Administratora Bezpieczeństwa Informacji, który sprawuje nadzór nad przetwarzaniem danych osobowych w systemie tradycyjnym;
3. Wyznaczono Informatyka który sprawuje nadzór nad przetwarzaniem danych osobowych w systemie informatycznym;
4. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony tych danych;
5. Wszyscy Użytkownicy systemu informatycznego zostali przeszkoleni w zakresie zasad korzystania i zabezpieczeń tego systemu;
6. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO oraz które podpisały oświadczenie o zachowaniu poufności zobowiązujące je do zachowania przetwarzanych danych w tajemnicy;
7. Prowadzone są wykazy osób i podmiotów, którym udostępniono lub powierzono przetwarzanie danych osobowych;
8. Przetwarzanie danych osobowych przez osoby upoważnione odbywa się w wyznaczonych pomieszczeniach, zgodnie ze strefami kontroli, w godzinach pracy lub po godzinach, po uprzednim uzyskaniu zgody ADO;
9. Dostęp osób nieposiadających stosownych upoważnień do pomieszczeń, w których przetwarzane są dane osobowe odbywa się wyłącznie za zgodą ADO lub w obecności i pod nadzorem osób upoważnionych;
10. Wykonane kopie zapasowe zbiorów danych osobowych przechowywane są w pomieszczeniu innym niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

§ 26.

1. Wszyscy pracownicy posiadający dostęp do danych osobowych przed przystąpieniem do pracy uczestniczą w szkoleniu dotyczącym obowiązujących

przepisów prawa z zakresu ochrony danych osobowych oraz obowiązujących w Spółce procedur wewnętrznych;
2. Zakres czynności dla osoby upoważnionej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę przetwarzanych danych osobowych w stopniu adekwatnym do jej zadań na stanowisku pracy;

§ 27.

1. Nadzór nad dostępem do pomieszczeń, w których przetwarzane są dane osobowe sprawuje ABI lub wyznaczona przez niego osoba;
2. Pracownicy Spółki są zobowiązani do informowania ABI o zauważonych próbach nieuprawnionego dostępu do pomieszczeń, o których mowa w ust. 1.

§ 28.

1. Po godzinach urzędowania dostęp do pomieszczeń mają pracownicy oraz osoby sprzątające upoważnione przez ADO;
2. ADO w porozumieniu z ABI oraz Informatykiem może określić pomieszczenia, do których dostęp osób sprzątających będzie ograniczony i możliwy tylko pod nadzorem osób uprawnionych do przebywania w tych pomieszczeniach;
3. Osoby opuszczające puste pomieszczenie, w którym przetwarzane są dane osobowe, zobowiązane są do zamknięcia drzwi na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie, za wyjątkiem sytuacji związanych z ochroną przeciwpożarową;
4. Zabrania się samowolnego dorabiania kluczy oraz ich wynoszenia poza siedzibę Spółki. Każdorazowa potrzeba dorobienia dodatkowego klucza lub kluczy winna być zgłoszona ABI, który wyraża na to zgodę oraz określa zasady wykonania raz posługiwania się kopią klucza/kluczy;
5. Po zakończeniu pracy pracownik zobowiązany jest wylogować się z systemu informatycznego, zamknąć okna w pomieszczeniu, umieścić materiały i dokumenty zawierające dane osobowe w szafach lub szufladach zamykanych na klucz, zgodnie z zasadą czystego biurka, czystej drukarki i czystej kopiarki (o ile takie urządzenia znajdują się w pomieszczeniu) zniszczyć w niszczarce wszystkie materiały zbędne w postaci błędnie utworzonej lub niepotrzebnej dokumentacji mającej krótkotrwałe znaczenie praktyczne, m.in. wydruków komputerowych i innych materiałów analogowych zawierających dane osobowe;

§ 29.

