

**POLITYKA**

**OCHRONY DANYCH OSOBOWYCH**

**W PRZEDSIĘBIORSTWIE**

**MEBLOBUK s.j.**

**HANNA I ZDZISŁAW BUKOWIEC**

Skórzewo, 2018

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

## SPIS TREŚCI

§ 1 Definicje.

§ 2 Zasady ogólne.

§ 3 Przetwarzanie zgodne z prawem.

§ 4 Obowiązek informacyjny.

§ 5 Podmiot przetwarzający.

§ 6 Rejestr czynności przetwarzania.

§ 7 Zgłoszenie naruszeń.

§ 8 Zabezpieczenie dostępu do Danych osobowych.

§ 9 Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 10 Identyfikacja ról w procesie zarządzania bezpieczeństwem.

§ 11 Procesy zarządzania Bezpieczeństwem Systemów.

## § 1.

### DEFINICJE

1. **Specjalista Ochrony Danych (Specjalista)** - osoba wyznaczona przez Administratora zgodnie z zasadami reprezentacji, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w Przedsiębiorstwie. W przypadku, jeżeli Administrator nie wyznaczył osoby Specjalisty, funkcję tę pełni sam Administrator.
2. **Administrator** - w świetle art. 4 pkt 7 Rozporządzenia rozumie się przez to ME-BLOBUK Hanna i Zdzisław Bukowiec, prowadzący Przedsiębiorstwo.
3. **Specjalista ds. Systemu Informatycznego (Specjalista ds. Systemu)** - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń Systemu służącego do przetwarzania danych osobowych w Przedsiębiorstwie.
4. **Analiza ryzyka** - proces identyfikacji ryzyka, określania jego wielkości i identyfikowania obszarów wymagających zabezpieczeń.
5. **Przedsiębiorstwo** – zorganizowany zespół składników niematerialnych i materialnych przeznaczony do prowadzenia działalności gospodarczej przez Administratora.
6. **Bezpieczeństwo Systemu** - wdrożenie przez Specjalistę lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
7. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określa-

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

jących fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

8. **Hasło** – specjalny, tajny ciąg znaków umożliwiający uwierzytelnienie Użytkownika w Systemie oraz jego logowanie do Systemu.
9. **Identyfikator** – nazwa Użytkownika w Systemie, umożliwiająca jego logowanie do Systemu.
10. **Kopia bezpieczeństwa** – kopia oprogramowania lub danych, pozwalająca na ich dokładne odtworzenie w wypadku utraty oryginału.
11. **Monitorowanie** – ciągle, aktywne sprawdzanie zgodności stanu faktycznego z zasadami umiejscowionymi w niniejszym Dokumencie.
12. **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Specjalistę i dopuszczona jako Użytkownik do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu. Listę Osób upoważnionych prowadzi Specjalista.
13. **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez Specjalistę do wykonywania w jego imieniu określonych czynności.
14. **Przetwarzanie** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
15. **Rozporządzenie** - Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
16. **Ryzyko** – prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenia zasobów
17. **Stacja robocza** – stacjonarne lub przenośne urządzenie wchodzący w skład lub połączone z Systemem, umożliwiające Użytkownikom dostęp do danych osobowych znajdujących się w Systemie.

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

18. **System** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych wykorzystywany, w jakimkolwiek zakresie, do przetwarzania Danych osobowych.
19. **Usunięcie Danych** – zniszczenie/ usunięcie Danych osobowych lub taka ich modyfikacja, która nie pozwoli na identyfikację (w tym również w przyszłości) tożsamości osoby, której dane dotyczą.
20. **Uwierzytelnianie** – proces pozwalający na jednoznaczną identyfikację Użytkownika w Systemie.
21. **Użytkownik** - osoba posiadająca uprawnienia do przetwarzania Danych osobowych w Systemie.
22. **Zarządzanie ryzykiem** – całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia pewnych zdarzeń, które mogą mieć wpływ na Dane osobowe.
23. **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.

### ZASADY OGÓLNE

1. Specjalista jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację niniejszego Dokumentu, standardów, zaleceń oraz procedur w Przedsiębiorstwie.
2. Podstawowym zadaniem niniejszego Dokumentu jest opis standardu Bezpieczeństwa Systemu i sieci teleinformatycznych służących do przetwarzania danych, w szczególności Danych osobowych, opis obiektów i zasobów podlegających przepisom Rozporządzenia. Dokument ten ustala wymogi bezpieczeństwa, którym podlegają wszystkie użytkowane u Administratora Systemy, zasoby oraz pracownicy i współpracownicy.

