Polityka
Ochrony Danych Osobowych
w

ART&DECOR PLACÓWKA OŚWIATOWA
EWA OSIŃSKA-MAJEWSKA

ul. Chocimska 14, 00-791 Warszawa

NIP 1131622323

REGON 014835219

Data i miejsce sporządzenia dokumentu: Warszawa, dn. 4.07.2018r.

Spis treści

Wstęp ... 3
1. Definicje ... 4
2. Osoby odpowiedzialne za ochronę danych osobowych ... 5
2.1. Administrator ... 5
2.2. Inspektor Ochrony Danych Osobowych ... 6
2.3. Osoby upoważnione do przetwarzania danych osobowych ... 8
3. Szacowanie ryzyka – ocena skutków dla ochrony danych osobowych ... 8
4. Przetwarzanie danych osobowych ... 9
4.1. Podstawy Prawne ... 9
5. Polityka prywatności – prawa osób których dane dotyczą ... 10
5.1. Zasady Ogólne ... 10
5.2. Procedura obsługi wniosków ... 11
5.3. Prawo do informacji ... 11
5.4. Prawo dostępu do danych ... 12
5.5. Prawo do sprostowania danych ... 12
5.6. Prawo do usunięcia danych ... 12
5.7. Ograniczenie przetwarzania ... 13
5.8. Przenoszenie danych ... 13
5.9. Prawo do sprzeciwu ... 14
6. Ogólne Zasady Bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych ... 14
6.1. Zasady Ogólne ... 14
6.2. Określanie ryzyka ... 15
6.3. Niszczenie dokumentów ... 15
6.4. Zasada czystego biurka i polityka kluczy ... 15
6.5. Pozostałe zasady: ... 16
7. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych ... 17
7.1. Zabezpieczenia organizacyjne ... 17
7.2. Zabezpieczenia ochrony fizycznej danych osobowych ... 17
7.3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej ... 17
8. Powierzenie przetwarzania danych ... 18
9. Naruszenie ochrony danych osobowych ... 18
9.1. Definicje ... 18
9.2. Informowanie o naruszeniach ochrony danych osobowych ... 19
9.3. Procedura postępowania w przypadku zagrożenia naruszenia danych osobowych ... 19
9.4. Procedura postępowania w przypadku stwierdzenia naruszenia danych osobowych ... 20
10. Kontrola przetwarzania i stanu zabezpieczenia danych osobowych ... 20
11. Szkolenia ... 21
12. Postanowienia końcowe ... 21

Wstęp

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony DANYCH OSOBOWYCH przetwarzanych przez **Administratora** przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane:

- były przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane
- prawidłowe i w razie potrzeby uaktualniane.

Administrator zapewnia danym poufność, integralność, dostępność i rozliczalność, gdzie przez:

- **poufność danych** – rozumie się właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
- **integralność danych** - rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- **dostępność danych** – rozumie się właściwość zapewniającą, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot
- **rozliczalność danych** - rozumie się właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Niniejsza procedura jest dokumentem wewnętrznym, poufnym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody Administratora.
Osoby, której dane dotyczą będą sposób czytelny i wyczerpujący informowane o przysługujących im prawach w polityce prywatności.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:
- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 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* (ogólne rozporządzenie o ochronie danych), *zwane dalej RODO.* (Dziennik Urzędowy Unii Europejskiej L 119/1, wersja PL 4.5.2016).
- ustawą z dnia 29 sierpnia 1997 r. o *ochronie danych osobowych* (Dz.U. 1997 nr 133 poz. 883 późn. zm.).