1. Udostępnianie drogą pocztową lub kurierską dokumentów i materiałów zawierających dane osobowe może odbywać się przesyłką rejestrowaną, a w przypadku danych zawartych na nośnikach magnetycznych, optycznych lub elektronicznych – przesyłką rejestrowaną za potwierdzeniem odbioru;
2. Pracownicy Spółki przygotowujący przesyłki, o których mowa w ust. 1 powinni dołożyć należytej staranności celem zabezpieczenia ich zawartości przed nieuprawnionym dostępem do ich zawartości osób trzecich;
3. W Spółce dopuszcza się stosowanie zabezpieczeń technicznych i organizacyjnych innych, niż wymienione w § 24-29.

§ 30.
Sprawdzenia.

1. Sprawdzenia zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznych regulacji obowiązujących w tym zakresie w Spółce dokonuje ABI we współpracy z Informatykiem w zakresie sprawdzeń dotyczących przetwarzania danych osobowych w systemie informatycznym. Odbiorcą sprawdzeń jest Administrator Danych Osobowych lub w określonych przypadkach GIODO;
2. ABI przeprowadza sprawdzenia w trybie sprawdzenia planowego, tj. według planu sprawdzeń, który określa przedmiot, zakres i termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania. Wzór planu sprawdzeń stanowi załącznik nr 18 do PBI;
3. W przypadku otrzymania informacji o naruszeniu bezpieczeństwa danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, ABI przeprowadza niezwłocznie sprawdzenie doraźne;
4. Sprawdzeniu podlega system informatyczny, w którym przetwarzane są dane osobowe, zabezpieczenia fizyczne i organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami prawnymi;
5. ABI przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan obejmuje co najmniej jedno sprawdzenie i jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu nim objętego;
6. Zbiory danych oraz system informatyczny służący do przetwarzania lub zabezpieczania danych osobowych są obejmowane sprawdzeniem co najmniej raz na pięć lat;
7. Dokumentowanie przez ABI czynności w toku sprawdzenia polega na tworzeniu materiałów w postaci papierowej lub elektronicznej w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i opracowania sprawozdania;
8. Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie, zgodnie z wytycznymi określnymi w art. 36c ustawy, które zawiera opis ustalonego stanu faktycznego podlegającego ocenie oraz analizę w zakresie przestrzegania przepisów o ochronie danych osobowych w odniesieniu do ustalonego stanu faktycznego. W sprawozdaniu ABI stwierdza, czy naruszone zostały przepisy o ochronie danych osobowych, a jeżeli tak, to jakie są planowane lub podjęte działania przywracające stan zgodny z prawem. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.
9. ABI przekazuje sprawozdanie ze sprawdzenia planowego do ADO nie później niż w terminie 30 dni od zakończenia sprawdzenia. Sprawozdanie ze sprawdzenia doraźnego przekazywane jest niezwłocznie po zakończeniu sprawdzenia.

§ 31.
Odpowiedzialność.

1. Za zapewnienie pracownikom warunków organizacyjnych mających na celu zapewnienie należytego bezpieczeństwa danych osobowych odpowiada Zarząd reprezentowany przez Prezesa w porozumieniu z osobami odpowiedzialnymi za poszczególne obszary działalności Spółki;

2. Administrator Bezpieczeństwa Informacji w porozumieniu z Informatykiem oraz osobami odpowiedzialnymi za poszczególne obszary działalności Spółki zapewnia bieżącą edukację pracowników dotyczącą zasad bezpieczeństwa danych osobowych

przetwarzanych w systemie informatycznym i systemie tradycyjnym oraz wnioskuje do ADO o szkolenia w tym zakresie;

3. Na pracownikach oraz osobach upoważnionych do przetwarzania danych osobowych, w zakresie ich uprawnień i odpowiedzialności, ciąży obowiązek dbałości o zabezpieczanie danych osobowych przed ich udostępnieniem, zabraniem, przetwarzaniem z naruszeniem ustawy przez osoby nieuprawnione oraz zmianą, uszkodzeniem, utratą lub zniszczeniem.

§ 32.

