POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Nazwa Administratora: Właścicielem danych jest Openity Sp. z o.o. (daw. Census Agnieszka Buczkowska) z siedzibą w Skórzewie przy ul. Poznańskiej 99 (60-185 Skórzewo), o numerze KRS 0000953194, o numerze NIP: 7773386057, o numerze REGON: 521376408, prowadząca również działalność oświatową pod nazwą: CENTRUM KREACJI MULTIMEDIALNEJ z siedzibą w Poznaniu 61-818 przy ul. Taczaka 10, NIEPUBLICZNA POLICEALNA WIELKOPOLSKA SZKOŁA FOTOGRAFII z siedzibą w Poznaniu 61-818 przy ul. Taczaka 10, NIEPUBLICZNA POLICEALNA WROCŁAWSKA SZKOŁA FOTOGRAFII z siedzibą we Wrocławiu 50-020 przy ul. Piłsudskiego 74.

ul. Poznańska 99, 60-185 Skórzewo

Numer KRS : 0000953194

Adres e-mail: abuczkowska@kursfoto.pl

Nr telefonu: 790-777-001

niezbędnikRODO.pl

Spis treści

I WPROWADZENIE

Polityka Bezpieczeństwa Danych Osobowych, zwana dalej Polityką bezpieczeństwa, została sporządzona w związku z wymaganiami 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 – dalej Rozporządzenie UE) oraz ustawy o ochronie danych osobowych.

Niniejszy dokument stanowi zbiór spójnych, precyzyjnych reguł i procedur, według których Podmiot buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Ustanawia przewidziane do wykonania działania oraz sposób ustanowienia zasad i reguł postępowania, koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych. Polityka bezpieczeństwa ustanawia zasady bezpieczeństwa przetwarzania danych osobowych, które powinny być przestrzegane i stosowane w Podmiocie przez wszystkie osoby przetwarzające dane osobowe. Polityka bezpieczeństwa reguluje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych w systemie informatycznym oraz metodami tradycyjnymi. Opisano w niej również zagrożenia bezpieczeństwa przetwarzanych danych osobowych oraz sposoby reakcji na przypadki naruszeń bezpieczeństwa.

Niniejszy dokument pełni również funkcję informacyjną i edukacyjną, poprzez zaprezentowanie obowiązków i odpowiedzialności osób związanych z przetwarzaniem danych osobowych.

Podmiot stosuje adekwatne do sytuacji środki, aby zapewnić bezpieczeństwo przetwarzanych danych osobowych.

Podmiot nie podjął decyzji o powołaniu Inspektora Ochrony Danych i Administratora Systemu Informatycznego. Ich obowiązki w zakresie dopuszczalnym prawem, zobowiązany jest sprawować Administrator Danych Osobowych.

PODSTAWA PRAWNA

Zasady przetwarzania danych osobowych regulują przepisy powszechnie obowiązującego prawa, a w szczególności:

- 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
- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

SŁOWNICZEK

ADO – Administrator danych osobowych, Właścicielem danych jest Openity Sp. z o.o. (daw. Census Agnieszka Buczkowska) z siedzibą w Skórzewie przy ul. Poznańskiej 99 (60-185 Skórzewo), o numerze KRS 0000953194, o numerze NIP: 7773386057, o numerze REGON: 521376408, prowadząca również działalność oświatową pod nazwą: CENTRUM KREACJI MULTIMEDIALNEJ z siedzibą w Poznaniu 61-818 przy ul. Taczaka 10, NIEPUBLICZNA POLICEALNA WIELKOPOLSKA SZKOŁA FOTOGRAFII z siedzibą w Poznaniu 61-818 przy ul. Taczaka 10, NIEPUBLICZNA POLICEALNA WROCŁAWSKA SZKOŁA FOTOGRAFII z siedzibą we Wrocławiu 50-020 przy ul. Piłsudskiego 74.

ASI – Administrator Systemu Informatycznego, będący wyznaczoną przez ADO osobą odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i ich konserwację, w zakresie wskazanym przez ADO.

Dane osobowe - wszelkie informacje dotyczące 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 określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane wrażliwe (szczególna kategoria danych) - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej oraz dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Hasło — ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Identyfikator użytkownika — ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Integralność danych — właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

IOD – Inspektor Ochrony Danych, będący wyznaczoną przez Administratora Danych Osobowych osobą nadzorującą stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez IOD lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

Podmiot – podmiot wskazany na pierwszej tytułowej stronie Polityki bezpieczeństwa, dla celów którego niniejsza Polityka bezpieczeństwa zostaje opracowana i wdrożona**.**

Polityka bezpieczeństwa – niniejszy dokument Polityki Bezpieczeństwa Danych Osobowych.