1. Definicje

Przez użyte w Polityce określenia należy rozumieć:

- **Administrator -** osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
- **Dane osobowe (dane)** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
- **Dane wrażliwe -** dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne (dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej), dane biometryczne (dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne), dane dotyczące zdrowia (dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia), dane dotyczące seksualności lub orientacji seksualnej tej osoby.
- **Identyfikator (login) użytkownika —** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- **Naruszenie ochrony danych osobowych -** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
- **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde.
- **Ograniczenie przetwarzania -** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
- **Osoba upoważniona –** rozumie się przez to osobę, która otrzymała od Administratora upoważnienie do przetwarzania danych.
- **Podmiot przetwarzający (procesor)** - osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
- **Przetwarzanie danych** – operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego

rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- **Rozporządzenie (RODO) -** Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 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 (ogólne rozporządzenie o ochronie danych), (Dziennik Urzędowy Unii Europejskiej L 119/1, wersja PL 4.5.2016).
- **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Upoważnienie –** rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu.
- **Ustawa** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. 1997 nr 133 poz. 883 późn. zm.).
- **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
- **Użytkownik** – osoba upoważniona przez Administratora, posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych.
- **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
- **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
- **Zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

2. Osoby odpowiedzialne za ochronę danych osobowych

Punkt ten wskazuje osoby odpowiedzialne za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia.

2.1. Administrator

2.1.1. Do najważniejszych obowiązków Administratora należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami Rozporządzenia i ustawy, w tym w fazie projektowania i by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych;

2) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w tym aby zapewnić

bezpieczne przetwarzanie danych w pomieszczeniach do tego przeznaczonych oraz systemu i sprzętu informatycznego umożliwiającego bezpieczne przetwarzanie danych;

3) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić: ciągłą poufność, integralność, dostępność danych, a także odporność systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;

5) wykonywanie rejestrowania czynności przetwarzania;

6) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych oraz prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych;

7) nadzór nad bezpieczeństwem danych osobowych, kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami, oraz prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;

8) należyte i terminowe wykonywanie uprawnień na wniosek osób, których dane są przetwarzane, zgodnie z polityką prywatności;

9) zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych oraz zawiadomienie o takim naruszeniu osoby, której dotyczą, jeżeli naruszenie powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych;

10) prowadzenie dokumentacji wszelkich naruszeń ochrony danych osobowych i rejestru naruszeń. Wzór rejestru stanowi Załącznik nr 1 do przedmiotowej procedury;

11) ocena, czy konieczne jest powołanie Inspektora Ochrony Danych Osobowych i powołanie takiego Inspektora, jeżeli jest to konieczne bądź jeżeli administrator uzna to za celowe;

12) wspieranie inspektora ochrony danych w wypełnianiu przez niego zadań, w tym zapewnienie mu zasobów, niezbędnych do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasobów niezbędnych do utrzymania jego wiedzy fachowej;

13) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

14) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych, w szczególności zapoznawanie z przepisami ochrony danych osobowych.

2.1.2. Poza obowiązkami wskazanymi w punkcie 2.1.1. Administrator wypełnia wszelkie obowiązki określone w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 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*

2.2. Inspektor Ochrony Danych Osobowych

2.2.1. Administrator może powołać Inspektora Ochrony Danych Osobowych.

2.2.2. Administrator powołuje Inspektora Ochrony Danych Osobowych, w przypadku gdy:

1) główna działalność administratora lub procesora polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
2) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych tzn. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

2.2.3. Administrator ocenia obowiązek bądź brak obowiązku wyznaczenia Inspektora Ochrony Danych Osobowych. Oceny dokonuje się poprzez ustalenie czy:
1) główna działalność administratora polega na operacjach przetwarzania – poprzez którą należy rozumieć zasadnicze, a nie poboczne czynności administratora, kluczowe z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego dane, w tym także czynności nierozerwalnie związane z działalnością główną administratora lub podmiotu przetwarzającego;
2) czy dochodzi do przetwarzania danych osobowych na „dużą skalę" - przy ustaleniu której należy wziąć pod uwagę liczbę osób, których dane dotyczą, zakres przetwarzanych danych osobowych, okres, przez jaki dane są przetwarzane, zakres geograficzny przetwarzania danych osobowych.
3) czy następuje regularne i systematyczne monitorowanie - poprzez które należy rozumieć wszelkie formy śledzenia i profilowania w sieci, w tym na potrzeby reklam behawioralnych, a także poza nią, wykonywane regularnie (to znaczy stale albo w określonych odstępach czasu przez ustalony okres, cykliczne albo powtarzające się w określonym terminie, odbywające się stale lub okresowo) i systematycznie (występujące zgodnie z określonym systemem, zaaranżowane, zorganizowane lub metodyczne, odbywające się w ramach generalnego planu zbierania danych, przeprowadzone w ramach określonej strategii).

