POLITYKA BEZPIECZEŃSTA DANYCH OSOBOWYCH

Funkcje strategiczne dla przestrzegania PBDO:

Administrator Danych Osobowych: Patrycja Olszewska, e-mail: biuro@oxfordzik.pl, telefon: 509113291.

Administrator Systemów Informatycznych: brak.

Inspektor Ochrony Danych: Adam Kania, e-mail: inspektor@SuperIOD.pl, telefon: 609786984.

DOKUMENT USTANOWIŁ:	
DOKUMENT SPRAWDZIŁ:	
DOKUMENT ZATWIERDZIŁ:	
Dokument obowiązuje od 25 maja 2018 roku.	

SPIS TREŚCI

1. WYKAZ SKRÓTÓW

SKRÓT	OPIS
PUODO	Prezes Urzędu Ochrony Danych Osobowych.
ADO	Administrator Danych Osobowych.
ASI	Administrator Systemów Informatycznych.
IOD	Inspektor Ochrony Danych.
SI	System Informatyczny.
PBDO	Polityka Bezpieczeństwa Danych Osobowych.
IZSI	Instrukcja Zarządzania Systemem Informatycznym.
EOG	Europejski Obszar Gospodarczy
RODO	Rozporządzenie 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).

2. WYKAZ PODSTAWOWYCH DEFINICJI

Ilekroć w niniejszej **Polityce Bezpieczeństwa Danych Osobowych** mowa o:

1. **Administratorze Danych Osobowych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2. **Administratorze Systemu Informatycznego** – rozumie się przez to pracownika Administratora Danych Osobowych lub inne osoby odpowiedzialne za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;
3. **Inspektorze Ochrony Danych** – rozumie się przez to osobę odpowiedzialną za bieżący nadzór stosowania przepisów dot. ochrony danych osobowych;
4. **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Osobą upoważnioną może być pracownik Spółki, osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż;
5. **Danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);
6. **Możliwej do zidentyfikowania osobie fizycznej** - rozumie się przez to osobę, 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 określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7. **Przetwarzaniu danych osobowych** – rozumie się przez to 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;
8. **Zbiorze danych osobowych** – rozumie się przez to uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy

zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

9. **Podmiocie przetwarzającym** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych;
10. **Odbiorcy danych** - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postepowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
11. **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
12. **Bezpieczeństwie danych osobowych** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał ich poufność, integralność oraz dostępność;
13. **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
14. **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
15. **Dostępności danych** – rozumie się przez to właściwość zapewniającą, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;
16. **Zgodzie osoby, której dane dotyczą** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych;
17. **Państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
18. **Incydencie** – rozumie się przez to naruszenie bezpieczeństwa danych osobowych;
19. **Zagrożeniu** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;
20. **Naruszeniu ochrony danych osobowych** - rozumie się przez to naruszenie bezpieczeństwa danych osobowych 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.

3. WPROWADZENIE

Polityka Bezpieczeństwa Danych Osobowych określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w firmie **DZIECIĘCA AKADEMIA EDUKACJI I ZABAWY OXFORDZIK DAWID OBRACAJ SPÓŁKA KOMANDYTOWA, al. Harcerska 3B, 41-500 Chorzów, Polska; NIP: 6272729132, Regon: 241718506, KRS: 0000539753.** Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z 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

4. CELE POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Celem PBDO jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w firmie **DZIECIĘCA AKADEMIA EDUKACJI I ZABAWY OXFORDZIK DAWID OBRACAJ SPÓŁKA KOMANDYTOWA**, a w szczególności:

a. zapewnienie spełnienia wymagań prawnych;
b. zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w firmie;
c. podnoszenie świadomości osób przetwarzających dane osobowe;
d. zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

5. ZAKRES ROZPOWSZECHNIANIA PBDO

Z treścią niniejszej PBDO powinny zapoznać się wszystkie podmioty przetwarzające dane osobowe w imieniu Administratora Danych Osobowych, a także wszyscy pracownicy Administratora. Niniejsza PBDO będzie opublikowana na stronie www Administratora.

6. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Za bezpieczeństwo danych osobowych w firmie odpowiadają:

1. Administrator Danych Osobowych.
2. Inspektor Ochrony Danych.
3. Administrator Systemu Informatycznego.
4. Osoby upoważnione do przetwarzania danych osobowych.

7. PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

1. Wszystkie dane osobowe w firmie należy przetwarzać zgodnie z obowiązującymi przepisami prawa.
2. W stosunku do osób, których dane osobowe są przetwarzane należy spełnić obowiązek informacyjny wynikający z przepisów RODO.
3. Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami.
4. Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane.
5. Dane osobowe w firmie można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
6. Należy zapewnić poufność, integralność oraz rozliczalność danych osobowych przetwarzanych w firmie.
7. Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem.