Poufność danych — właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym osobom lub podmiotom.

Przetwarzanie danych – oznacza 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.

PUODO – Prezes Urzędu Ochrony Danych Osobowych, będący organem powołanym do spraw z zakresu ochrony danych osobowych**.**

Rozliczalność — właściwość zapewniająca, że działania osoby na danych osobowych mogą być przypisane w sposób jednoznaczny tylko tej osobie, nadto właściwość zapewniająca możliwość udowodnienia realizacji praw osób, których dane osobowe są przetwarzane.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Usuwanie danych – zniszczenie danych osobowych lub ich modyfikacja, która uniemożliwia ustalenie tożsamości osoby, której dane dotyczą.

Uwierzytelnianie — działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby lub podmiotu.

Zabezpieczenie danych w systemie informatycznym –wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

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 – oznacza 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.

II OGÓLNA INSTRUKCJA DLA ADO / IOD / ASI

Niniejsza instrukcja jest przeznaczona dla ADO i IOD oraz ASI w przypadku powołania.

OBOWIĄZKI ADO

1. zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia, w szczególności poprzez stosowanie obowiązków informacyjnych, zgodnych z szablonem obowiązku informacyjnego (**zał. nr 1.1 lub 1.2**).
2. dbałość o prawidłowe przetwarzanie danych osobowych, w szczególności poprzez zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,
3. dbałość o prawidłową realizację zasady czasowości, w szczególności poprzez zapewnienie usuwania danych osobowych po czasie niezbędnego ich przetwarzania,
4. wdrożenie procedur i środków bezpieczeństwa zapewniających prawidłowe przetwarzanie danych osobowych,
5. analiza ryzyka wdrażanych i wdrożonych procedur, środków bezpieczeństwa, zasobów i procesów przetwarzania danych osobowych (**zał. nr 2**),
6. egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych,
7. prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka bezpieczeństwa oraz wynikające z niej instrukcje i procedury),
8. prowadzenie rejestru czynności przetwarzania danych osobowych (**zał. nr 3**)
9. nadawanie i uchylanie upoważnień do przetwarzania danych osobowych w Podmiocie przez pracowników (**zał. nr 4**) oraz upoważnień do przetwarzania danych osobowych w Podmiocie przez osoby zatrudnione na podstawie umów cywilnoprawnych (**zał. nr 5**),
10. prowadzenie rejestru pracowników upoważnionych do przetwarzania danych (**zał. nr 6**) i rejestru osób zatrudnionych na podstawie umowy cywilnoprawnej upoważnionych do przetwarzania danych osobowych (**zał. nr 7**),
11. wdrożenie środków zapoznania z przepisami dotyczącymi ochrony danych osobowych i zasadami w tym przedmiocie oraz zagrożeniami związanymi z przetwarzaniem danych przez pracowników Podmiotu,
12. zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z zasadami przetwarzania danych osobowych,
13. prowadzenie zgodnych z Instrukcją działań w przypadku stwierdzenia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
14. w przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – dokonuje ich zgłoszenia do PUODO (**zał. nr 8**), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
15. analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie zaleceń i rekomendacji dotyczących eliminacji ryzyka ich ponownego wystąpienia,
16. mierzenie, testowanie i ocena skuteczności wdrożonej Polityki bezpieczeństwa i środków bezpieczeństwa.

OBOWIĄZKI INSPEKTORA OCHRONY DANYCH

W przypadku braku powołania IOD, niniejsze obowiązki stosuje się odpowiednio względem ADO.

1. informowanie ADO oraz jego pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia UE oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
2. monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk ADO lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
3. prowadzenie rejestru czynności przetwarzania danych osobowych (**zał. nr 3**)
4. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
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. 36 Rozporządzenia UE, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
7. w przypadku, gdy zachodzi ku temu przesłanka, pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia UE.

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

IOD, a w przypadku braku jego wyznaczenia ADO, prowadzi rejestr czynności przetwarzania danych osobowych (**zał. nr 3**), za które odpowiada. W rejestrze tym zamieszcza wszystkie następujące informacje:

1. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
2. cele przetwarzania;
3. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi Rozporządzenia UE, dokumentacja odpowiednich zabezpieczeń;
6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
7. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Wyłączenie obowiązku prowadzenia rejestru czynności przetwarzania stosuje się w przypadkach określonych w art. 30 pkt 5 Rozporządzenia.

ANALIZA RYZYKA

IOD, a w przypadku braku jego wyznaczenia ADO, przeprowadza analizę ryzyka.