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

3. Ochrona Danych osobowych przetwarzanych w Przedsiębiorstwie obowiązuje wszystkie osoby, które mają dostęp do Danych osobowych zbieranych, Przetwarzanych oraz przechowywanych przez Administratora, bez względu na zajmowane stanowisko oraz miejsce wykonywania, jak również charakter zatrudnienia/współpracy.
4. Osoby mające dostęp do Danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych Danych osobom nieupoważnionym.
5. Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy/współpracy, jak i po jego ustaniu.
6. Polecenia wydawane przez Specjalistę w zakresie działań związanych z ochroną Danych osobowych muszą być bezwzględnie wykonywane przez wszystkich pracowników/współpracowników Administratora, w szczególności przez Użytkowników.
7. Obowiązkiem pracowników oraz współpracowników Administratora jest przestrzeganie szczegółowych zasad postępowania zawartych w Procedurze rozpoczęcia, zawieszania i kończenia pracy w Systemie, stanowiącej Załącznik nr 9 do niniejszego Dokumentu
8. Niniejszy Dokument ma zastosowanie do wszystkich informacji w postaci dokumentów papierowych, elektronicznych i innych przetwarzanych w Systemie, zawierających Dane osobowe.
9. Na podstawie niniejszego Dokumentu zostały sformułowane poszczególne cele w zakresie bezpieczeństwa Danych osobowych:
  - 1) zapewnienie przetwarzania Danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
  - 2) zapewnienie zbierania Danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; ("ograniczenie celu");

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- 3) zapewnienie zbierania Danych osobowych adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
  - 4) Dane osobowe winny być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
  - 5) Dane osobowe winny być przechowywane w formie umożliwiającej identyfikację osoby, której one dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane ("ograniczenie przechowywania");
  - 6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").
10. Cele te są realizowane poprzez podejmowanie odpowiednich działań i stosowanie efektywnych zabezpieczeń, które obejmują w szczególności:
- 1) stałe podnoszenie świadomości i wiedzy pracowników/współpracowników w zakresie bezpieczeństwa Danych osobowych,
  - 2) zakomunikowanie pracownikom/współpracownikom konsekwencji, w tym dyscyplinarnych, w przypadku naruszenia bezpieczeństwa Danych osobowych,
  - 3) przydzielanie dostępu do dokumentów, materiałów lub Systemów, zawierających Dane osobowe, tylko Osobom upoważnionym przez Specjalistę,
  - 4) zabezpieczenie dokumentów, materiałów lub Systemów przed utratą lub zniszczeniem zawartych w nich Danych osobowych,

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- 5) wdrożenie szczegółowych zasad określających sposób zarządzania uprawnieniami Użytkowników i zasadami Uwierzytelniania, we wszystkich Systemach eksploatowanych w Przedsiębiorstwie,
- 6) przeprowadzanie gruntownych testów w procesie przygotowania nowego oprogramowania,
- 7) regularne wykonywanie kopii bezpieczeństwa Systemów,
- 8) raportowanie incydentów związanych z bezpieczeństwem informacji,
- 9) regularna Analiza Ryzyka w obszarze bezpieczeństwa informacji i projektowanie działań minimalizujących potencjalne Ryzyka,
- 10) powierzanie Danych osobowych wyłącznie takim podmiotom trzecim, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia, niniejszego Dokumentu oraz chroniło prawa osób, których dane dotyczą.

### § 3.

#### **PRZETWARZANIE ZGODNE Z PRAWEM**

1. Dane osobowe są przetwarzane wyłącznie w przypadku, gdy:

- 1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich Danych osobowych w jednym lub większej liczbie określonych celów,
- 2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- 3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
- 4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- 5) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.



których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony Danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Zgoda osoby, której dane dotyczą, powinna być wyrażona w formie pisemnej lub w formie elektronicznej. W wyjątkowych przypadkach dopuszcza się możliwość wyrażenia takiej zgody w formie ustnej, w miarę możliwości powinna być ona jednak potwierdzona przez osobę, której dane dotyczą, na piśmie lub w formie elektronicznej.