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z rozdziału 8 art. 49 – 54a ustawy o ochronie danych osobowych;
2. Odpowiedzialności karnej podlega każdy pracownik, który:
    1) przetwarza w zbiorze danych dane osobowe, do których nie jest upoważniony,
    2) przetwarza w zbiorze danych dane, których przetwarzanie jest zabronione,
    3) przetwarza w zbiorze danych dane niezgodne z celem stworzenia tego lub innych zbiorów,
    4) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
    5) nie zgłasza zbiorów danych podlegających rejestracji,
    6) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,
    7) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw;
3. Złamanie zasad Polityki Bezpieczeństwa Informacji stanowi incydent, o którym powinien być niezwłocznie powiadomiony ABI. O podjęciu działań naprawczych decyduje ADO na podstawie projektu działań opracowanego przez ABI. W przypadku wystąpienia incydentu związanego z przetwarzaniem danych osobowych w systemie informatycznym, projekt naprawczy opracowuje i przedstawia również Informatyk.
4. Łamanie zasad wynikających z niniejszej PBI może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych i może skutkować nałożeniem kary porządkowej na zasadach określonych w przepisach prawa pracy oraz procedurach wewnętrznych, w szczególności w przypadku osoby, która po stwierdzeniu naruszenia bezpieczeństwa danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie ABI;
5. Udokumentowane umyślne złamanie zasad określonych w PBI jest traktowane jako ciężkie naruszenie obowiązków pracowniczych uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia z winy pracownika.

Rozdział 4.
Ogólne warunki korzystania z systemu informatycznego.

§ 33.

1. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji przed ich nieuprawnionym przetwarzaniem;
2. Każdy Użytkownik systemu informatycznego stosowanego w Spółce do przetwarzania danych osobowych jest zobowiązany do zapoznania się z zasadami korzystania z tego systemu;
3. Korzystanie z funkcjonalności systemu informatycznego jest możliwe pod warunkiem nadania przez Informatyka uprawnień Użytkownika systemu informatycznego;
4. Szczegółowe procedury nadawania uprawnień do systemu informatycznego określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w MS Sp. z o.o. w Straszynie;

§ 34.

1. Zgodnie z postanowieniami niniejszej PBI, zabrania się Użytkownikowi systemu informatycznego podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń tego systemu;
2. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom;
3. Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika;
4. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora;
5. Użytkownik zobowiązany jest do przestrzegania zasady „czystego biurka”, w szczególności przed opuszczeniem swego stanowiska pracy powinien schować wszelkie dokumenty oraz informatyczne nośniki danych;
6. W czasie kopiowania, drukowania dokumentów zawierających dane osobowe, Użytkownik zobowiązany jest do zachowania zasady „czystej drukarki”, „czystej kopiarki”, w szczególności przed opuszczeniem stanowiska kopiowania/drukowania upewnić się, że w urządzeniach nie pozostały dokumenty zawierające dane osobowe;
7. Przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych z użyciem urządzeń mobilnych, Użytkownik jest zobowiązany do sprawdzenia, czy posiadane przez niego dane są należycie zabezpieczone przed dostępem osób nieupoważnionych;
8. Po zakończeniu przetwarzania danych osobowych, Użytkownik zobowiązany jest do należytego zabezpieczenia ich przed dostępem osób nieupoważnionych.

Rozdział 5.
Poczta elektroniczna.

§ 35.

1. Użytkownik zobowiązany jest do dbania o bezpieczeństwo poczty elektronicznej, w szczególności do używania silnego hasła dostępu, nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł oraz zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców;
2. Szczegółowe procedury korzystania z poczty elektronicznej oraz konfiguracji sprzętu komputerowego Użytkownika systemu informatycznego reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych MS Sp. z o.o. w Straszynie;

§ 36.

W stosunku do pozostałych informacji podlegających ochronie, przetwarzanych w związku z działalnością MS Sp. z o.o. w Straszynie, stosuje się zasady bezpieczeństwa określone w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2016 r., poz. 1167 ze zm.);

Rozdział 6.
Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych.

