Załącznik Nr 1
do Zarządzenia
Prezesa Zarządu
Nr …..……/……
z dnia ……..

POLITYKA BEZPIECZEŃSTWA INFORMACJI w Przedsiębiorstwie Usługowo Handlowym PERFEKTA SP. Z O.O.

Zatwierdzam do stosowania

SPIS TREŚCI

Rozdział 1.
Postanowienia ogólne

§ 1.
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 Przedsiębiorstwo Usługowo Handlowe PERFEKTA SP. Z O.O. z siedzibą przy ul. Warszawskiej 2/c, 59-800 Lubań reprezentowana przez Prezesa Zarządu;
2. **Administrator Bezpieczeństwa Informacji (ABI)** - osoba fizyczna upoważniona przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem wymaganej prawem dokumentacji związanej z przetwarzaniem tych danych przez administratora. Po zmianie przepisów krajowych w związku z wejściem w życie Rozporządzenia ogólnego (RODO), funkcję Administratora Bezpieczeństwa Informacji pełni **Inspektor Ochrony Danych Osobowych (IOD);**
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. **Spółka** – Przedsiębiorstwo Usługowo Handlowe PERFEKTA SP. Z O.O.
6. **Administrator Systemów Informatycznych (ASI)** – osoba fizyczna wyznaczona przez Administratora Danych Osobowych, zajmująca się sprawowaniem ogólnego nadzoru nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym danych osobowych przetwarzanych w systemie informatycznym;
7. **GIODO –** Generalny Inspektor Ochrony Danych Osobowych – organ nadzorczy w stosunku do administratorów danych osobowych. Po zmianie przepisów krajowych w związku z wejściem w życie Rozporządzenia ogólnego (RODO) rolę organu nadzorczego przejmie **Urząd Ochrony Danych Osobowych** (UODO);
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9. **Identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
10. **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;

11. **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;
12. **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);
13. **Podatność** - luka (słabość), która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę;
14. **PBI / Polityka** – niniejszy dokument*;*
15. **Pracownik** – osoba fizyczna świadcząca na rzecz administratora 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 (t.j. Dz.U. z 2017r., poz. 1778);
16. **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;
17. **System informatyczny (system IT)** - zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
18. **System tradycyjny** - zespół procedur organizacyjnych, wyposażenia i środków trwałych związanych z mechanicznym przetwarzaniem informacji zawierających dane osobowe na nośnikach papierowych;
19. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
20. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
21. **Usługi świadczone drogą elektroniczną** – wszystkie usługi, których wykonanie następuje przez wysyłanie i odbieranie danych za pomocą systemów teleinformatycznych na indywidualne żądanie usługobiorcy (klienta), bez jednoczesnej obecności stron, transmitowanych za pośrednictwem sieci publicznych, zgodnie z Ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 r., Nr 144, poz. 1204 ze zmianami).
22. **Użytkownik** – każda osoba, która uzyskała upoważnienie od ADO do przetwarzania danych osobowych w systemie informatycznym, a także osoba upoważniona przez podmiot, z którym została podpisana umowa powierzenia przetwarzania danych osobowych;
23. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

24. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

§ 2.
Cel i zakres stosowania Polityki Bezpieczeństwa Informacji.

1. Polityka Bezpieczeństwa Informacji jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych w Przedsiębiorstwie Usługowo Handlowym PERFEKTA SP. Z O.O..
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 oraz pozostałych informacji podlegających ochronie;
3. Niniejsza Polityka została udostępniona każdej osobie mającej dostęp do danych osobowych przetwarzanych w Spółce w formie tradycyjnej (papierowej) oraz w systemie informatycznym;
4. Potwierdzeniem zapoznania się z postanowieniami niniejszego dokumentu jest złożenie pisemnego oświadczenia (załącznik nr 3 do Zarządzenia). Złożone oświadczenie winno być wpięte do akt osobowych pracownika lub dołączone do zawartej umowy cywilnoprawnej.

§ 3.

Niniejsza Polityka Bezpieczeństwa Informacji określa w szczególności:

1) prawa, obowiązki oraz granice dopuszczalnego zachowania osób przetwarzających dane osobowe, Użytkowników systemu IT i tradycyjnego, w których przetwarzane są dane osobowe oraz konsekwencje naruszenia przepisów o ochronie danych osobowych wymienionych w § 1 ust. 1-8;

2) sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne 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;

4) wymagania w zakresie odnotowywania udostępniania danych osobowych;

5) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych;

6) instrukcję bezpiecznego przetwarzania danych osobowych w systemie IT.