Poszczególne:

1. czynności przetwarzania danych osobowych,
2. istotne zasoby Podmiotu (takie jak serwer, serwerownia, archiwum),
3. wdrożone środki bezpieczeństwa,

należy poddać analizie ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

Analizę ryzyka należy przeprowadzać uwzględniając:

1. charakter przetwarzania danych osobowych,
2. zakres przetwarzania danych osobowych,
3. kontekst przetwarzania danych osobowych,
4. cele przetwarzania danych osobowych,
5. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Na podstawie przeprowadzonej analizy ryzyka, wdraża się odpowiednie środki techniczne i organizacyjne, w celu zapewnienia przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, a także w celu możliwości wykazania tak okoliczności.

Przyjęte środki bezpieczeństwa są w razie potrzeby poddawane przeglądom i uaktualniane.

Oceniając, czy stopień bezpieczeństwa wdrożonych środków jest odpowiedni, uwzględnia się w szczególności ryzyko związane z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

ŚRODKI BEZPIECZEŃSTWA

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, ADO wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem UE i aby móc to wykazać. Środki te są poddawane przeglądom i uaktualniane co najmniej raz w roku. Jeżeli zachodzi taka konieczność okres ten może ulec skróceniu.

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, ADO i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W opisie organizacyjnych środków bezpieczeństwa wykazanych w rejestrze czynności przetwarzania danych osobowych, wymienia się wszelkie środki organizacyjne, przyjęte w celu zapewnienia bezpieczeństwa systemu przetwarzania danych osobowych.

W zakresie technicznych środków bezpieczeństwa wykazanych w rejestrze czynności przetwarzania danych osobowych, wymienia się wszelkie środki techniczne, wdrożone w celu zapewnienia bezpieczeństwa systemu przetwarzania danych osobowych.

PROCEDURA UDOSTĘPNIANIA KLUCZY DO POMIESZCZEŃ, W KTÓRYCH PRZETWARZA SIĘ DANE

1. Klucze do poszczególnych pomieszczeń służbowych są w ciągłym posiadaniu pracowników, którzy własnoręcznie podpisali protokół zdawczo – odbiorczy przekazania kluczy, potwierdzając tym samym ich odbiór, ponosząc pełną odpowiedzialność za ich należyte zabezpieczenie. (Wzór protokołu zdawczo-odbiorczego stanowi załącznik **Nr 9).**
2. Kluczy nie wolno przekazywać / udostępniać innej osobie pod żadnym pozorem.
3. Drzwi otwiera i zamyka wyłącznie pracownik, który pokwitował odbiór kluczy.
4. Pomieszczenie służbowe, w którym chwilowo nie przebywa żaden pracownik powinno być zamknięte na klucz.
5. Klucze od szafek stanowiskowych, szaf biurowych oraz kasetek metalowych są w ciągłym posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
6. Po otwarciu pomieszczeń służbowych, jeszcze przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w danym pomieszczeniu dokumentacji.
7. W przypadku zauważenia naruszenia zabezpieczeń, pracownicy zobowiązani są do niezwłocznego poinformowania o tym fakcie ADO.
8. W trakcie pracy pracownicy zobowiązani są do:
   a) Zwrócenia uwagi na zachowanie osób wchodzących i wychodzących z pomieszczeń Podmiotu,
   b) Reagowanie na wejście do pomieszczeń Podmiotu osób będących pod wpływem alkoholu lub środków odurzających,
   c) Reagowania na próby niszczenia lub wynoszenia mienia Podmiotu,
   d) Reagowania na próby wnoszenia do pomieszczeń Podmiotu przedmiotów niebezpiecznych, materiałów lub substancji budzącej podejrzenie,

e) natychmiastowego reagowania poprzez powiadomienie odpowiednich służb (Straż Miejska, Policja, Straż Pożarna, Pogotowie Ratunkowe) o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia

9. Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swojego stanowiska pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności: wylogowanie się z systemu oraz sprzętu na którym przetwarza się dane osobowe, schowanie dokumentacji w wersji papierowej do szaf, zamknięcia okien i drzwi.

10. Zgubienie kluczy, przekazanie ich innej osobie lub utrata w jakikolwiek inny sposób grożący wyciekiem danych osobowych może skutkować dla pracownika konsekwencjami służbowym lub dyscyplinarnymi. Po utracie klucza należy wymienić zamki, do których przeznaczone były utracone klucze.

11. Po zakończeniu stosunku pracy pracownik zobowiązany jest do zdania kompletu kluczy oraz uzupełnienia protokołu zdawczo – odbiorczego przekazania kluczy, z własnoręcznym podpisem.