3. Przyjmuje się następujący wzorzec oświadczenia osoby, której dane dotyczą, zawierającego zgodę na Przetwarzanie:

*Zgadzam się na przetwarzanie moich następujących danych osobowych: .....  
przez ..... z siedzibą w ....., ul. ...., w celu .....  
(np. marketingowym).*

*Zgadzam się na przetwarzanie moich następujących danych osobowych: .....  
przez ..... z siedzibą w ....., ul. ...., w celu .....  
(np. przygotowanie i przedstawienia oferty dotyczącej produktu .....*

*Podanie danych jest dobrowolne. Podstawą przetwarzania danych jest moja zgoda. Odbiorcami danych mogą być ..... [np. podmioty zajmujące się obsługą informatyczną Administratora]. Mam prawo wycofania zgody w dowolnym momencie. Dane osobowe będą przetwarzane ..... [np. do ew. odwołania zgody, a po takim odwołaniu, przez okres przedawnienia roszczeń przysługujących administratorowi danych i w stosunku do niego].*

*Mam prawo żądania od Administratora dostępu do moich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania [o prawie do przenoszenia danych, jeżeli przysługuje], a także prawo wniesienia skargi do organu nadzorczego. [jeżeli dochodzi do profilowania, wówczas informacje dotyczące profilowania].*

4. Zgoda, o której mowa w ust. 2 powyżej, może być w każdym czasie wycofana. W przypadku, jeżeli nie zachodzi inna przesłanka przetwarzania Danych osobowych osoby, która zgodę cofnęła, Administrator winien podjąć działania polegające na Usunięciu Danych.

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

5. W przypadku, jeżeli Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, Dane osobowe są Przetwarzane przez okres nie dłuższy niż upływ terminu przedawnienia roszczeń wynikających z takiej umowy.
5. W przypadku, jeżeli Przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, Administrator Usuwa Dane w przypadku, jeżeli nie dojdzie do zawarcia wzmiankowanej umowy. Jeżeli umowę zawarto, zastosowanie mają zasady opisane w ust. 4.
6. Jeżeli Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze, Administrator Usuwa Dane w przypadku, jeżeli obowiązek taki przestaje go wiązać, w szczególności w przypadku upływu terminu, w jakim Administrator zobowiązany był do przechowywania określonych informacji (m.in. pracowniczych, księgowych itp.).
7. Dane osobowe mogą być Przetwarzane wyłącznie zgodnie z brzmieniem Rozporządzenia oraz innych aktów prawnych, obowiązujących na terytorium Rzeczypospolitej Polskiej.
8. Specjalista kontroluje w wybrany przez siebie sposób, co najmniej raz na kwartał, spełnienie przesłanek przetwarzania Danych osobowych oraz spełnienie obowiązków związanych z Usuwaniem Danych oraz przedkłada w tym zakresie pisemną informację Administratorowi.

#### § 4.

### OBOWIĄZEK INFORMACYJNY

1. Specjalista podejmuje odpowiednie środki, w szczególności opisane w niniejszym Dokumencie, aby w zwartej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności gdy informacje są kierowane do dziecka - udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 Rozporządzenia. oraz prowadzić z nią wszelką niezbędną ko-

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

munikację. Wzór odpowiednich klauzul informacyjnych zawiera Załącznik nr 1 do niniejszego Dokumentu.

2. Informacje, o których mowa w ust. 1 przekazywane są przez Specjalistę co do zasady w formie dokumentowej lub w formie pisemnej. Przekazanie wzmiankowanych informacji ustnie możliwe jest wyłącznie w wyjątkowych przypadkach, na wyraźne żądanie osoby, której dane dotyczą, o ile innymi sposobami potwierdzona zostanie jej tożsamość. W miarę możliwości ustne udzielenie informacji, o których mowa w ust. 1, powinno zostać potwierdzone w najkrótszym możliwym terminie w formie pisemnej lub dokumentowej.
3. Specjalista zobowiązany jest, na żądanie osoby, której dane dotyczą, do przekazania potwierdzenia, że jej dane są Przetwarzane, a jeżeli ma to miejsce, przekazania informacji dotyczących celów Przetwarzania, kategorii Przetwarzanych Danych osobowych oraz innych, opisanych w art. 15 Rozporządzenia.
4. Specjalista zobowiązany jest, na żądanie osoby, której Dane osobowe dotyczą, do niezwłocznego ich sprostowania, jeżeli są nieprawidłowe, a także do Usunięcia Danych, jeżeli nie zachodzą już przesłanki umożliwiające ich Przetwarzanie oraz ograniczenia Przetwarzania w przypadkach wymienionych w art. 18 Rozporządzenia. Administrator o działaniach, o których mowa w zdaniu poprzednim, niezwłocznie informuje osobę, której Dane osobowe dotyczą chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
5. Specjalista przekazuje na żądanie osoby, której dane dotyczą, jej Dane osobowe, które dostarczyła Administratorowi, poprzez ich przekazanie za pośrednictwem wiadomości e-mail na adres wskazany przez tę osobę, w formacie Microsoft Word, Microsoft Excel lub innym powszechnie wykorzystywanym formacie plików w przypadku, jeżeli Przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy i odbywa się w sposób zautomatyzowany.
6. Specjalista kontroluje w wybrany przez siebie sposób, co najmniej raz na kwartał, spełnienie wymagań dotyczących wypełnienia obowiązków informacyjnych opisanych powyżej oraz ujętych w Rozporządzeniu i przedkłada w tym zakresie pisemną informację Administratorowi.