§ 4.

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, 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 (ABI). Inspektor Ochrony Danych Osobowych (IOD). Administrator Systemów Informatycznych (ASI).

§ 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 niniejszej Polityce;
3. Administrator Danych Osobowych powołuje Administratora Bezpieczeństwa Informacji (ABI) zgodnie z ustawą o ochronie danych osobowych oraz Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku (Dz.U., poz. 1934);
4. W przypadku niepowołania ABI, funkcje mu przypisane ADO pełni w zakresie zgodnym z obowiązującymi przepisami;
5. Po zmianie przepisów krajowych w związku z wejściem w życie Rozporządzenia ogólnego (RODO), Administrator Danych Osobowych powierza obowiązki ABI Inspektorowi Ochrony Danych Osobowych (IOD) na zasadach określonych w przepisach prawa.

§ 6.

Zadania nałożone na Administratora Danych Osobowych ustawą o ochronie danych osobowych oraz RODO obejmują ponadto:

1) rzetelne i przejrzyste wypełnienie obowiązku informacyjnego;
2) wykazanie, że zastosowane środki techniczne i organizacyjne zapewniają należyty poziom ochrony danych osobowych oraz, że dane osobowe przetwarzane są zgodnie z zasadami zgodności z prawem, ograniczenia, minimalizacji danych, prawidłowości,

ograniczenia przechowywania, integralności i poufności i prawidłowości przetwarzania danych osobowych;
3) dokonywanie oceny ryzyka naruszenia praw i wolności osób, których dane osobowe są przetwarzane z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych. Ocena ryzyka jest konieczna dla wdrożenia przez Przedsiębiorstwo Usługowo Handlowe PERFEKTA SP. Z O.O. właściwych środków technicznych, zapewniających bezpieczeństwo przetwarzanych danych osobowych;
4) nadawanie i anulowanie upoważnień do przetwarzania danych osobowych,
5) dbałość o ochronę danych osobowych już na etapie projektowania wdrażanych rozwiązań związanych z przetwarzaniem danych,
6) prowadzenie rejestru czynności przetwarzania danych osobowych, zgodnie z wzorem stanowiącym załącznik nr 16 do PBI);
7) zgłaszanie do organu nadzorczego faktu naruszenia ochrony danych osobowych, nie później niż po upływie 72 godzin.

§ 7.
Administrator Bezpieczeństwa Informacji (ABI)

Administrator Bezpieczeństwa Informacji (ABI) jest powoływany przez Administratora danych Osobowych 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).

§ 8.

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
   3) współpraca z ASI w zakresie dotyczącym przetwarzania danych osobowych w systemie informatycznym,
   4) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych, środki ich ochrony oraz przestrzegania zasad w niej określonych,
   5) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   6) 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,
   7) we współpracy z ADO, nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób,
   8) zapewnienie przeciwdziałania incydentom oraz prowadzenie rejestru incydentów i zagrożeń (załącznik nr 10 do PBI),
   9) zapewnienie edukacji pracowników (w tym Użytkowników systemu IT) na temat zasad ochrony danych osobowych i polityki bezpieczeństwa informacji

stosowanej w Spółce poprzez wnioskowanie do ADO o systematyczne szkolenia w tym zakresie oraz bieżące monitorowanie poziomu wiedzy pracowników, np. poprzez cykliczne przeprowadzanie testów sprawdzających (przynajmniej raz w roku);

§ 9.

1. Administrator Bezpieczeństwa Informacji prowadzi jawny rejestr zbiorów danych osobowych (załącznik nr 20) przetwarzanych na potrzeby realizacji celów i zadań Spółki, wykaz charakteryzujący sposób przepływu danych osobowych pomiędzy systemami informatycznymi (załącznik nr 2) oraz rejestr czynności przy przetwarzaniu danych osobowych (załącznik nr 15);
2. W ramach nadzoru nad przetwarzaniem danych osobowych, ABI sprawdza cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia tych danych, w tym w porozumieniu z ASI, zabezpieczenia urządzeń mobilnych wykorzystywanych w Spółce;
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 Spółki z wykorzystaniem urządzeń mobilnych. Dokumentację analizy ABI przedstawia ADO w celu dokonania oceny ryzyka i podjęcia stosownych działań;
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 umów powierzenia oraz podmiotów, którym powierzono dane osobowe (załącznik nr 8 do PBI) oraz wykazu udostępnień danych osobowych osobom, których dane dotyczą (załącznik nr 9 do PBI);