12. ADO zobowiązany jest do uzupełniania rejestru pracowników otrzymujących i zdających klucze.

13. ADO dopuszcza odpłatne korzystania z pomieszczeń służbowych Podmiotu przez osoby postronne (wyłącznie dot. wynajmu pomieszczeń szkoleniowych typu: studio fotograficzne, pracownia komputerowa, ciemnia fotograficzna) bez konieczności podpisywania wewnętrznego protokołu zdawczo – odbiorczego przekazania kluczy.

14. W przypadku odpłatnego korzystania z pomieszczeń służbowych Podmiotu, pracownik zobowiązany jest do wpisania osoby korzystającej do właściwego rejestru. Dodatkowo zobowiązany jest do przekazania informacji do portierni właściwego budynku dot. osoby pobierającej klucz do pomieszczenia służbowego, w tym: imienia i nazwiska osoby korzystającej, daty i godziny najmu.

15. Zabrania się:
    a) Dorabiania kluczy do pomieszczeń bez zgody ADO
    b) Udostępniania kluczy osobom nieupoważnionym
    c) Pozostawiania otwartych pomieszczeń lub kluczy bez nadzoru

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. W Podmiocie do przetwarzania danych osobowych uprawnione są wyłącznie osoby upoważnione do przetwarzania danych osobowych.
2. Celem niniejszej procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty ich poufności przez osoby nieupoważnione.
3. ADO jest uprawniony do przyznawania upoważnień (poleceń) w przedmiocie przetwarzania danych osobowych, w drodze pisemnego upoważnienia do przetwarzania danych osobowych (**zał. nr 4** dla pracowników i **zał. nr 5** dla osób współpracujących na podstawie umów cywilnoprawnych/umów współpracy),

4. ADO może wyznaczyć osoby uprawnione do przyznawania upoważnień w przedmiocie przetwarzania danych osobowych, w drodze pisemnego uprawnienia.
5. Upoważnienie do przetwarzania danych osobowych następuje wyłącznie na podstawie indywidualnego upoważnienia.
6. Upoważnienie do przetwarzania danych osobowych wydane dal osób współpracujących na podstawie umów cywilnoprawnych / umów współpracy uznaje się za przedłużone jeśli z osobami tymi przedłużane są te same umowy cywilnoprawne / umowy współpracy bez zmiany zakresu dostępu do danych.
7. Nadanie upoważnienia do przetwarzania danych osobowych musi nastąpić przed rozpoczęciem przetwarzania danych osobowych przez osobę upoważnioną.
8. ADO lub osoba przez niego upoważniona prowadzi dokument rejestru osób upoważnionych do przetwarzania danych osobowych na podstawie umowy o pracę **(zał. nr 6)** i na podstawie umów cywilnoprawnych/umów współpracy **(zał. nr 7)**.
9. W przypadku konieczności nadania bądź zmiany uprawnień (np. z powodu zatrudnienia osoby lub zmiany stanowiska pracy), ADO lub osoba przez niego upoważniona zobowiązany jest do sprawdzenia, czy dana osoba:
    a. odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych,
    b. będzie przetwarzała dane osobowe w zakresie i celu określonym w Polityce i instrukcji zarządzania systemem informatycznym.
10. Nadanie upoważnienia do przetwarzania danych osobowych wymaga zaznajomienia się z niniejszą Polityką bezpieczeństwa i przepisami dotyczącymi ochrony danych osobowych, w zakresie niezbędnym do czynności wykonywanych w ramach udzielonego upoważnienia.
11. ADO jest odpowiedzialny za organizację i przeprowadzenie szkoleń z zasad przetwarzania danych osobowych lub zaznajomienie w innej formie osób upoważnionych z zasadami ochrony danych osobowych.

PROCEDURA POSTĘPOWANIA Z NARUSZENIEM ZASAD OCHRONY DANYCH DLA ADO / IOD

Naruszeniem ochrony danych osobowych jest 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. W przypadku wystąpienia naruszenia ochrony danych osobowych należy uruchomić procedurę postępowania z naruszeniem, opisaną poniżej.