2.2.4. Administrator publikuje dane kontaktowe inspektora ochrony danych i zawiadamia o nich organ nadzorczy.

2.2.5. Inspektorem może być osoba, która posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktykę w dziedzinie ochrony danych.

2.2.6. Inspektor ochrony danych może być członkiem personelu administratora lub wykonywać zadania na podstawie umowy o świadczenie usług. Inspektor ochrony danych może wykonywać inne zadania i obowiązki, ale nie mogą one powodować konfliktu interesów.

2.2.7. Inspektor ochrony danych jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, nie otrzymuje on instrukcji dotyczących wykonywania zadań z zakresu ochrony danych, nie jest odwoływany ani karany przez administratora wypełnianie swoich zadań.

2.2.8. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora.

2.2.9. Do zadań Inspektora Ochrony Danych Osobowych należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania Rozporządzenia oraz innych przepisów o ochronie danych, a także niniejszej procedury, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) sporządzanie, prowadzenie i aktualizacja rejestrów, które stanowią załączniki do przedmiotowej procedury i wykonywania innych zadań z zakresu ochrony danych osobowych, zleconych przez Administratora;
4) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;
5) współpraca z organem nadzorczym;
6) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 39 Rozporządzenia.

2.3. Osoby upoważnione do przetwarzania danych osobowych

2.3.1. Administrator obowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona.
2.3.2. Upoważnienie powinno zawierać:
1) datę z którą zostało nadane;
2) datę z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony;
3) zakres upoważnienia.

2.3.3. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.
2.3.4. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.
2.3.5. Wzór upoważnienia i oświadczenia dla osoby upoważnionej do przetwarzania danych stanowi Załącznik nr 2 do niniejszej procedury.
2.3.6. W przypadku, gdy zostały upoważnione osoby do przetwarzania danych osobowych, Administrator prowadzi ewidencję osób upoważnionych w wersji papierowej lub elektronicznej. Wzór ewidencji stanowi załącznik nr 3 do procedury bezpieczeństwa.
2.3.7. Ewidencja zawiera:
1) imię i nazwisko osoby upoważnionej;
2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

3. <u>Szacowanie ryzyka – ocena skutków dla ochrony danych osobowych</u>

3.1. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadku, gdy dany rodzaj przetwarzania danych osobowych ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w szczególności w przypadku:

1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

2) przetwarzania na dużą skalę (przy ustaleniu należy wziąć pod uwagę liczbę osób, których dane dotyczą, zakres przetwarzanych danych osobowych, okres, przez jaki dane są przetwarzane, zakres geograficzny przetwarzania danych osobowych) danych wrażliwych;

3) systematycznego monitorowania (występujące zgodnie z określonym systemem, zaaranżowane, zorganizowane lub metodyczne, odbywające się w ramach generalnego planu zbierania danych, przeprowadzone w ramach określonej strategii) na dużą skalę miejsc dostępnych publicznie.

3.2. Formularz oceny stanowi Załącznik nr 4 do niniejszej procedury.

4. <u>Przetwarzanie danych osobowych</u>

4.1. Podstawy Prawne

4.1.1. Przetwarzane mogą być dane osobowe 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 w tym m.in. marketing usług własnych, chyba, że 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.

4.1.2. Dane wrażliwe mogą być przetwarzane w przypadku, gdy:

1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;

2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy,

zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub przepisami krajowego prawa pracy;

3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

4.1.3. Administrator prowadzi Rejestr czynności przetwarzania.

4.1.4. Rejestr zawiera dane wskazane w artykule 30 Rozporządzenia.

4.1.5. Rejestr prowadzi się w formie pisemnej, w tym elektronicznej.

4.1.6. Wzór rejestru stanowi załącznik nr 5 do niniejszej procedury bezpieczeństwa.

5. <u>Polityka prywatności – prawa osób których dane dotyczą</u>

Administrator realizuje uprawnienia osób, których dane dotyczą. W tym celu ustanawia się zasady i procedury opisane poniżej. Wyciąg z Procedury Ochrony Danych Osobowych – Politykę prywatności publikuje się na stronie internetowej administratora. Powyższe nie narusza uprawnienia osób, których dane dotyczą do uzyskania informacji, o których mowa w ust. 5.1. w inny sposób, w zależności od sposobu pozyskiwania danych osobowych i podstawy prawnej ich przetwarzania.