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

## § 5.

### PODMIOT PRZETWARZAJĄCY

1. W przypadku, jeżeli Administrator przekaze podmiotowi trzeciemu co najmniej część Danych osobowych do Przetwarzania, winien dokonać uprzedniej weryfikacji, czy podmiot taki zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia, niniejszego Dokumentu oraz chroniło prawa osób, których Dane osobowe dotyczą.
2. Powierzenie Przetwarzania Danych osobowych winno odbywać się na podstawie umowy. Wzorce umowy, o której mowa w zdaniu poprzednim, zawiera Załącznik nr 2 do niniejszego Dokumentu.

## § 6.

### REJESTR CZYNNOŚCI PRZETWARZANIA

1. Specjalista prowadzi w imieniu Administratora rejestr czynności Przetwarzania. Wzór rejestru, o którym mowa w zdaniu poprzednim, zawiera Załącznik nr 3 do niniejszego Dokumentu.
2. Rejestr prowadzony jest w formie elektronicznej, w formacie Microsoft Excel lub podobnym formacie plików.
3. Obowiązek, o którym mowa w niniejszym paragrafie nie ma zastosowania, jeżeli Administrator zatrudnia nie więcej niż 250 osób chyba, że Przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie Danych osobowych.
4. Przetwarzanie dotyczące Danych osobowych pracowników lub kontrahentów Administratora nie ma co do zasady charakteru sporadycznego (tj. rejestr o którym mowa w ust. 1 winien być prowadzony co najmniej w zakresie wzmiankowanych Danych osobowych). Inne kategorie Danych osobowych, co do których Admini-

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

strator prowadzi rejestr, wskazuje Specjalista, po dokonaniu stosownej analizy, w szczególności w zakresie sporadyczności przetwarzania.

## § 7.

### ZGŁOSZENIE NARUSZEŃ

1. W przypadku wystąpienia naruszenia ochrony Danych osobowych (tj. naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób Przetwarzanych), Specjalista w porozumieniu z Administratorem winien podjąć uzasadnione i odpowiednie działania zmierzające do minimalizacji Ryzyka oraz niezwłocznie, nie później niż w terminie 72 godzin od chwili ich wykrycia, zgłosić je organowi nadzorcemu. Informacje przekazane przez organowi nadzorcemu winny być kompletne, dokładne i poprawne.
2. Zgłoszenie, o którym mowa w ust. 1, nie jest konieczne w przypadku, jeżeli jest mało prawdopodobne, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Oceny prawdopodobieństwa zgodnie ze zdaniem poprzednim dokonuje Specjalista i przedkłada w tym zakresie pisemne uzasadnienie Administratorowi.
3. Specjalista zobowiązany jest do odpowiedniego dokumentowania naruszeń, o których mowa w ust. 1, w szczególności poprzez sporządzenie stosownej notatki służbowej lub nakazanie pracownikom/ współpracownikom udzielenia pisemnych wyjaśnień.
4. Jeżeli ocena prawdopodobieństwa przeprowadzona zgodnie z ust. 2 przez Specjalistę wykaże, że zaistniałe naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, nie zachodzą zaś okoliczności wskazane w art. 34 ust. 3 Rozporządzenia, Specjalista bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie takie winno być w miarę możliwości przekazane pisemnie lub w formie dokumentowej.

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

## § 8.

### **ZABEZPIECZENIE DOSTĘPU DO DANYCH OSOBOWYCH**

1. Dostęp do pomieszczeń, w których przetwarzane są Dane osobowe oraz do pomieszczeń, w których znajdują się serwery, na których umieszczone są Dane osobowe, w tym również Zbiory Danych osobowych lub przechowywane są Kopie bezpieczeństwa mogą mieć wyłącznie osoby do tego upoważnione. Centrum Przetwarzania (serwery) i przechowywane dane (Kopie bezpieczeństwa) znajdują się w wydzielonych strefach ograniczonego dostępu. Dostęp do pomieszczeń, w których znajdują się serwery na których umieszczone są Dane osobowe, w tym również Zbiory danych osobowych lub przechowywane są kopie zapasowe posiadają wyłącznie Osoby upoważnione wyznaczone przez Specjalistę.
2. Pomieszczenia, w których przetwarzane są Dane osobowe, są zamykane na czas nieobecności w nich Osób upoważnionych, w sposób uniemożliwiający dostęp do nich osób trzecich. Kontrolą dostępu do pomieszczeń przeznaczonych do Przetwarzania zajmuje się Specjalista lub Osoba uprawniona.
3. Przetwarzać Dane osobowe może wyłącznie Osoba upoważniona. Procedura postępowania w zakresie nadawania/odwołania uprawnień do przetwarzania Danych osobowych stanowi Załącznik nr 4 do niniejszego Dokumentu.