W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych ADO jest zobowiązany niezwłocznie:

1. poinformować osobę zgłaszającą o dalszym trybie postępowania i zalecić jej właściwe czynności,
2. w miarę możliwości przywrócić stan zgodny z zasadami ochrony danych osobowych,

3. ustalić czas trwania i charakter naruszenia, w miarę możliwości określając kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
4. ustalić możliwe konsekwencje naruszenia ochrony danych osobowych,
5. zarekomendować działania zapobiegawcze w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
6. w przypadku zaistnienia przesłanek określonych w Rozporządzeniu UE, zgłosić naruszenie w ciągu 72 godzin do PUODO, z uwzględnieniem informacji zamieszczonych w szablonie zgłoszenia naruszenia do PUODO (**zał. nr 8**),
7. w razie konieczności zainicjować działania dyscyplinarne,
8. udokumentować prowadzone postępowanie w rejestrze naruszeń bezpieczeństwa danych osobowych (**zał. nr 10**).

III OGÓLNA INSTRUKCJA DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

Niniejsza instrukcja jest przeznaczona dla ADO i ASI w przypadku powołania. W przypadku braku powołania ASI, niniejszą instrukcję i procedury stosuje się odpowiednio względem ADO.

OBOWIĄZKI ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

1. właściwa konfiguracja systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, w celu zapewnienia jego zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
2. dbałość o utrzymanie i zabezpieczenie serwerów systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, niezależnie od tego czy serwer znajduje się w zasobach lokalowych Podmiotu, czy poza nim, a w szczególności zapewnienie jego poufności, integralności, dostępności i odporności,
3. zapewnianie zdolności systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, 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 systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie, mających zapewnić bezpieczeństwo przetwarzania danych osobowych z jego użyciem,
5. instalacja, konfiguracja, usuwanie, zamawianie licencji i ich przedłużanie, w odniesieniu do oprogramowania używanego w urządzeniach teleinformatycznych stosowanych w systemie teleinformatycznym Podmiotu,
6. nadzór nad pracami podmiotów zewnętrznych, przeprowadzających prace przy naprawach, konserwacjach systemów informatycznych służących do przetwarzania danych osobowych w Podmiocie, w celu zapewnienia zgodności tych czynności z zasadami przyjętymi w Podmiocie,
7. nadawanie, zmiana i wycofywanie identyfikatorów i haseł oraz uprawnień do korzystania z aplikacji i programów osobom upoważnionym do przetwarzania danych osobowych w Podmiocie,
8. nadzór nad prawidłowym wdrożeniem i funkcjonowaniem systemu sporządzania kopii bezpieczeństwa wszelkich nośników informacji, służących do przetwarzania danych osobowych w Podmiocie, zgodnie z przyjętą polityką tworzenia kopii zapasowych w Podmiocie,

9. podejmowanie działań w przypadku podejrzenia lub wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie,
10. świadczenie pomocy technicznej w zakresie obsługi oprogramowania i urządzeń używanych w ramach systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie,
11. zabezpieczenie komputerów przenośnych służących do przetwarzania danych osobowych w Podmiocie,
12. pozostałe działania przewidziane Polityką bezpieczeństwa.

PROCEDURA EWIDENCJONOWANIA

ADO jest zobowiązany do ewidencjonowania wszelkich czynności wykonywanych w systemie informatycznym służącym do przetwarzania danych osobowych w Podmiocie, a także do ewidencjonowania urządzeń i nośników, służących do przetwarzania danych osobowych. Ewidencjonowanie następuje w:

1. Rejestrze napraw, przeglądów i konserwacji systemu informatycznego (**zał. nr 11**),
2. Rejestrze urządzeń i nośników, służących do przetwarzania danych osobowych (**zał. nr 12**).

PROCEDURA WYKONYWANIA KONTROLI DOSTĘPU DO SYSTEMU

Ustanawia się poniższe wymogi dotyczące kontroli dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w Podmiocie. ADO jest zobowiązany do monitorowania i zapewnienia ich przestrzegania.

1. W systemie informatycznym służącym do przetwarzania danych osobowych w Podmiocie stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych osobowych przetwarzanych w systemie informatycznym (w szczególności do urządzenia, aplikacji lub programu, posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
    a. w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
    b. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
3. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
    a. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
    b. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
4. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być przydzielony innej osobie.
5. W przypadku, gdy do uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych używa się hasła, wdraża się środki wymuszające stosowanie haseł składających się co najmniej z 8 znaków, w tym małych i wielkich liter oraz cyfr lub znaków specjalnych.

PROCEDURA ZABEZPIECZENIA ANTYWIRUSOWEGO

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe. Ustanawia się poniższe wymogi dotyczące ochrony antywirusowej. ADO jest zobowiązany do monitorowania i zapewnienia ich przestrzegania.