§ 37.

1. Ryzyko w zakresie bezpieczeństwa informacji, w tym danych osobowych, definiuje się jako prawdopodobieństwo wystąpienia zagrożeń i powstanie szkód, zniszczeń oraz przerw lub zakłóceń prawidłowego funkcjonowania systemu tradycyjnego oraz systemu informatycznego, w których przetwarzane są dane osobowe;
2. Zarządzanie ryzykiem jest procesem identyfikacji zasobów, odpowiadających im podatności i zagrożeń, oceny prawdopodobieństwa ich wystąpienia, wielkości potencjalnych strat oraz przeciwdziałania i określenia kryteriów akceptowalności ryzyka.
3. Zarządzanie ryzykiem obejmuje możliwie jak najszybszą identyfikację ryzyka związanego z planowanym działaniem, ocenę stopnia wpływu ryzyka na uzyskane wyniki lub cele oraz zastosowanie odpowiednich środków kontroli ryzyka;
4. Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, odnoszącym się do działalności MS Sp. z o.o. w Straszynie, dokonywany jest przez ABI we współpracy z osobami odpowiedzialnymi za poszczególne obszary działalności (właścicielami ryzyka) oraz Informatykiem w zakresie systemu informatycznego;
5. Narzędziem wsparcia w tym procesie jest Arkusz zarządzania ryzykiem w zakresie bezpieczeństwa danych osobowych zawierający ryzyka zidentyfikowane dla MS Sp. z o.o. w Straszynie, przy czym katalog zidentyfikowanych ryzyk jest zbiorem otwartym, który może ulegać zmianom w zależności od warunków funkcjonowania Spółki. Wzór arkusza stanowi załącznik nr 16 do PBI;

1. Pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko.
2. Lista możliwych do zastosowania mechanizmów kontroli redukujących ryzyko stanowi załącznik nr 17 do PBI. Lista nie stanowi zamkniętego katalogu mechanizmów i może

ulegać modyfikacjom dostosowanym do aktualnych warunków funkcjonowania Spółki;

3. Wypełnione arkusze zarządzania ryzykiem przekazywane są do ABI. Na ich podstawie ABI, w przypadku ryzyk dotyczących bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym w porozumieniu z Informatykiem, opracowuje roczne sprawozdania, które w postaci raportu o zidentyfikowanych ryzykach przekazuje ADO.

§ 38.

1. Niezależnie od corocznej oceny ryzyk, ABI przeprowadza ocenę ryzyk po każdorazowym wystąpieniu incydentu oraz każdorazowej zmianie mogącej wpływać na poziom ryzyka, w tym szczególnie zmianie struktury organizacyjnej, otoczenia dotyczącego realizacji umów z nowymi podmiotami, technologii, infrastruktury, pracowników, metod pracy, przepisów prawa;
2. Niezwłocznie po wystąpieniu incydentu, ABI przedstawia ADO wyniki oceny zidentyfikowanych ryzyk wraz z propozycjami działań korygujących i zapobiegawczych, do których należy w szczególności: określenie zadań do realizacji, zdefiniowanie odpowiedzialności, ram czasowych oraz propozycji zmian celem poprawy bezpieczeństwa informacji;
3. Na podstawie raportów i sprawozdań otrzymanych od ABI, ADO podejmuje ostateczną decyzję w zakresie realizacji działań zapewniających ochronę przetwarzanych informacji;
4. Do działań wskazanych w ust. 3 należy w szczególności:
    1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,
    2) utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
    3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
    4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,
    5) dokonanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4,
    6) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
        1) zagrożenia bezpieczeństwa informacji,
        2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
        3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,
    7) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
        1) monitorowanie dostępu do informacji,
        2) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
        3) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,

8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
10) zawieranie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
11) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
12) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
    1) dbałości o aktualizację systemu operacyjnego,
    2) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
    3) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
    4) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
    5) zapewnieniu bezpieczeństwa plików systemowych,
    6) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
    7) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
    8) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i PBI,
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w sposób, umożliwiający szybkie podjęcie działań korygujących,
14) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

§ 39.