5.1. Zasady Ogólne

5.1.1. Administrator udziela osobie, której dane dotyczą i prowadzi z nią korespondencję na piśmie lub w inny sposób w tym drogą elektroniczną, w tym na żądanie tej osoby udziela informacji także ustnie. Jeżeli osoba uprawniona przekazała swoje żądanie elektronicznie, odpowiedzi udziela się także w takiej formie, chyba, że osoba ta zażądała innej formy.

5.1.2. Administrator w przypadku uzasadnionych wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może domagać się dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

5.1.3. Wykonanie uprawnień osoby, której dane dotyczą przez Administrator odbywa się bez zbędnej zwłoki, maksymalnie w terminie miesiąca od otrzymania żądania. W tym terminie należy co najmniej udzielić tej osobie informacji o działaniach podjętych w związku z żądaniem tej osoby, dotyczącym prawa dostępu do danych, sprostowania, usunięcia danych, prawa żądania ograniczenia przetwarzania, prawa przenoszenia danych, prawa do sprzeciwu. Termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, informując osobę, której dane dotyczą o takim przedłużeniu terminu z podaniem przyczyn opóźnienia w terminie miesiąca od otrzymania żądania.

5.1.4. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje

osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

5.1.5. Wykonywanie uprawnień osoby uprawnionej są wolne od opłat. Administrator może jednak pobrać rozsądną opłatę, uwzględniając koszty administracyjne wykonania żądania, albo odmówić podjęcia działań w związku z żądaniem, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter.

5.2. Procedura obsługi wniosków

5.2.1. Osoba, której dane dotyczą może zwrócić się w dowolnej formie (pisemnie, elektronicznie, telefonicznie, ustnie) o wykonanie przysługujących jej uprawnień, o których mowa w ust. 5 Procedury Ochrony Danych Osobowych. W celu ułatwienia osobie uprawnionej wykonania praw jej przysługujących udostępnia się specjalny adres poczty elektronicznej _____@drukfirmowy.pl. Informacje o powyższym publikuje się na stronie internetowej Administratora.

5.2.2. Wnioski osoby uprawnionej rozpatruje _____ (np. Dział Obsługi Klienta) ze współpracy z pozostałymi działami Administratora, które przetwarzają dane osobowe.

5.2.3. W przypadku zgłoszenia żądania przez osobę uprawnioną każdy pracownik Administratora ma obowiązek utrwalenia tego żądania, jego treści, zakresu i danych osoby uprawnionej, w szczególności danych, na które należy skierować odpowiedź osobie uprawnionej. Informacje o żądaniu przekazuje się niezwłocznie do Działu _____ (patrz ust. 5.2.2.).

5.2.4. Dział _____ dokumentuje proces wykonywania uprawnień osoby, której dane osobowe dotyczą w tym archiwizuje udzielone odpowiedzi i skierowane żądania.

5.2.5. Wykonanie uprawnień osoby zainteresowanej odbywa się na podstawie rejestru czynności przetwarzania.

5.2.6. W przypadku żądania kopii danych przez osobę, której dane dotyczą żądanie realizuje uprawniony dział w ścisłej współpracy z Działem Informatyki. W przypadku żądania przez osobę uprawnioną kopii w formie elektronicznej dane zapisuje się w formacie możliwym do powszechnego odczytu dla przeciętnej osoby np. pdf., _____, itd.

5.2.7. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

5.3. Prawo do informacji

5.3.1. W przypadku pozyskiwania danych od osoby, której dane dotyczą administrator podaje jej informacje, wskazane w art. 13 Rozporządzenia. Treść klauzuli informacyjnej stanowi załącznik nr 6 do niniejszej procedury bezpieczeństwa.