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.
2. Za zaplanowanie i zapewnienie ochrony antywirusowej, w tym za zapewnienie odpowiedniej ilości licencji odpowiada ADO.
3. Każdy plik wczytywany do urządzenia informatycznego, w tym także wiadomość e-mail, podlega przetestowaniu programem antywirusowym.
4. W każdym urządzeniu informatycznym wyposażonym w dostęp do internetu, musi być zainstalowanie oprogramowanie antywirusowe.
5. Aktualizacja definicji wirusów odbywa się automatycznie przez system.

PROCEDURA TWORZENIA KOPII ZAPASOWYCH

Ustanawia się poniższe wymogi dotyczące wykonywania kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym Podmiotu. ADO jest zobowiązany do bezpośredniej realizacji ich przestrzegania.

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych tych danych:
    a) w przypadku korzystania z usług operatorów hostingu, zgodnie z ofertą hostingodawcy
    b) w przypadku korzystania z własnych serwerów w zależności od typu urządzenia oraz danych co najmniej raz w miesiącu
2. Za sporządzanie kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym operatora hostingu odpowiedzialny jest odpowiedni hostingodawca.
3. Kopie zapasowe danych osobowych znajdujących się na sprzęcie Podmiotu wykonuje ADO.
4. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
5. Kopie zapasowe powinny być cyklicznie kontrolowane przez ADO, w szczególności pod kątem prawidłowości ich wykonania oraz możliwości odtworzenia, poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym. W przypadku usług hostingowych kopie zapasowe powinny być kontrolowane w miarę możliwości.
6. Nośniki zawierające kopie danych osobowych przetwarzanych w systemie informatycznym Podmiotu są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
7. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

PROCEDURA EWIDENCJONOWANIA URZĄDZEŃ I NOŚNIKÓW

Ustanawia się poniższe wymogi dotyczące ewidencjonowania urządzeń i nośników informacji, służących do przetwarzania danych osobowych w Podmiocie. ADO jest zobowiązany do prowadzenia ich rejestru.

1. Należy zewidencjonować wszystkie urządzenia i nośniki służące do przetwarzania danych osobowych w Podmiocie, poprzez wprowadzenie ich do pisemnego rejestru urządzeń i nośników, służących do przetwarzania danych osobowych (**zał. nr 12**).
2. Przed dopuszczeniem do użycia nowych urządzeń i nośników służących do przetwarzania danych osobowych w Podmiocie, należy je zewidencjonować.
3. Po usunięciu urządzenia lub nośnika służącego do przetwarzania danych osobowych w Podmiocie, należy wykreślić go z Rejestru urządzeń i nośników, służących do przetwarzania danych osobowych.

PROCEDURA USUWANIA URZĄDZEŃ I NOŚNIKÓW

Ustanawia się poniższe wymogi dotyczące usuwania nośników informacji, służących do przetwarzania danych osobowych w Podmiocie. ADO jest zobowiązany do bezpośredniej realizacji ich przestrzegania.

1. Nośniki informacji służące do przetwarzania danych osobowych w Podmiocie pozbawia się tych danych przed usunięciem, a następnie poddaje się je procedurze przynajmniej dwukrotnego całkowitego nadpisywania.
2. W przypadku braku możliwości o której stanowi pkt wyżej, (np. płyty CD, uszkodzone dyski twarde) nośniki informacji służące do przetwarzania danych osobowych w Podmiocie, przed usunięciem poddaje się innym czynnościom skutkującym ich trwałemu fizycznemu uszkodzeniu, uniemożliwiającemu odczytanie danych zgromadzonych na nośniku.
3. Po usunięciu urządzenia lub nośnika służącego do przetwarzania danych osobowych w Podmiocie, należy wykreślić go z Rejestru urządzeń i nośników, służących do przetwarzania danych osobowych.

PROCEDURA PRZEGLĄDÓW I KONSERWACJI

Ustanawia się poniższe wymogi dotyczące realizacji przeglądów, napraw i konserwacji systemu informatycznego, służącego do przetwarzania danych osobowych. Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem. ADO jest zobowiązany do monitorowania i zapewnienia ich przestrzegania.

1. Przeglądy, naprawy i konserwacje urządzeń informatycznych służących do przetwarzania danych osobowych, przeprowadzane są w lokalizacji Podmiotu przez ADO, z zastrzeżeniem poniższych warunków.
2. Naprawy i konserwacje urządzeń informatycznych służących do przetwarzania danych osobowych mogą być wykonywane przez przedsiębiorstwa lub wykonawców zewnętrznych wyłącznie na podstawie zleceń z wyłączeniem naprawy i konserwacji urządzeń informatycznych należących do dostawcy usług hostingowych.
3. W przypadku przekazywania do naprawy urządzeń informatycznych służących do przetwarzania danych osobowych:
    a. jeśli uszkodzenie dotyczy nośników pamięci, należy zniszczyć je, przywracając pliki zawierające dane osobowe z kopii zapasowej,

b. jeśli uszkodzenie dotyczy nośników pamięci a jednocześnie brak jest plików zawierających dane osobowe, wówczas należy zrealizować naprawę pod bezpośrednim nadzorem osoby upoważnionej albo po zawarciu umowy powierzenia danych osobowych.