8. Przetwarzanie danych osobowych w firmie może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej: kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
9. W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych.
10. Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

8. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

ADO upoważnia IOD do przetwarzania danych osobowych we wszystkich zbiorach ADO oraz poza nimi, w zakresie niezbędnym dla należytego wykonywania funkcji IOD, a także do wydawania w imieniu ADO upoważnień do przetwarzania danych osobowych.

9. OBOWIĄZKI I UPRAWNIENIA INSPEKTORA OCHRONY DANYCH

1. IOD monitoruje przestrzeganie zasad bezpieczeństwa oraz prowadzi kontrolę przetwarzania danych osobowych.
2. IOD wykonuje w szczególności następujące zadania:
   a. zapewnienia przestrzeganie przepisów o ochronie danych osobowych;
   b. stworzenie oraz wdrożenie zbioru odpowiednich praktyk, środków i sposobów postępowania w obszarze przetwarzania danych;
   c. przeszkolenie osób upoważnionych do przetwarzania danych zgodnie z wypracowanymi procedurami i praktykami;
   d. systematyczna kontrola przestrzegania wypracowanych zachowań przez osoby upoważnione do ich przetwarzania podczas audytów kontrolnych;
   e. doradztwo w sprawach wymagających interwencji IOD i/lub ich prowadzenie;
   f. reprezentowanie spółki w przypadkach kontroli organów nadzorczych;
   g. opiniowanie, pod względem zgodności z PBDO oraz z przepisami prawa umów, procedur i innych wytworzonych dokumentów dotyczących bezpieczeństwa i przetwarzania danych osobowych;
   h. podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych oraz prowadzenie adekwatnej dokumentacji w tym zakresie;
3. IOD uprawniony jest do:
   a. przeprowadzania zapowiedzianych audytów kontrolnych;
   b. wglądu w systemy informatyczne oraz dokumentację firmową związaną z przetwarzaniem powierzonych spółce danych osobowych w zakresie niezbędnym do prawidłowego sprawowania funkcji IOD;
   c. podejmowania stosownych działań w przypadku potencjalnego zagrożenia naruszenia bezpieczeństwa przetwarzanych danych osobowych, mających na celu jego eliminację.
4. IOD może wykonywać swoje obowiązki poprzez wyznaczonych zastępców za zgodą ADO.

10. POWOŁANIE (REJESTRACJA), ZMIANA I ODWOŁANIE INSPEKTORA OCHRONY DANYCH

1. Tylko Administrator Danych Osobowych może powołać IOD.
2. IOD może być osoba, która:

a. ma pełną zdolność do czynności prawnych oraz korzystania z pełni praw publicznych,
b. posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
c. nie była karana za umyślne przestępstwo.

3. Administrator Danych jest obowiązany zgłosić do rejestracji Prezesowi Urzędu Ochrony Danych Osobowych powołanie i odwołanie IOD w terminie do 14 dni od dnia jego powołania lub odwołania.
4. Zgłoszenie powołania i odwołania IOD dokonuje się w formie elektronicznej na odpowiednim formularzu poprzez stronę PUODO.
5. Administrator danych może powierzyć IOD wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania jego ustalonych zadań i nie spowoduje konfliktu interesu.
6. Administrator danych może powołać zastępców IOD, którzy spełniają warunki określone w punkcie 2.
7. IOD podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej Administratorem Danych.
8. W przypadku nie powołania IOD zadania jego, z wyłączeniem obowiązku sporządzenia sprawozdań, wykonuje Administrator Danych Osobowych.

11. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

a. zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami PBDO i IZSI;
b. stosowanie się do zaleceń wydanych przez IOD;
c. przetwarzanie danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez ADO w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
d. niezwłoczne informowanie IOD o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w firmie;
e. ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
f. korzystanie z systemów informatycznych firmy w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
g. bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
h. zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

12. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik PBDO/Z4) wydane przez ADO oraz złożyły stosowne oświadczenie dotyczące właściwej realizacji przepisów RODO (oświadczenia w załączniku PBDO/Z4).
2. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji stanowi załącznik PBDO/Z5).

13. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. ADO może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.
2. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych (wzór umowy stanowi załącznik PBDO/Z1) określa się przede wszystkim przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

14. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Dane osobowe udostępnia się na wniosek (według wzoru stanowiącego załącznik nr PBDO/Z3 do niniejszej PBDO) lub na podstawie umowy o udostępnienie danych osobowych (wzór umowy stanowi załącznik nr PBDO/Z2).
2. Wniosek o udostepnienie danych, który wpłynął do firmy rozpatruje ADO.
3. Wniosek o udostepnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany, wraz z informacjami niezbędnymi dla jego rozpatrzenia, do IOD w celu zajęcia stanowiska w sprawie. Do wniosku dołącza się projekt odpowiedzi ADO wraz z uzasadnieniem.
4. Informacje, zawierające dane osobowe są udostępniane uprawnionym podmiotom:
    a. w formie wydruku listem poleconym lub za potwierdzeniem osobistego odbioru,
    b. w drodze teletransmisji danych (w sposób gwarantujący poufność przesyłanych danych),
    c. na elektronicznych nośnikach informacji, za potwierdzeniem odbioru,
    d. w inny sposób określony przepisami prawa lub umową.
5. Udostępniane dane osobowe podlegają kontroli przez ADO, od którego one pochodzą.
6. Ewidencja przypadków udostepnienia danych prowadzona jest przez ADO w wersji elektronicznej lub papierowej według wzoru stanowiącego załącznik numer PBDO/Z7 do niniejszej PBDO.
7. Właściciel zbioru zobowiązany jest umożliwić dostęp IOD do prowadzonych ewidencji udostępnień.

15. PRZEKAZYWANIE DANYCH OSOBOWYCH POZA POLSKĘ

1. ADO może przekazywać dane osobowe do:
    a. państw Europejskiego Obszaru Gospodarczego;
    b. pozostałych państw (państwa trzecie).
2. Przekazywanie danych osobowych w ramach EOG traktuje się tak, jakby były przetwarzane na terenie Polski.
3. W przypadku przekazywania danych osobowych do państwa trzeciego, przekazywanie następuje zgodnie z Rozdziałem V art. 44 – 49 RODO.

16. WYKAZ OBSZARÓW PRZETWARZANIA DANYCH OSOBOWYCH

IOD na zlecenie ADO odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz budynków, pomieszczeń lub części pomieszczeń tworzący obszar, w którym przetwarzane są dane osobowe zarówno w formie papierowej jak i elektronicznej. Aktualny wykaz obszarów przetwarzania danych osobowych zawarto w załączniku PBDO/Z8.

17. WYKAZ PROGRAMÓW DO PRZETWARZANIA DANYCH OSOBOWYCH

IOD na zlecenie ADO odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Aktualny wykaz zbiorów danych osobowych zawarto w załączniku PBDO/Z9.

18. OPIS STRUKTURY ZBIRÓW DANYCH OSOBOWYCH

IOD na zlecenie ADO odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis struktury zbiorów danych osobowych przetwarzanych w firmie. Aktualny opis struktury zbiorów danych osobowych zawarto w załączniku PBDO/Z10.

19. OPIS PRZEPŁYWU DANYCH OSOBOWYCH MIĘDZY SYSTEMAMI

IOD na zlecenie ADO odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej opis sposobu przepływu danych pomiędzy poszczególnymi systemami. Aktualny opis sposobu przepływu danych zawarto w załączniku PBDO/Z11.

20. OPIS ŚRODKÓW OCHRONY DANYCH OSOBOWYCH

IOD na zlecenie ADO odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Aktualny opis stosowanych środków technicznych i organizacyjnych zawarto w załączniku PBDO/12.

21. ZARZĄDZANIE INCYDENTAMI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Szczegółowy sposób zarządzania incydentami dotyczącymi ochrony danych osobowych reguluje przyjęta przez firmę Procedura Zarządzania Incydentami Bezpieczeństwa Danych Osobowych (załącznik numer PBDO/PI1), a wzór zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych stanowi załącznik numer PBDO/PI2.

22. WZORY ZAŁĄCZNIKÓW

IOD na zlecenie ADO odpowiedzialny jest za projektowanie, prowadzenie oraz udostępnianie wzorów formularzy pomocniczych stanowiące załączniki do niniejszej PBDO. Dokumentacja prowadzona jest w konsultacji z ASI oraz lokalnymi IOD (jeśli funkcjonują). Wzory załączników prowadzona jest zarówno w formie papierowej jak i elektronicznej oraz udostępniania osobom upoważnionym do przetwarzania danych osobowych.