5.3.2. W przypadku pozyskiwania danych nie od osoby, której dane dotyczą administrator podaje jej informacje, wskazane w art. 14 Rozporządzenia, w terminie wskazanym w art. 14 ust. 3 Rozporządzenia. Treść klauzuli informacyjnej stanowi załącznik nr 7 do niniejszej procedury bezpieczeństwa.

5.4. Prawo dostępu do danych

5.4.1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji, takich jak:

1) cele przetwarzania;
2) kategorie odnośnych danych osobowych;
3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) informacje o prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
9) Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, informacje o odpowiednich zabezpieczeniach, związanych z przekazaniem.

5.4.2. Administrator dostarcza bezpłatnie osobie wnioskującej kopię danych osobowych jej dotyczących, podlegających przetwarzaniu - drogą elektroniczną, chyba że osoba, której dane dotyczą zaznaczyła, że żąda dostarczenia jej kopii danych drogą tradycyjną. W przypadku żądania kolejnej kopii przez tą osobę, administrator może pobrać opłatę odpowiadającą jego kosztom administracyjnym.

5.5. Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Ponadto osoba, której dane dotyczą, z uwzględnieniem celów przetwarzania, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

5.6. Prawo do usunięcia danych

5.6.1. Administrator jest zobowiązany na etapie pozyskiwania danych ustalić, przez jaki okres te dane będą przechowywane, bądź wskazać kryteria ustalenia tego okresu. Powyższe wskazuje się w rejestrze czynności przetwarzania. Po upływie ustalonego okresu dane osobowe powinny zostać usunięte.

5.6.2. Niezależnie od powyższego, na żądanie osoby, której dane dotyczą, administrator zobowiązany jest do niezwłocznego usunięcia dotyczących jej danych osobowych, jeżeli:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
3) osoba, której dane dotyczą, wnosi sprzeciw na mocy wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych do celów marketingu bezpośredniego;
4) dane osobowe były przetwarzane niezgodnie z prawem;
5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w przepisach prawa;
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego dziecku.

5.6.3. Przy ustalaniu okresu przechowywania danych należy ustalić, czy istnieją prawne obowiązki wymagające przetwarzania, którym podlega administrator, oraz czy przechowywanie danych nie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

5.6.4. W przypadku upublicznienia danych, które administrator ma obowiązek usunąć, administrator w miarę możliwości – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

5.7. Ograniczenie przetwarzania

5.7.1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania danych, gdy:

1) kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania
3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
4) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

5.7.2. W przypadku ograniczenia przetwarzania takie dane można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej.

5.7.3. Przed uchyleniem ograniczenia administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

5.8. Przenoszenie danych

5.8.1. Osoba, której dane dotyczą, ma prawo otrzymać dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się:

1) na podstawie zgody;
2) na podstawie umowy, której stroną jest osoba, której dane dotyczą;
3) przetwarzanie odbywa się w sposób zautomatyzowany.

5.8.2. Dane powinny zostać przekazane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

5.9. Prawo do sprzeciwu

5.9.1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw:

1) z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, w tym profilowania na podstawie tych przepisów.
2) w przypadku przetwarzania danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

5.9.2. Administratorowi nie wolno już przetwarzać danych osobowych, o których mowa w ust. 5.9.1. pkt. 1), chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

5.9.3. W przypadku wniesienia sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

6. Ogólne Zasady Bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

6.1. Zasady Ogólne

6.1.1. Za bez przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy mający dostęp do danych.

6.1.2. Każdy mający dostęp do danych osobowych nie może ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych. Obowiązek jest bezterminowy.

6.1.3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.

6.1.4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.

6.1.5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy

zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.