## § 9.

### **OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH**

1. Ogólna lista zasobów wykorzystywanych przez Administratora w Przedsiębiorstwie, które należy zabezpieczyć w związku z ochroną Danych osobowych w Systemach obejmuje:
  - 1) Stacje robocze – serwery, komputery osobiste, drukarki i inne urządzenia zewnętrzne;

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- 2) okablowanie teletechniczne oraz urządzenia sieci telekomunikacyjnej;
- 3) oprogramowanie – kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające, programy komunikacyjne, legalność oprogramowania;
- 4) dane zapisane na dyskach oraz dane podlegające przetwarzaniu w Systemie;
- 5) Hasła Użytkowników, charakter ich aktywności w Systemie (uprawnienia);
- 6) pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa;
- 7) wydruki, jako specyficzny element przetwarzania informacji.

## 2. Zasady dodatkowe dotyczące Przetwarzania:

- 1) przetwarzać Dane osobowe w Systemach mogą wyłącznie Osoby upoważnione;
- 2) dostęp do Danych osobowych przetwarzanych w Systemie może mieć miejsce wyłącznie po Uwierzytelnieniu, tj. po podaniu Identyfikatora i właściwego Hasła;
- 3) Identyfikator jest w sposób jednoznaczny przypisany Użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu Identyfikatora, którym się posługuje lub posługiwał;
- 4) rozpoczęcie pracy Użytkownika w Systemie obejmuje prawidłowe Uwierzytelnienie (tj. wprowadzenie Identyfikatora i Hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione) oraz ogólne stwierdzenie poprawności działania Systemu;

## 3. Środki organizacyjne:

- 1) opracowanie strategicznych dokumentów (Polityka Bezpieczeństwa, instrukcje, zarządzenia);
- 2) powołanie Specjalisty oraz Specjalisty ds. Systemu, odpowiedzialnych za działania organizacyjne i środki techniczne zapewniające odpowiedni poziom bezpieczeństwa Danych osobowych oraz Zarządzanie ryzykiem;
- 3) prowadzenie ewidencji osób zatrudnionych/współpracujących przy Przetwarzaniu;
- 4) kontrola dostępu do pomieszczeń, w których Przetwarzane są Dane osobowe oraz ścisła kontrola dostępu do pomieszczeń, w których znajdują się serwery;

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- 5) tworzenie kopii archiwalnych baz danych zawierających Dane osobowe;
  - 6) testowanie przez Specjalistę ds. Systemu modyfikacji oprogramowania przed wdrożeniem go do użytku operacyjnego zarówno pod kątem poprawności działania jak i podatności na „ataki” z zewnątrz;
  - 7) ochrona dokumentacji;
  - 8) Uwierzytelnianie - potwierdzanie wiarygodności dostępu;
  - 9) powtarzanie Uwierzytelnienia po upływie określonego czasu braku aktywności;
  - 10) bezpieczeństwo dostępu – uprawnienia do działania w Systemie na zasadzie „najmniejszy wymagany dostęp”;
  - 11) polityka w zakresie wymagań co do Hasła (musi się składać z co najmniej 8 znaków, z czego muszą wystąpić małe i duże litery, cyfra lub znak specjalny oraz być zmieniane nie rzadziej niż co 30 dni);
  - 12) zarządzanie kontem Użytkownika – potwierdzenie praw dostępu do Systemu;
  - 13) okresowy przegląd zasadności dostępu do Danych osobowych;
  - 14) prowadzenie szkoleń pracowników/współpracowników i akcji uświadamiających;
  - 15) procedury reagowania na incydenty (Instrukcja Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych – Załącznik nr 5);
  - 16) raporty dotyczące działań związanych z bezpieczeństwem i naruszenia bezpieczeństwa;
  - 17) Zarządzanie ryzykiem;
  - 18) audyty bezpieczeństwa;
  - 19) analiza pracy zasobu - gromadzenie i analiza logów systemów;
  - 20) aktualizacje oprogramowania.
4. Zabezpieczenia fizyczne:
- a) siedziba firmy całodobowo strzeżona przez odpowiednio wyszkolonych pracowników firmy ochroniarskiej;
  - b) kontrola odwiedzających;
  - c) budynek dostatecznie oświetlony nocą i wyposażony w solidne zamknięcia;
  - d) pomieszczenia zamykane na atestowane zamki;

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.