4. ADO jest zobowiązany wykonywać przynajmniej wyrywkowe przeglądy techniczne urządzeń służących do przetwarzania danych osobowych nie rzadziej niż raz w roku. W przypadku usług hostingowych przeglądy techniczne powinny być wykonywane w miarę możliwości.
5. ADO prowadzi rejestr napraw, przeglądów i konserwacji systemu informatycznego (**zał. nr 11**) z wyłączeniem systemu zarządzanego przez operatora hostingu.

IV OGÓLNA INSTRUKCJA DLA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ DLA ADO.

Niniejsza instrukcja jest przeznaczona dla wszystkich osób przetwarzających dane osobowe w Podmiocie, a także dla ADO.

OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Każda osoba jest uprawniona do przetwarzania danych osobowych tylko po otrzymaniu upoważnienia do tej czynności. Do obowiązków osób upoważnionych do przetwarzania danych osobowych, należy postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych, a w szczególności:

1. zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po ustaniu zatrudnienia lub innego stosunku cywilnoprawnego,
2. niewykorzystywanie w celach pozasłużbowych danych osobowych i programów służących do przetwarzania danych osobowych w Podmiocie,
3. zabezpieczanie obszaru, w którym przetwarza się dane osobowe przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych, przy użyciu środków zapewnionych przez ADO,
4. zapewnianie, aby przebywanie osób nieupoważnionych do przetwarzania danych osobowych w obszarze ich przetwarzania, następowało wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych i pod jej nadzorem,
5. informowanie ADO o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe,
6. niezwłoczne przekazywanie ADO wszelkich zgłoszeń dotyczących przetwarzania danych osobowych przez Podmiot,
7. realizacja obowiązku informacyjnego w stosunku do osób, których dane osobowe są przetwarzane przez Podmiot, w przypadku gdy to osoba upoważniona jest osobą zbierającą te dane,
8. używanie wyłącznie programów i aplikacji dopuszczonych do używania przez ADO,
9. ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
10. znajomość i stosowanie Polityki bezpieczeństwa w części nr III oraz przepisów powszechnie obowiązującego prawa w obszarze ochrony danych osobowych, przetwarzanych przez Podmiot,

Postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez ADO za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie umowy cywilnoprawnej obowiązującej pomiędzy stronami tej umowy.

CZYM SĄ DANE OSOBOWE?

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, Podmiot dokonuje zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Danymi osobowymi będą zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

KIEDY MOŻNA PRZETWARZAĆ DANE OSOBOWE ZWYKŁE?

Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, 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 ADO,
4. kiedy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
5. kiedy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO,
6. kiedy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, z wyjątkiem sytuacji, w 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.

KIEDY MOŻNA PRZETWARZAĆ DANE OSOBOWE „WRAŻLIWE”?

Podmiot nie przetwarza danych wrażliwych (szczególnej kategorii danych), z wyjątkiem sytuacji, gdy:

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu,

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,
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,
6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,
8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego,
9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,
10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Podmiot realizuje obowiązki poprzez dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, zapewniając aby dane te były:

1. **Przetwarzane zgodnie z prawem.**

Tj. zgodne z wszelkimi normami prawa, zarówno tymi już istniejącymi w momencie wejścia w życie Rozporządzenia UE, jak i tymi, które dopiero później zostały wprowadzone do porządku prawnego. Zgodność z prawem dotyczy przestrzegania zarówno przepisów prawa materialnego, jak i przepisów dotyczących postępowania.

2. **Zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.**
3. **Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.**
   Tj. informacje wynikające z danych przetwarzanych przez ADO są zgodne z prawdą, kompletne oraz odpowiadają aktualnemu stanowi rzeczy. ADO przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane.
4. **Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.**
5. **ADO stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną**.
   W szczególności, ADO powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów powszechnie obowiązującego prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Dodatkowo Podmiot zapewnia bezpieczeństwo przetwarzanych danych osobowych, w szczególności poprzez:

1. **Poufność danych osobowych.**
   Tj. dane osobowe nie są udostępniane lub wyjawiane osobom nieupoważnionym, a osoby nieuprawnione nie mają dostępu do danych osobowych.
2. **Integralność danych osobowych.**
   Tj. dane osobowe są kompletne i niezmieniane w sposób nieuprawniony.
3. **Rozliczalność działań na danych osobowych.**
   Tj. wszystkie istotne czynności wykonane przy przetwarzaniu danych osobowych zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała.