23. POLITYKA COOKIES

Polityka dotyczy plików cookies i odnosi się do stron internetowych Administratora:

a. www.Oxfordzik.pl – załącznik numer PBDO/PC1;

24. PRZEGLĄDY I AUDYTY PROCEDUR OCHRONY DANYCH

1. IOD zobowiązany jest przynajmniej raz na rok przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
2. Zakres, przebieg i rezultaty audytu należy udokumentować na piśmie w protokole podpisywanym przez ADO oraz IOD.
3. Prezes Ii/lub właściciel firmy może zlecić przeprowadzenie audytu zewnętrznego, także poprzez wyspecjalizowany podmiot.

4. Po przeprowadzonej kontroli IOD zobowiązany jest do zainicjowania działań korygujących i zapobiegawczych.
5. Raz w roku IOD przygotowuje sprawozdanie roczne stanu funkcjonowania procedur ochrony danych osobowych. Przygotowany raport przedstawiany jest prezesowi lub właścicielowi firmy.

25. DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE

1. IOD jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Źródłami informacji o incydentach, zagrożeniach lub słabościach są:
   a. zgłoszenia od pracowników;
   b. wyniki kontroli.
2. W przypadku, gdy IOD stwierdza konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
   a. źródło powstania incydentu lub zagrożenia;
   b. zakres działań korygujących lub zapobiegawczych;
   c. termin realizacji;
   d. osobę odpowiedzialną.
3. IOD jest odpowiedzialny za nadzór nad poprawą i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po wprowadzeniu działań korygujących lub zapobiegawczych, IOD jest zobowiązany do oceny efektywności ich zastosowania.

26. PRZEPISY KARNE I PORZĄDKOWE

1. Wobec osoby, która w przypadku naruszenia zasad ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiednich osób zgodnie z określonymi zasadami, można wszcząć postępowanie dyscyplinarne.
2. Osoba upoważniona dopuszczająca się nieuprawnionego ujawniania lub wykorzystywania danych osobowych w sposób sprzeczny z ich przeznaczeniem, czy też ich przetwarzania w sposób niezgodny z przyjętymi w firmie zasadami i procedurami, może zostać ukarany karą upomnienia lub karą nagany.
3. Naruszenie zasad ochrony danych osobowych przez osobę upoważnioną przez ADO do przetwarzania danych osobowych może skutkować postawieniem zarzutu popełnienia jednego z przestępstwa określonych w Rozdziale 10 UODO lub przestępstwa określonego w art. 266 Kodeksu Karnego.
4. Przepisy karne i porządkowe reguluje:
   a. Rozporządzenie 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);
   b. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).
   c. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 1998 r., Nr 21, poz. 94, z późn. zm.).

27. POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy Rozporządzenia 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).

28. SPIS ZAŁĄCZNIKÓW

a. PBDO/Z1 – wzór Umowy Powierzenia Przetwarzania Danych Osobowych (UPPDO);
b. PBDO/Z2 – wzór Umowy Udostępnienia Danych Osobowych (UUDO);
c. PBDO/Z3 – wzór Wniosku o Udostępnienie Danych ze Zbioru Danych Osobowych (WUDO);
d. PBDO/Z4 – wzór Upoważnienia Przetwarzania Danych Osobowych (UPDO);
e. PBDO/Z5 – wzór Ewidencji Osób Upoważnionych do Przetwarzania Danych Osobowych (EUPDO);
f. PBDO/Z6 – wzór Wniosku o Udostępnienie Danych ze Zbioru Danych Osobowych (WUDO);
g. PBDO/Z7 – wzór Ewidencji Udostępnień Danych ze Zbioru Danych Osobowych (EUDO);
h. PBDO/Z8 – wzór Ewidencji Obszarów Przetwarzania Danych Osobowych (WOPDO);
i. PBDO/Z9 – wzór Wykazu Zbiorów Danych Osobowych (WZDO);
j. PBDO/Z10 – wzór Opisu Struktury Zbiorów Danych Osobowych (OSZDO);
k. PBDO/Z11 – wzór Opisu Sposobu Przepływu Danych Osobowych (OSPDO);
l. PBDO/Z12 – wzór Opis Stosowanych Środków Technicznych i Organizacyjnych (OSŚTiO);
m. PBDO/Z13 – wzór Zgody na Przetwarzanie Danych Osobowych (ZPDO);
n. PBDO/Z14 – wzór Zgody Rozszerzonej na Przetwarzanie Danych Osobowych (ZRPDO);
o. PBDO/PI1 – Procedura Zarządzania Incydentami Bezpieczeństwa Danych Osobowych (PZIBDO).
p. PBDO/PI2 – wzór Zawiadamiania Osoby, której Dane Dotyczą, o Naruszeniu Ochrony Danych Osobowych (ZNODO);
q. PBDO/PC1 – Polityka Cookies dla strony www.Oxfordzik.pl.