§ 10.
Inspektor Ochrony Danych Osobowych (IOD)

1. Po zmianie przepisów krajowych w związku z wejściem w życie Rozporządzenia ogólnego (RODO) funkcje Administratora Bezpieczeństwa Informacji pełni Inspektor Ochrony Danych Osobowych (DPO);
2. Inspektor Ochrony Danych Osobowych to osoba wyznaczona przez ADO na podstawie upoważnienia (załącznik nr 5 do PBI), która w Spółce zajmuje się doradzaniem w sprawie zasad ochrony danych osobowych oraz monitorowaniem działań administratora danych w tym zakresie;
3. Zadania IOD może pełnić osoba powołana przez Administratora Danych Osobowych spośród pracowników Spółki lub osoba z zewnątrz na podstawie umowy o świadczenie usług – outsourcing (art. 37 ust. 6 RODO);
4. Zadania IOD wynikające z art. 39 RODO obejmują:
    1) informowanie administratora oraz pracowników o obowiązkach spoczywających na nich na mocy przepisów prawa,
    2) monitorowanie przestrzegania przepisów krajowych oraz Unii i państw członkowskich oraz polityk administratora lub procesora,
    3) szkolenie personelu uczestniczącego w operacjach przetwarzania danych osobowych,
    4) przeprowadzanie systematycznych audytów wewnętrznych,

5) udzielanie wskazówek Administratorowi Danych Osobowych w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych jak również organizacyjnych mających zabezpieczyć dane osobowe,
6) udzielanie wskazówek Administratorowi Danych Osobowych, jak wykazać przestrzeganie prawa w zakresie identyfikowania ryzyka związanego z przetwarzaniem danych osobowych, jego oceny pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz w zakresie najlepszych praktyk pozwalających zminimalizować to ryzyko,
7) udzielanie zaleceń w zakresie oceny skutków oraz monitorowanie ich wykonania w przypadku, gdy administrator danych przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych,
8) utrzymywanie stałej współpracy z organem nadzorczym,
9) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
10) prowadzenie rejestru czynności przy przetwarzaniu danych osobowych, za które odpowiada administrator danych i rejestru kategorii czynności przetwarzania danych dokonywanych w imieniu administratora przez podmiot przetwarzający (załącznik nr 15 do PBI).

§ 11.

Spółka, jako Administrator Danych Osobowych, gwarantuje IOD niezależność oraz podległość najwyższemu kierownictwu tak, aby IOD mógł bezpośrednio kontaktować się z osobami decyzyjnymi w sprawie przetwarzania danych osobowych oraz mieć dostęp do wszystkich informacji, które związane są z przetwarzaniem danych osobowych w Spółce.

§ 12.

IOD jest właściwie i niezwłocznie angażowany we wszystkie sprawy dotyczące ochrony danych osobowych przetwarzanych w Spółce, tzn. uczestniczy we wszystkich pracach, które mogą wpływać na kształt operacji związanych z przetwarzaniem danych osobowych w u (art. 35 ust. 2 RODO).

§ 13.
Administrator Systemów Informatycznych.

1. Do zadań ASI należy zapewnienie działania infrastruktury teleinformatycznej i oprogramowania w sposób zapewniający właściwy poziom bezpieczeństwa informacji wynikający z obowiązujących przepisów, PBI oraz zaleceń ABI (IOD);
2. Nadzorowanie przez ASI przestrzegania bezpieczeństwa danych osobowych gromadzonych i przetwarzanych w systemie 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 ASI należy w szczególności:
   1) zapewnienie właściwego poziomu bezpieczeństwa systemu informatycznego, w tym danych osobowych w nim przetwarzanych,

2) zapewnienie mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych oraz kontrola dostępu do tych danych,
3) inicjatywa w zakresie zapewnienia alternatywnego, awaryjnego zasilania systemu informatycznego oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, w tym raportowanie do ABI (IOD) stanu zabezpieczeń w zakresie centralnego awaryjnego zasiania 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 tego systemu,
6) zapewnienie ochrony danych osobowych w związku z naprawą, konserwacją oraz likwidacją systemu informatycznego, w tym urządzeń komputerowych i mobilnych, 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 informatycznym oraz realizacja tych czynności po akceptacji ADO,
8) zapewnienie przeglądów, konserwacji oraz uaktualnień systemu służącego do przetwarzania danych osobowych z uwzględnieniem specyfiki funkcjonowania 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.