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    1) próby naruszenia ochrony danych:
       - z zewnątrz - włamania do systemu, podsłuch, kradzież danych
       - z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych,
    2) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne,
    3) awarie sprzętu lub uszkodzenie oprogramowania,
    4) zabór sprzętu lub nośników z ważnymi danymi ,
    5) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
    6) usiłowanie zakłócenia działania systemu informatycznego;
2. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
    a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
    d) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

e) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
f) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania);

3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:
   a) zgłoszenia od Użytkowników,
   b) alarmy z systemów informatycznych,
   c) analizy incydentów,
   d) wyniki audytów / kontroli.

§ 40.

Każdy pracownik, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora Bezpieczeństwa Informacji lub Informatyka w sytuacjach dotyczących użytkowania systemu informatycznego. Zasady działania w takich przypadkach określa **tabela nr 1:**

Tabela nr 1. Zasady działania w przypadku zagrożenia lub naruszenia ochrony danych osobowych

Kod uchybienia lub zagrożenia	**Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne**	**Postępowanie w przypadku uchybienia lub zagrożenia**
W zakresie wiedzy:		
A 1.	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym. Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informacyjnej. Dopuszczenie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	Natychmiast przerwać rozmowę lub inną czynność prowadzoną do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Administratora Bezpieczeństwa Informacji.
W zakresie sprzętu i oprogramowania		
B 1.	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
B 2.	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z komputera do opuszczenia stanowiska. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
B 3.	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłem w sposób umożliwiający odczytanie. Niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
B 4.	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymieniona czynność, aby jej zaniechała. Wezwanie Administratora Systemów Informatycznych w celu odinstalowania programów. Sporządzić raport.

B 5.	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
W zakresie dokumentów i obrazów zawierających dane osobowe		
C 1.	Pozostawianie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
C 2.	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
C 3.	Wyrzucenie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
C 4.	Dopuszczenie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
C 5.	Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane. Sporządzić raport.
W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych		
D 1.	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonego. Sporządzić raport.
D 2.	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonego i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci		
E 1.	Dopuszczenie lub ignorowanie faktu, że osoby spoza administracji systemów informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić Administratora Systemów Informatycznych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
E 2.	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej centralnych lub węzłów sieci komputerowej osób spoza administracji systemów informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić tożsamość. Powiadomić Administratora Systemów Informatycznych i Administratora Bezpieczeństwa Informacji. Sporządzić raport.
Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych		
F 1.	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.

F 2.	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służących do przetwarzania danych osobowych.	Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
F 3.	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
F 4.	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Powiadomić niezwłocznie Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z Użytkownikiem		
G 1.	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.
G 2.	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem Użytkownika.	Powiadomić Administratora Bezpieczeństwa Informacji. Sporządzić raport.

§ 41.

1. W przypadku stwierdzenia wystąpienia zagrożenia, ABI prowadzi postępowanie wyjaśniające, w toku którego ustala zakres i przyczyny zagrożenia oraz jego potencjalne skutki, inicjuje ewentualne działania dyscyplinarne, rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości, dokumentuje prowadzone postępowania;
2. W przypadku stwierdzenia incydentu (naruszenia) ABI prowadzi postępowanie wyjaśniające, w toku którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   2) ustala osoby odpowiedzialne za naruszenie,
   3) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   4) dokumentuje prowadzone postępowania;
3. ABI jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Gdy stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa źródło powstania incydentu, zagrożenia lub słabości, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną;
4. ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

Rozdział 6.
Postanowienia końcowe

§ 42.

1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
2. Nad aktualnością Polityki Bezpieczeństwa Informacji w MS Sp. z o.o. w Straszynie czuwa ABI we współpracy z Informatykiem w zakresie przetwarzania danych osobowych w systemie informatycznym.