- e) pomieszczenia w których znajdują się serwery i inne powiązane z nimi urządzenia są zawsze zamknięte,;
  - f) dostęp do serwerowni mają tylko upoważnione osoby;
  - g) kopie zapasowe elementów Systemu są przechowywane w szafie pancерnej;
  - h) ekrany monitorów automatycznie wygaszane i blokowane po upływie ustalonego czasu nieaktywności Użytkownika;
  - i) ekrany monitorów są ustawione taki sposób, żeby uniemożliwić innym osobom wgląd w dane;
5. Zabezpieczenia techniczne:
- a) zabezpieczeniem okablowania i urządzeń towarzyszących poprzez ograniczenie dostępu;
  - b) oprogramowanie antywirusowe chroniące przed innym nieuprawnionym oprogramowaniem;
  - c) zapory ogniowe (firewall);
  - d) konserwacja Stacji roboczych;
  - e) stosowanie niszczarek;
  - f) systemy alarmowe;
  - g) czujniki dymu;
  - h) klimatyzacja;
  - i) instalacja przeciwpożarowa;
  - j) stabilizatory i zasilacze awaryjne UPS.
6. Sposób postępowania w zakresie komunikacji w sieciach komputerowych wchodzących w skład Systemu:
- a) ruch dla usług publicznych jest chroniony przy pomocy access-list na systemie firewall, udostępniając tylko wybrane porty na serwerach znajdujących się w sieci. System firewall jest zdublowany a urządzenia pracują w trybie active/standby. Urządzenie zapasowe podejmuje pracę natychmiast po wykryciu awarii urządzenia podstawowego;
  - b) cały ruch do sieci dedykowanej przechodzi przez serwer pełniący rolę zapory ogniowej (firewall), gdzie jest filtrowany i translowany na lokalną klasę adresów;

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- c) na stacjach roboczych zainstalowany, licencjonowany system MS Windows.
- d) zabezpieczona konfiguracja Stacji roboczej – Hasło administratora Stacji roboczej. Niedopuszczalne jest, aby Użytkownik posiadał uprawnienia administratora Stacji roboczej. Zablokowane konto „guest” lub inne posiadające szersze uprawnienia;
- e) Hasła dostępu dla administratora Stacji roboczej przekazane i przechowywane przez Specjalistę;
- f) Uwierzytelnienie Użytkownika w systemie operacyjnym;
- g) monitorowanie i detekcja ataków sieciowych - analiza logów systemowych, aplikacji, etc, stały nadzór prowadzony przez oprogramowanie do monitoringu zasobów IT oraz urządzeń sieciowych;
- h) blokada portów dla wybranych usług;
- i) monitorowanie zdarzeń bezpieczeństwa i powiadamianie – analiza logów systemowych, aplikacji, zabezpieczeń. poprzez skrypty opracowane przez administratorów;
- j) switche zabezpieczone hasłem;

## § 10.

### **IDENTYFIKACJA RÓL W PROCESIE ZARZĄDZANIA BEZPIECZEŃSTWEM**

1. Nad bezpieczeństwem i ochroną Systemów czuwają:

- 1) Specjalista,
  - 2) Specjalista ds. Systemu.
  - 3) wszyscy Użytkownicy Systemów.
2. Imiennego wskazania Specjalisty oraz Specjalisty ds. Systemu dokonuje Administrator.
3. Specjalista działa w oparciu o Regulamin Specjalisty Ochrony Danych, stanowiący Załącznik numer 6 do niniejszego Dokumentu.
4. Zadania Użytkowników obejmują:
- 1) znajomość i przestrzeganie zasad zawartych w niniejszym Dokumencie oraz załącznikach do niego i procedurach;

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- 2) obowiązek zachowania w tajemnicy swoich Hasel oraz informacji dostępnych podczas przetwarzania danych, a także sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia/współpracy;
- 3) uświadomienie odpowiedzialności za utrzymanie bezpieczeństwa;
- 4) ściśle przestrzeganie zapisów zawartych w Regulaminie użytkownika i ochrony informacji, stanowiącym załącznik numer 7 do niniejszego Dokumentu;

## § 11.

### **PROCESY ZARZĄDZANIA BEZPIECZEŃSTWEM SYSTEMÓW**

1. Zarządzanie Bezpieczeństwem Systemów jest w Przedsiębiorstwie działaniem ciągłym i składa się z różnych powiązanych ze sobą procesów. Procesy te to:

- 1) zarządzanie konfiguracją,
- 2) zarządzanie zmianami,
- 3) Zarządzanie ryzykiem,
- 4) rozliczalność,
- 5) monitorowanie,
- 6) planowanie awaryjne,
- 7) odtwarzanie.