§ 14.
Zasady przetwarzania danych osobowych.

1. Spółka gromadzi dane osobowe swoich pracowników, kandydatów do pracy, klientów, zleceniobiorców, kontrahentów i podmiotów współpracujących (dostawców, usługodawców itp.);

2. Spółka pozyskuje dane osobowe osób, o których mowa w ust. 1 na dwa sposoby:

   1) bezpośrednio od osoby, której dane dotyczą,

   2) z wykorzystaniem innych źródeł niż osoba, której dane dotyczą, w granicach dopuszczalnych przepisami prawa;

3. Spółka przetwarza dane osobowe w sposób adekwatny, stosowny oraz ograniczony do tego, co jest niezbędne w celu realizacji usługi;

4. Wszystkie osoby upoważnione do przetwarzania danych osobowych Przedsiębiorstwo Usługowo Handlowe PERFEKTA SP. Z O.O. są zobowiązane do zachowania w tajemnicy tych danych poprzez złożenie oświadczenia o zachowaniu poufności (załącznik nr 4) nawet po ustaniu zatrudnienia, zakończenia współpracy, wygaśnięciu umowy itd.

§ 15.

1. Uprawnienia do przetwarzania danych osobowych w systemie IT nadawane są zgodnie z właściwą procedurą określoną w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Przedsiębiorstwo Usługowo Handlowe PERFEKTA SP. Z O.O. Uprawnienia, o których mowa w zdaniu pierwszym, ważne są do dnia odwołania lub do chwili ustania zatrudnienia uprawnionego pracownika;

2. Ochrona dotyczy w szczególności:

   1) danych osobowych gromadzonych i przetwarzanych w związku z działalnością Spółki, w tym danych osobowych podmiotów współpracujących 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.
3. Katalog przetwarzanych danych osobowych może ulec rozszerzeniu, w zależności od bieżącej działalności Spółki, niemniej musi mieścić się w granicach zgodnych przepisami prawa.

§ 16.

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

§ 17.

Wszystkie osoby, które posiadają dostęp do danych osobowych w obszarze wymienionym w § 14 ust. 2 pkt 2 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.

§ 18.

1. W zbiorach danych gromadzonych w systemie informatycznym **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);

§ 19.
Profilowanie danych osobowych.

1. Profilowanie polega na automatycznym przetwarzaniu danych osobowych, dopuszczalnym pod warunkiem spełnienia przesłanek określonych przepisami prawa;
2. W przypadku profilowania danych osobowych w związku z działalnością Spółki zabrania się używania danych wymienionych w § 16, chyba, że wymagają tego obowiązujące przepisy prawa, osoba, której dane dotyczą wyraziła na to zgodę, jest to podyktowane ważnym interesem publicznym;
3. Przy profilowaniu danych Spółki, jako Administrator Danych Osobowych, obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą;
4. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą;
5. Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

§ 20.
Powierzenie przetwarzania danych osobowych.

1. 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;

2. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy podmiotów współpracujących lub świadczących usługi na rzecz Spółki (procesorów) w zakresie adekwatnym do celu powierzenia;

3. Umowa powierzenia danych osobowych określa przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą oraz 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. Szczegółowy zakres praw i obowiązków procesorów określono w dokumencie o nazwie Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów

współpracujących z Przedsiębiorstwem Usługowo Handlowym PERFEKTA SP. Z O.O.

5. Administrator Danych Osobowych zobowiązany jest do dokumentowania powierzania tych danych w postaci wykazu umów powierzenia oraz 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.

§ 21.
Udostępnianie danych osobowych.

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której Spółka, jako administrator udostępniający dane, oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności;
2. Spółka 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.

§ 22.
Obowiązek informacyjny.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, Spółka, jako Administrator Danych Osobowych, 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 oraz danych kontaktowych do ABI (nr tel., e-mail) / Inspektorze Ochrony Danych Osobowych od chwili przejęcia obowiązków ABI;
   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, Spółka jest zobowiązana 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.

§ 23.
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.

§ 24.

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.

§ 25.
Zabezpieczenia danych osobowych.

1. W celu zapewnienia należytej ochrony przetwarzania danych osobowych, w Spółce zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych typu hasła i loginy, zamki i karty dostępu, szafy i szafki zamykane na klucz, procedury postępowania, wyznaczone godziny i dni pracy, automatyczne wylogowywanie z systemu, dostęp do określonych zasobów sieci, upoważnienia, rejestry, audyty, przeglądy itp.
2. Pracownicy oraz pozostałe osoby posiadające dostęp do danych osobowych są zobowiązane do przestrzegania zasad zabezpieczania pomieszczeń i urządzeń w strefach stanowiących obszar przetwarzania danych osobowych.