6.2. Określanie ryzyka

6.2.1. W celu sprawnego zarządzania zabezpieczeniami systemu informatycznego oraz ochrony danych osobowych, Administrator przed przystąpieniem do przetwarzania danych w nim zawartych i w jego trakcie jest zobowiązany do:

1) określenia metod zabezpieczenia systemu informatycznego;
2) określenia, i w miarę możliwości, wyeliminowania zagrożenia oraz zmniejszenia ryzyka przetwarzania danych osobowych;
3) określenia potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych z uwzględnieniem potrzeby kryptograficznej ochrony danych osobowych, w szczególności podczas ich przesyłania za pomocą urządzeń teletransmisji danych;
4) monitorowania działania zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania.

6.2.2. Administrator prowadzi, tam gdzie jest to możliwe, działania nad dostosowaniem aplikacji wykorzystywanych do przetwarzania danych osobowych, tak aby zapis (rekord) zawierający dane osobowe zawierał również następujące dane:

1) komu, kiedy i w jakim zakresie dane zostały udostępnione;
2) żądanie usunięcia danych osobowych, ich sprostowania, ograniczenia ich przetwarzania;
3) sprzeciw wobec przetwarzania danych osobowych lub wobec przekazania danych innemu administratorowi danych.

6.3. Niszczenie dokumentów

Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści z wykorzystaniem niszczarek. Zaleca się, aby niszczarka spełniała wymogi normy DIN 66399, klasa bezpieczeństwa nie niższa niż 3 lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu na piśmie umowy o powierzeniu przetwarzania danych osobowych.

6.4. Zasada czystego biurka i polityka kluczy

6.4.1. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej osoby mające dostęp do danych osobowych zobowiązane są do stosowania zasady tzw. „czystego biurka”. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym.

6.4.2. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.

6.4.3. Osoby mające dostęp do danych osobowych zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Osoby

mające dostęp do danych osobowych zobowiązane są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

6.4.4. Dokumenty i nośniki elektroniczne zabezpiecza się w specjalnie przeznaczonych do tego szafach lub pomieszczeniach. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każda z osób mająca dostęp do danych osobowych.

6.4.5. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.

6.4.6. Osoba która utraciła posiadane klucze do pomieszczeń Administratora w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność Administratorowi lub osobie upoważnionej czy Inspektorowi Ochrony Danych Osobowych, jeśli został ustanowiony.

6.4.7. Administrator lub osoby upoważnione podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

6.5. Pozostałe zasady:

6.5.1. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

6.5.2. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

6.5.3. Zabronione jest kopiowanie lub wykorzystywanie danych osobowych do celów innych niż służbowe. Zabronione jest samodzielne zapisywanie danych osobowych na zewnętrznych nośnikach danych (np. pamięci Flash/USB, smartfony, płyty CD-ROM/DVD-ROM, itp.). Powyższe nie dotyczy kopii zapasowych, dokonywanych przez upoważnionych pracowników Pionu Technologii (Działu Informatyki) lub kopii wykonywanych przez tych pracowników w przypadku uzasadnionych potrzeb biznesowych.

6.5.4. Regularnie tworzy się kopie zapasowe danych oraz kopie zapasowe systemu informatycznego używanego do ich przetwarzania. Szczegółowy tryb wykonywania kopii zapasowych i archiwizacji opisuje Instrukcja Zarządzania Systemem Informatycznym.

6.5.5. Dostęp użytkowników do sieci publiczne (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy, a dostęp do przeglądania stron internetowych możliwy jest po nadaniu odpowiednich uprawnień. Szczegółowy zapisy zawiera Instrukcja Zarządzania Systemem Informatycznym.

6.5.6. Zarządzanie dostępem do informacji w systemie informatycznym (uwierzytelnianie, przyznawanie i odbieranie identyfikatora, uprawnienia do operacji) szczegółowo określa Instrukcja Zarządzania Systemem Informatycznym.

6.5.7. Politykę haseł określa Instrukcja Zarządzania Systemem Informatycznym.

6.5.8. Zasady konserwacji i naprawy sprzętu informatycznego, w tym nośników danych, zawierających dane osobowe oraz zasady ich likwidacji określa Instrukcja Zarządzania Systemem Informatycznym.

7. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

7.1. Zabezpieczenia organizacyjne

7.1.1. W ramach zabezpieczeń organizacyjnych została opracowana u Administratora Procedura Ochrony Danych Osobowych.

7.1.2. Zastosowano także następujące zasady bezpieczeństwa:

1) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych;
2) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
3) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
4) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
5) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
6) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
7) stosuje się umowy powierzenia przetwarzania danych dla współpracy z podmiotami przetwarzającymi dane osobowe (procesorami).

7.2. Zabezpieczenia ochrony fizycznej danych osobowych

7.2.1. W organizacji stosuje się następujące zabezpieczenia ochrony fizycznej danych osobowych:

1) Monitoring
2) Alarm
3) ochrona całodobowa/system kontroli dostępu
4) gaśnice
5) szafy zamykane na klucz
6) szafy metalowe
7) rolety antywłamaniowe
8) ewidencja osób wchodzących i wychodzących.

7.2.2. Szczegółowy rodzaj zabezpieczenia danego zbioru określa Rejestr czynności przetwarzania prowadzony przez Administratora.

7.3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

7.3.1. Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

8. Powierzenie przetwarzania danych

8.1. Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, w tym w formie elektronicznej, przetwarzanie danych osobowych.

8.2. Administrator korzysta wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia, ustawy i chroniło prawa osób, których dane dotyczą.

8.3. Administrator musi udzielić uprzedniej szczegółowej lub ogólnej pisemnej zgody na korzystanie przez podmiot przetwarzający z usług innego podmiotu przetwarzającego. W przypadku udzielenia ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

8.4. Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.

8.5. Umowa powierzenia musi zawierać zapisy, o których mowa w art. 28 ust. 3 Rozporządzenia. Wzór umowy powierzenia stanowi załącznik nr 8 do procedury ochrony danych osobowych.

8.6. Administrator prowadzi rejestr podmiotów, którym powierzono przetwarzanie danych osobowych. Stanowi on załącznik nr 9 do procedury ochrony danych osobowych.

9. Naruszenie ochrony danych osobowych

Instrukcja definiuje katalog zagrożeń i naruszeń ochrony danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia naruszeń, ograniczenie ryzyka powstania zagrożeń i występowania naruszeń w przyszłości.

9.1. Definicje

9.1.1. Naruszeniem ochrony danych osobowych jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

9.1.2. Naruszeniem ochrony danych osobowych będą m.in.:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
3) 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)

9.1.3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych

3) nieprzestrzeganie zasad ochrony danych osobowych (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

9.2. Informowanie o naruszeniach ochrony danych osobowych

9.2.1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Generalnemu Inspektorowi Ochrony Danych Osobowych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

9.2.2. Zgłoszenia do Generalnego Inspektora Ochrony Danych Osobowych nie dokonuje się, jeżeli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Za takie ryzyko uważa się możliwość spowodowania:

1) kradzieży tożsamości;
2) straty finansowej;
3) naruszenia dobrego imienia;
4) naruszenia poufności danych chronionych tajemnicą zawodową,
5) utraty przysługujących osobom praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
6) ujawnienia danych wrażliwych.

9.2.3. O naruszeniu ochrony danych osobowych zawiadamia się bez zbędnej zwłoki osobę, której dane dotyczą, jeżeli naruszenie powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

9.2.4. Zawiadomienie nie jest wymagane, jeżeli Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony, które zostały zastosowane do danych osobowych, których dotyczy naruszenie lub zastosował następnie te środki, w szczególności takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

9.2.5. Zawiadomienia nie dokonuje się, jeżeli wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, tak by osoby, których dane dotyczą, zostały poinformowane w skuteczny sposób.

9.3. Procedura postępowania w przypadku zagrożenia naruszenia danych osobowych

9.3.1. W przypadku stwierdzenia wystąpienia zagrożenia, Inspektor Ochrony Danych Osobowych albo osoba upoważniona przez Administratora, jeżeli nie powołano Inspektora Ochrony Danych Osobowych, prowadzi sprawdzenie doraźne w toku, którego:

9.3.2. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

9.3.3. inicjuje ewentualne działania dyscyplinarne;

9.3.4. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

9.3.5. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;

9.3.6. dokumentuje prowadzone postępowania

9.4. Procedura postępowania w przypadku stwierdzenia naruszenia danych osobowych

9.4.1. W przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, należy poinformować Administratora, osobę przez nią upoważnioną lub Inspektora Ochrony Danych Osobowych, jeśli został wyznaczony.