2. Zarządzanie konfiguracją.

W Przedsiębiorstwie śledzi się na bieżąco zmiany w konfiguracji Systemów w celu zapewnienia, że nie obniżają one efektywności zabezpieczeń i całkowitego bezpieczeństwa Przedsiębiorstwa. Za zarządzanie konfiguracją odpowiedzialny jest Specjalista ds. Systemu .

3. Zarządzanie zmianami.

W celu identyfikacji nowych wymagań, Specjalista analizuje pozyskane dane na temat zmian w Systemach. W tym zakresie Użytkownicy oraz Specjalista ds. Systemu ściśle współpracują ze Specjalistą i niezwłocznie powiadamiają go o planowanych lub dokonanych zmianach. Informacje mające wpływ na System to m.in.:

- nowe procedury Systemu,

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- nowe funkcje Systemu,
- aktualizacja oprogramowania,
- wymiana Stacji roboczych,
- nowi Użytkownicy,
- dodatkowe połączenia sieciowe i międzysieciowe.

Na podstawie uzyskanych informacji Specjalista określa czy i jaki wpływ ta zmiana będzie miała na bezpieczeństwo Systemu. W razie konieczności przeprowadza analizę, aby określić nowe wymagania dotyczące bezpieczeństwa.

#### 4. Zarządzanie ryzykiem.

W Przedsiębiorstwie procesy związane z Zarządzaniem ryzykiem są przeprowadzane w sposób ciągły. Ponieważ uzyskanie absolutnego bezpieczeństwa Systemu lub sieci teleinformatycznej nie jest możliwe, dopuszcza się pewien poziom akceptowanego ryzyka w kontekście następstw oraz prawdopodobieństwa zajścia określonego zdarzenia. Niniejszy Dokument pozwala na zapewnienie odpowiedniego stopnia bezpieczeństwa, proporcjonalnego zarówno co do wagi chronionej informacji jak i ilości zastosowanych środków ochrony.

Specjalista oraz Specjalista ds. Systemu cyklicznie sprawdzają poziom wdrożonych zabezpieczeń i proponują zmiany w tym zakresie. Proponowane zmiany są wynikiem porównania określonych dotychczasowych i nowych Ryzyk z zyskami lub kosztami zabezpieczeń. W oparciu o takie zestawienie opracowuje się plan działania określający ukierunkowanie działań na najbardziej prawdopodobne zagrożenia. Realizacja planu skutkuje dokumentacją techniczną w postaci formularza Analizy ryzyka.

Formularz Analizy ryzyka zawiera następujące informacje:

- 1) potencjalne skutki zagrożeń bezpieczeństwa informacji,
- 2) szacunkowe koszty finansowe, logistyczne, techniczne i osobowe zagrożeń ,
- 3) koszty zabezpieczeń i prowadzenia działań zapobiegawczych,
- 4) priorytety realizacji przedsięwzięć profilaktycznych,
- 5) opis działań zapobiegawczych.

Analiz ryzyka dokonuje się :

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

- stosownie do potrzeb – analiza problemowa, która przeprowadzana jest doraźnie w związku ze zmianami pojawiającymi się w Systemie,
- kontrolnie – przegląd postępu wdrożeń zabezpieczeń zaleconych przy poprzedniej kontroli.

#### 5. Rozliczalność.

Ścisłe przypisanie i przyjęcie obowiązków z zakresu bezpieczeństwa wymagane jest dla realizacji skutecznej polityki ochrony Danych osobowych. Istotna dla bezpieczeństwa jest własność zasobów i związane z tym obowiązki. Rozliczalność jest realizowana w Przedsiębiorstwie przez przypisanie zasobów do konkretnych osób odpowiedzialnych i Użytkowników. Tabela rozliczalności przedstawia się następująco:

<b>Zasób</b>	<b>Osoba odpowiedzialna</b>
Serwery	Specjalista ds. Systemu
Stacje robocze (komputery)	Użytkownik
Pozostały sprzęt komputerowy	Specjalista ds. Systemu
Komputery przenośne	Użytkownik
Okablowanie	Specjalista ds. Systemu
Przetwarzane dane	osoba przetwarzająca dane
Hasła użytkowników	Specjalista
Kopie zapasowe i archiwa	Specjalista ds. Systemu
Dane administratorów	Specjalista
Dokumentacje Systemów	Specjalista ds. Systemu
Dokumenty Polityki Bezpieczeństwa	Specjalista
Wydruki	Użytkownik
Dokumenty analizy pracy Systemu	Specjalista ds. Systemu