§ 26.
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 są zabezpieczone przed skutkami pożaru za pomocą instalacji przeciwpożarowej;
3. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce;
4. W przypadku wystąpienia konieczności dostępu do zbioru danych osobowych w czasie nieobecności pracownika upoważnionego do przetwarzania danych w tym zbiorze, ABI (IOD), w porozumieniu z ASI 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;
5. Z każdego zdarzenia opisanego w ust. 3 niniejszego paragrafu, ABI (IOD) sporządza Raport, w którym podaje: imiona i nazwiska osób zastępujących nieobecnego pracownika;
6. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
7. Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych;
8. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 27.
Zabezpieczenia organizacyjne.

1. Opracowano i wdrożono Politykę Bezpieczeństwa Informacji w Przedsiębiorstwie Usługowo Handlowym PERFEKTA SP. Z O.O.;
2. Wyznaczono ASI, który sprawuje nadzór nad przetwarzaniem danych osobowych w systemie informatycznym;
3. Powołano Administratora Bezpieczeństwa Informacji, który sprawuje nadzór nad zgodnością przetwarzania danych osobowych z obowiązującymi w tym zakresie

przepisami oraz realizuje obowiązki opisane w § 9 i 10 niniejszego dokumentu. Po zmianie przepisów krajowych w związku z wejściem w życie Rozporządzenia ogólnego (RODO) rolę i zadania ABI pełni Inspektor Ochrony Danych Osobowych (IOD);

4. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony tych danych;

5. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych w systemie informatycznym (Użytkownicy systemu) zostały przeszkolone w zakresie zasad korzystania i zabezpieczeń tego systemu;

6. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych 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 z obszarem przetwarzania danych;

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. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w zabezpieczonych pomieszczeniach (zamki na klucz, karty zbliżeniowe);

11. 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.

§ 28.

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 określa jednocześnie zakres odpowiedzialności tej osoby za ochronę przetwarzanych danych osobowych w stopniu adekwatnym do jej zadań na stanowisku pracy;

§ 29.

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

§ 30.

1. ADO w porozumieniu z ABI oraz ASI może określić pomieszczenia, do których dostęp osób sprzątających będzie ograniczony i możliwy tylko pod nadzorem osób uprawnionych do przebywania w tych pomieszczeniach;
2. 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;
3. Zabrania się samowolnego dorabiania kluczy oraz ich wynoszenia poza siedzibę Spółki. Każdorazowa potrzeba dorobienia dodatkowego klucza lub kluczy winna być zgłoszona ABI (IOD), który wyraża na to zgodę oraz określa zasady wykonania raz posługiwania się kopią klucza/kluczy;
4. 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;

§ 31.

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. W Spółce dopuszcza się stosowanie zabezpieczeń organizacyjnych i technicznych innych, niż wymienione w § 23-29.

§ 32.
Sprawdzenia.

1. Sprawdzenia zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi regulacjami obowiązującymi w tym zakresie w Spółce dokonuje ABI (IOD) we współpracy z ASI w zakresie sprawdzeń dotyczących przetwarzania danych osobowych w systemie informatycznym. Odbiorcą sprawdzeń jest Administrator Danych Osobowych lub w określonych przypadkach organ nadzorczy;
2. ABI (IOD) 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 17 do PBI;
3. W przypadku otrzymania informacji o naruszeniu bezpieczeństwa danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, ABI (IOD) 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 (IOD) 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 (IOD) 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 (IOD) 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 (IOD) 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 (IOD) 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.

§ 33.
Odpowiedzialność.

1. Za zapewnienie pracownikom warunków organizacyjnych i technicznych mających na celu zapewnienie należytego bezpieczeństwa danych osobowych odpowiada Administrator Danych Osobowych w porozumieniu z osobami odpowiedzialnymi za poszczególne komórki organizacyjne Spółki;

2. ABI (IOD) w porozumieniu z ASI oraz osobami odpowiedzialnymi za poszczególne komórki organizacyjne Spółki odpowiada za zapewnienie bieżącej edukacji pracowników dotyczącej 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.

§ 34.