9.4.2. Miejsce zdarzenia należy pozostawić w stanie nienaruszonym do czasu przybycia Inspektora Ochrony Danych Osobowych lub innej osoby upoważnionej przez Administratora.

9.4.3. Do obowiązków Inspektora Ochrony Danych lub innej osoby odpowiedzialnej, wyznaczonej przez administratora należą czynności związane z dokumentowaniem okoliczności naruszenia, tj.:

1) sporządzenie notatki z przeprowadzonych oględzin miejsca zdarzenia;
2) sporządzenie kopii obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem;
3) sporządzenie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu;
4) odebranie pisemnych wyjaśnień od osoby, która ujawniła naruszenie;
5) niezwłocznego przedstawienia zebranych materiałów administratorowi danych;.
6) przedstawienia administratorowi przez inspektora ochrony danych, jeśli został powołany, skutków naruszenia oraz środków i działań mających zaradzić naruszeniu, a także, jeżeli to konieczne, mających zminimalizować negatywne skutki naruszenia.

9.4.4. Na podstawie uzyskanych informacji Administrator z pomocą inspektora ochrony danych, albo innej osoby upoważnionej ocenia, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu oraz powiadomieniu osoby, której dane dotyczą.

9.4.5. W przypadku ustalenia, że istnieje obowiązek zgłoszenia organowi nadzorczemu oraz powiadomieniu osoby, której dane dotyczą, sporządza się zgłoszenie do organu nadzorczego oraz zawiadamia osobę, której dane dotyczą.

9.4.6. Administrator, osoba przez nią upoważniona lub Inspektor Ochrony Danych Osobowych, jeśli został wyznaczony dokumentuje skutki oraz podjęte środki i działania. Ponadto prowadzi się Rejestr Naruszeń, który stanowi Załącznik nr 1 do procedury ochrony danych osobowych.

10. <u>Kontrola przetwarzania i stanu zabezpieczenia danych osobowych</u>

10.1. Administrator bądź osoba przez niego wyznaczona, a w przypadku powołania Inspektor Ochrony Danych Osobowych dokonuje sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdanie w tym zakresie.

10.2. Sprawdzenie powinno dokonywać się, zgodnie z ustalonym planem sprawdzeń, chyba że konieczne jest dokonanie sprawdzenia doraźnego.

10.3. Plan sprawdzeń zawiera przedmiot, zakres, termin sprawdzeń oraz sposób i zakres ich dokumentowania.

10.4. Plan sprawdzeń przygotowywany jest na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany Administratorowi nie później niż

na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

10.5. Osoba dokonująca sprawdzenia zawiadamia Administratora o rozpoczęciu sprawdzenia doraźnego przed podjęciem pierwszej czynności.

10.6. Osoba dokonująca sprawdzenia zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności. Zawiadomienia nie przekazuje się w przypadku sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne.

10.7. Po zakończeniu sprawdzenia osoba dokonująca sprawdzenia przygotowuje sprawozdanie. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

11. Szkolenia

9.1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu i zapoznany z niniejszą procedurą ochrony danych osobowych.

9.2. Za przeprowadzenie szkolenia i zapoznania użytkowania odpowiada osoba wyznaczona przez Administratora, a jeśli został powołany Inspektor Ochrony Danych Osobowych.

9.3. Po szkoleniu lub po zapoznaniu się z niniejszą procedurą ochrony danych osobowych użytkownik zobowiązany jest do podpisania Oświadczenia użytkownika o poufności. Dokument ten, stanowiący Załącznik nr 3, jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

12. Postanowienia końcowe

1. Procedura Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie, za wyjątkiem wyciągu z Polityki Prywatności,
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Procedurze Ochrony Danych Osobowych dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Procedurze.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
5. W sprawach nieuregulowanych w niniejszej Procedurze Ochrony Danych Osobowych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy Rozporządzenia, Ustawy oraz wydanych na jej podstawie aktów wykonawczych.