#### 6. Monitorowanie.

W celu weryfikacji działania używanych zabezpieczeń, wszystkie procesy związane z bezpieczeństwem informacji w Przedsiębiorstwie są monitorowane, dla upewnienia się, czy zmiany w środowisku nie wpłynęły negatywnie na ochronę zasobów i czy zapewniona jest rozliczalność. Taka praktyka weryfikuje sposób przetwarzania informacji, w szczególności Danych osobowych, w porównaniu z normami przepisów ogólnych oraz wewnętrznych procedur ochrony danych i Systemów. Działania monitorujące są realizowane w sposób systematyczny. Użytkownicy są powiadamiani o kontroli ich

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

działań w Systemie. Tym samym mają świadomość, że służy to ochronie Systemu przed nieuprawnionym dostępem i powoduje ostrożność oraz niechęć do nielegalnego używania Systemu i naruszania zasad bezpieczeństwa.

Monitorowanie jest realizowane następującymi metodami:

- 1) kontrola przeprowadzana przez Specjalistę, zgodnie z zapisami w Regulaminie kontroli przeprowadzanych przez Specjalistę, stanowiącym załącznik numer 8 do niniejszego dokumentu. Efektem przeprowadzanej kontroli są protokoły zawierające między innymi opis zastanej sytuacji, opis odstępstw od zasad bezpieczeństwa Systemu, wykaz środków zaradczych jakie trzeba podjąć, aby usunąć odstępstwa;
- 2) ocena okresowa bezpieczeństwa Systemu – składają się na nią ocena kosztów eksploatacji Systemu, określenie, czy nakłady finansowe na System są wystarczające, prognozowanie czy obecny stan zabezpieczeń będzie wystarczający w przyszłości, określenie planów rozwoju Bezpieczeństwa Systemu.
- 3) ocena nowych projektów – realizowana w momencie tworzenia nowych projektów i wprowadzania zmian w otoczeniu jednostki. Specjalista oraz Specjalista ds. Systemu uczestniczą w fazie definiowania każdego nowego projektu w celu ustalenia czy stwarza on jakieś nowe ryzyko czy też je zmniejsza. Jeśli ryzyko zostanie wcześniej wykryte, definiowanie projektu może zostać zweryfikowane, może także wprowadzić mechanizmy Zarządzania ryzykiem.
- 4) audyty pracy urzędzeń zabezpieczających. W tym celu analizuje dane wyjściowe urzędzeń zabezpieczających, które są przeglądane w poszukiwaniu zdarzeń istotnych dla bezpieczeństwa.

#### 7. Planowanie awaryjne i odtwarzanie.

W celu zapewnienia szybkiej, efektywnej i uporządkowanej reakcji na incydenty związane z bezpieczeństwem, stworzono dokument określający metody działania i zakres odpowiedzialności poszczególnych osób, pełniących role w systemie bezpieczeństwa. Zasady postępowania w przypadku zaistnienia sytuacji kryzysowej dotyczącej bezpieczeństwa danych opisane są w dokumencie Instrukcja Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych – załącznik nr 5 do niniejszego

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.

Dokumentu. W przypadku wystąpienia w Przedsiębiorstwie sytuacji zagrożenia bezpieczeństwa informacji dalsze działanie musi być ściśle zgodne z wyżej wymienioną instrukcją.

Załączniki:

1. Wzór klauzul informacyjnych.
2. Wzór umowy dotyczącej powierzenia przetwarzania Danych osobowych.
3. Wzór rejestru czynności Przetwarzania.
4. Procedura postępowania w zakresie nadawania/odwołania uprawnień do przetwarzania Danych osobowych Instrukcja Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych.
5. Instrukcja Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych.
6. Regulamin Specjalisty Ochrony Danych.
7. Regulamin użytkownika i ochrony informacji.
8. Regulamin kontroli przeprowadzanych przez Specjalistę.
9. Procedura rozpoczynania, zawieszania i kończenia pracy w Systemie.

Niniejsze materiały objęte są prawami autorskimi należącymi do KPF EDUKACJA Sp. z o.o. i udostępnione są uczestnikom szkolenia organizowanego przez KPF EDUKACJA Spółka z o.o. Materiały nie mogą być udostępniane i wykorzystywane przez inne osoby niebędące uczestnikami szkoleń.