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z rozdziału 8 art. 49 – 54a ustawy o ochronie danych osobowych oraz RODO;

2. Odpowiedzialności karnej podlega każda osoba w Spółce, która:
   1) przetwarza w zbiorze danych dane osobowe, do których nie jest upoważniona,
   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 (IOD). O podjęciu działań naprawczych decyduje ADO na podstawie projektu działań opracowanego przez ABI (IOD).
   W przypadku wystąpienia incydentu związanego z przetwarzaniem danych osobowych w systemie informatycznym, projekt naprawczy opracowuje i przedstawia także ASI.
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 (IOD);
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. Konfiguracja sprzętu informatycznego użytkownika systemu. Procedury nadawania uprawnień. Poczta elektroniczna. Procedury niszczenia nośników danych.

§ 35.
Zasady korzystania z systemu informatycznego.

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Priorytetowe jest zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemów informatycznych stosowanych w Spółce;
2. Istotnym elementem osiągnięcia celu, o którym mowa w ust. 1 jest zapewnienie odpowiedniego poziomu kontroli dostępu:

1) do sieci, w tym urządzeń serwerowych,
2) do systemów operacyjnych,
3) do aplikacji,
4) do informacji i zbiorów danych, wraz z określeniem trybu dostępu.

3. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji przed ich nieuprawnionym przetwarzaniem;
4. Każdy Użytkownik systemu informatycznego stosowanego w Spółce jest zobowiązany do zapoznania się z zasadami korzystania z tego systemu;
5. Ze względu na fakt, że użytkowane w Spółce programy informatyczne służące do przetwarzania danych osobowych są połączone z siecią Internet, wprowadza się **wysoki poziom bezpieczeństwa**;
6. Korzystanie z funkcjonalności systemu informatycznego jest możliwe pod warunkiem nadania przez ASI uprawnień Użytkownika systemu informatycznego;
7. Szczegółowe procedury nadawania uprawnień do systemu informatycznego reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Przedsiębiorstwie Usługowo Handlowym PERFEKTA SP. Z O.O..

§ 36.

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 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

§ 37.

Konfiguracja sprzętu komputerowego Użytkownika systemu.

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych oraz logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym kontroli przepływu informacji pomiędzy system a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu;

1. Każdy dostęp do danych osobowych jest zarejestrowany;
2. Urządzenie mobilne (laptop, tablet itp.) zawierające dane osobowe jest zabezpieczone przed nieuprawnionym dostępem;
3. Minimalne środki ochrony to:
   1) zainstalowanie na stacjach zapory sieciowej firewall i oprogramowania antywirusowego,
   2) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników,
   3) wymaganie podania hasła przed uzyskaniem dostępu do systemu operacyjnego,
   4) niepozostawianie niezablokowanych stacji roboczej bez nadzoru,
   5) praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.
4. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej oraz na urządzeniach mobilnych i reagowania na nie;

5. W przypadku niesprawdzenia przez Użytkownika systemu pliku dostarczonego z zewnątrz, oprogramowanie antywirusowe automatycznie chroni system poprzez monitorowanie plików w stanie rzeczywistym. W przypadku wykrycia zagrożenia, oprogramowanie stosownie reaguje na to zagrożenie
6. Wygaszacze ekranu systemowo ustawiane są na aktywację po 10 minutach bezczynności na danej stacji roboczej oraz w razie potrzeby (np. opuszczenie miejsca przetwarzania danych) skrótem klawiaturowym;
7. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej.

§ 38.

Procedury nadawania uprawnień.

1. Dostęp do systemu informatycznego służącego do przetwarzana danych osobowych może uzyskać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez ADO (załącznik nr 3 do PBI), która podpisała oświadczenie o zachowaniu poufności (załącznik nr 4 do PBI);
2. Uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych nadaje ASI na wniosek osoby odpowiedzialnej za daną komórkę

organizacyjną Spółki;

3. Uprawnienia, o których mowa w ust. 2 określają poziom dostępu do sieci, w tym urządzeń serwerowych, do systemów operacyjnych, do aplikacji i informacji;
4. Po nadaniu uprawnień w systemie informatycznym, ASI przydziela Użytkownikowi login i hasło tymczasowe. Hasło tymczasowe Użytkownik zmienia na własne przy pierwszym logowaniu;
5. Hasło Użytkownika musi się składać co najmniej z 8 znaków, w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne**,** nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr, nie może zawierać imion, nazwisk, przezwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione, nie może być zapisywane w systemie w postaci jawnej**,** nie może być wyświetlane na ekranie komputera w sposób jawny**,** nie może być ujawnione innej osobie, nawet po utracie ważności**,** musi być zabezpieczone przez Użytkownika przed nieuprawnionym dostępem osób trzecich;
6. W przypadku 5-krotnego wprowadzenia błędnych danych (login, hasło), dostęp zostanie zablokowany na 10 minut. Po upływie 10 minut, Użytkownik może ponownie podjąć czynności zalogowania się. W przypadku nieodblokowania systemu, należy niezwłocznie zawiadomić ASI;
7. W przypadku zapomnienia przez Użytkownika konstrukcji hasła, winien on niezwłocznie zawiadomić ASI, który nadaje nowe hasło, postępując zgodnie z procedurą obowiązującą przy nadawaniu uprawnień dostępu do systemu informatycznego;
8. ASI dokonuje rejestracji i prowadzi wykaz loginów przydzielonych poszczególnym Użytkownikom, który wiąże loginy z imiennie wskazanymi osobami;
9. Użytkownikom nadawane są uprawnienia do prac tylko w modułach i funkcjach programu wymaganych dla realizacji powierzonych im zadań*;*
10. Użytkownik systemu informatycznego ponosi odpowiedzialność za bezpieczeństwo danych osobowych przetwarzanych we wszystkich operacjach wykonanych przy użyciu jego loginu i hasła dostępu;
11. W przypadku wygaśnięcia przesłanek uprawniających Użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia do ich przetwarzania, ASI przy współpracy z ABI (IOD) zobowiązany jest do wyrejestrowania Użytkownika z systemu informatycznego, do którego był uprawniony;
12. Wyrejestrowanie Użytkownika z ewidencji osób upoważnionych do przetwarzania informacji następuje poprzez zablokowanie go we wszystkich opcjach systemu informatycznego, do których miał dostęp.

§ 39.
Poczta elektroniczna.

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 zasady korzystania z poczty elektronicznej reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Przedsiębiorstwie Usługowo Handlowym PERFEKTA SP. Z O.O..

§ 40.
Procedura niszczenia danych na nośnikach elektronicznych.

1. W odniesieniu do nośników przenośnych (pen-drive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
   1) za pomocą specjalistycznego oprogramowania,
   2) przy użyciu demagnetyzacji,
   3) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników;
2. ASI dokonuje kontroli prawidłowości usunięcia informacji;
3. Nośniki elektroniczne, które nie mogą być ponownie wykorzystane, są niszczone mechanicznie lub oddawane do utylizacji przez firmę specjalistyczną;
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada Użytkownik;
5. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada ASI;
6. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia (załącznik nr 19 do PBI)

Rozdział 5.
Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych.

§ 41.

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 zawierających dane osobowe, odnoszącym się do działalności Spółki, dokonywany jest przez ABI (IOD) we współpracy z osobami odpowiedzialnymi za poszczególne komórki organizacyjne oraz z ASI w zakresie systemu informatycznego;
5. 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;
6. ABI (IOD) w porozumieniu z ASI w przypadku ryzyk dotyczących bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym, opracowuje roczne sprawozdania, które w postaci raportu o zidentyfikowanych ryzykach przekazuje ADO.

§ 42.

1. Niezależnie od corocznej oceny ryzyk, Administrator Danych Osobowych na podstawie informacji od ABI (IOD) dokonuje ich oceny 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 (IOD) przedstawia ADO do oceny zidentyfikowane ryzyka oraz propozycje działań korygujących i zapobiegawczych;
3. Na podstawie raportów i sprawozdań otrzymanych od ABI (IOD), ADO podejmuje ostateczną decyzję w zakresie realizacji działań zapewniających ochronę przetwarzanych informacji;
4. Do działań ADO 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 zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, 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 monitorowanie dostępu do informacji, czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, 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:
      a) dbałości o aktualizację systemu operacyjnego,
      b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
      c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnieniu bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) 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 lub zewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

§ 43.

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:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
   4) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasiania, utrata łączności),
   5) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   6) 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:
   1) zgłoszenia od Użytkowników,
   2) alarmy z systemów informatycznych,
   3) analizy incydentów,
   4) wyniki audytów / kontroli.

§ 44.

Każda osoba posiadająca dostęp do danych osobowych, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony tych danych, zobowiązana jest poinformować Administratora Bezpieczeństwa Informacji lub ASI w sytuacjach dotyczących użytkowania systemu informatycznego. Zasady działania w takich przypadkach określa **tabela nr 1:**

Tabela nr 1. Zasady działania w przypadku zagrożenia bezpieczeństwa danych osobowych

Kod uchybienia lub zagrożenia	Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych		
A1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru	Należy zabezpieczyć dane osobowe oraz powiadomić ABI (IOD), który powiadamia ADO. ABI (IOD) sporządza Protokół uchybienia (załącznik nr 12 do PBI)
A2	Dostęp do danych mają osoby nieupoważnione	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI (IOD), który powiadamia ADO i sporządza Protokół uchybienia.
A3	Próba kradzieży danych osobowych w formie papierowej	Należy nie dopuścić do kradzieży danych osobowych i powiadomić ABI (IOD), który powinien zabezpieczyć dane i powiadomić ADO. ABI (IOD), powiadamia ADO i sporządza Protokół zagrożenia.
A4	Nieuprawniony dostęp do danych osobowych w formie papierowej	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI (IOD), który sporządza Protokół uchybienia i powiadamia ADO.
A5	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Należy powiadomić ABI, który powinien zabezpieczyć pomieszczenie, powiadomić ADO i sporządzić Protokół uchybienia.
A6	Próba włamania do pomieszczenia/ budynku	Należy zabezpieczyć dowody i powiadomić ABI (IOD), który sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI (IOD), powiadamia ADO i sporządza protokół zagrożenia (załącznik nr 13 do PBI).
A7	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Należy zabezpieczyć dowody i powiadomić ABI (IOD), który sprawdza stan uszkodzeń, zabezpiecza dowody, powiadamia ADO oraz sporządza protokół zagrożenia.
A8	Wyrzucenie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie	Należy zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić ABI (IOD) oraz przełożonych. ABI (IOD), sporządza Protokół zagrożenia.
W zakresie przetwarzania danych osobowych w systemie informatycznym		
B1	Komputer nie jest zabezpieczony hasłem	Należy zabezpieczyć dane osobowe oraz powiadomić ASI i ABI (IOD),, który powiadamia ADO i sporządza Protokół uchybienia.
B2	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Należy powiadomić ASI i ABI (IOD), który we współpracy z ASI powinien sprawdzić system uwierzytelniania oraz sprawdzić, czy nie doszło do kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, ABI (IOD) powiadamia ADO i sporządza Protokół uchybienia.

B3	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Należy nie dopuścić do kradzieży danych i powiadomić ABI (IOD) i ASI. ASI w porozumieniu z ABI (IOD), powinien zabezpieczyć nośnik danych i powiadomić ADO. ABI (IOD), sporządza Protokół zagrożenia.
B4	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy zawiadomić ASI i ABI (IOD). ASI powinien przeprowadzić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych i firewall. ASI przekazuje wynik audytu ABI (IOD), który powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia. ABI (IOD) powiadamia ADO.
B11	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić ASI. ASI powinien zaktualizować lub nabyć oprogramowanie antywirusowe i powiadomić ABI (IOD), który powiadamia ADO i sporządza Protokół uchybienia.
B13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym	Należy zabezpieczyć dowody i powiadomić ASI. ASI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ABI (IOD), który powiadamia ADO i sporządza Protokół zagrożenia.
B14	Uszkodzenie komputerów, nośników danych	Należy powiadomić ABI (IOD), który w porozumieniu z ASI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. ABI (IOD) powiadamia ADO i sporządza Protokół zagrożenia.
B15	Próba nieprawidłowej interwencji przy sprzęcie komputerowym	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI, który powiadamia ABI (IOD), który powiadamia ADO i sporządza Protokół uchybienia.
W zakresie zdarzeń niezależnych od działalności człowieka		
C16	Zdarzenia losowe (powódź, pożar, zalanie itp.)	ABI (IOD) powoduje oszacowanie strat, powiadamia ADO i sporządza Protokół zagrożenia lub uchybienia.

Źródło: opracowanie własne

§ 45.

1. W przypadku stwierdzenia wystąpienia zagrożenia, ABI (IOD) 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 incydentów naruszenia bezpieczeństwa danych osobowych ABI (IOD) 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 (IOD) 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 (IOD) 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.

§ 46.

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 Przedsiębiorstwie Usługowo Handlowym PERFEKTA SP. Z O.O. czuwa Administrator Bezpieczeństwa Informacji (Inspektor Ochrony Danych Osobowych) we współpracy z ASI w zakresie przetwarzania danych osobowych w systemie informatycznym.