OBOWIĄZKI PRZY PROJEKTOWANIU PROCESÓW

Już na etapie projektowania i opracowywania sposobów przetwarzania danych, a ponadto także na każdym kolejnym etapie przetwarzania, należy uwzględniać obowiązujące zasady ochrony danych osobowych.

W szczególności należy zadbać o zachowanie zasad:

- minimalizacji przetwarzania danych osobowych,
- przejrzystości co do funkcji i przetwarzania danych osobowych,
- umożliwienia osobie, której dane dotyczą, monitorowania przetwarzania danych,
- umożliwienia ADO tworzenia i doskonalenia zabezpieczeń.

Do obowiązków ADO należy zapewnienie, by stosowane rozwiązania były zgodne z przepisami rozporządzenia i chroniły prawa osób, których przetwarzane dane dotyczą. Niemniej osoby upoważnione, przy wykonywaniu czynności służbowych, powinny mieć tę zasadę na względzie.

OBOWIĄZEK DOMYŚLNEGO ZACHOWANIA PRYWATNOŚCI

Już na etapie projektowania i opracowywania sposobów przetwarzania danych, a ponadto także na każdym kolejnym etapie przetwarzania, należy uwzględniać obowiązek wdrożenia domyślnych ustawień prywatności.

Jego istotą jest wdrożenie przez ADO odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Zasada ta oznacza, że ustawienia prywatności stosowane przez administratora danych mają mieć na celu maksymalną ochronę użytkownika.

Wprowadzenie zasady domyślnej ochrony danych jest równoznaczne z koniecznością podjęcia przez użytkownika dodatkowych kroków w przypadku, gdyby chciał swoją prywatność w jakikolwiek sposób ograniczyć, np. poprzez udostępnianie swoich danych większej liczbie osób fizycznych.

Zatem zmiana domyślnie stosowanej maksymalnej ochrony prywatności będzie następować jedynie na wyraźne żądanie użytkownika danego systemu czy oprogramowania.

PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO W PRZYPADKU ZEBRANIA DANYCH OSOBOWYCH

W przypadku zbierania danych osobowych, zwykle należy czytelnie udzielić informacji zgodnych z szablonem obowiązku informacyjnego (**zał. nr 1.1 lub 1.2 lub 1.3**).

W odniesieniu do procesów zbierania danych od osób, których one dotyczą, podanych w załączniku zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

W odniesieniu do procesów zbierania danych nie od osób, których one dotyczą, podanych w załączniku zasad nie stosuje się, jeżeli:

1. przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
2. poinformowanie wymaga niewspółmiernie dużego wysiłku – w szczególności, gdy dane przetwarzane są w celach archiwizacyjnych, statystycznych, badań naukowych,
3. przekazanie informacji okazuje się niemożliwe,
4. utrwalenie lub ujawnienie danych jest wyraźnie nakazane prawem UE lub prawa krajowego,
5. dotyczy to tajemnicy zawodowej wynikającej z prawa UE lub prawa krajowego.

PROCEDURA POWIERZANIA PRZETWARZANIA DANYCH OSOBOWYCH

W przypadku konieczności przetwarzania danych osobowych przez odrębne podmioty świadczące usługi dla ADO, może on powierzyć ich przetwarzanie.

Powierzenie nie polega na udostępnieniu danych. Udostępnienie jest przekazaniem danych innemu podmiotowi (odbiorcy danych), który staje się ich ADO w zamiarze realizacji własnych celów. Powierzenie polega na przetwarzaniu danych przez podmiot przyjmujący w powierzenie, w zamiarze realizacji celów ADO. Powierzeniem jest np. ujawnienie danych osobowych do zewnętrznego biura rachunkowego. Udostępnieniem jest zwykle np. ujawnienie danych osobowych Urzędowi Skarbowemu.

Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy (**zał. Nr 15**) lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i ADO, określają w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

W przypadku, gdy stosowana jest inny wzorzec umowny, odmienny od wzorca umowy pozostającego w dyspozycji ADO, konieczna jest szczegółowa weryfikacja zgodności tego innego wzorca z przepisami powszechnie obowiązującego prawa, w szczególności RODO.

W umowach stanowiących podstawę przetwarzania danych osobowych umieszcza się prawo Podmiotu do kontroli wykonania przedmiotu umowy w siedzibie Procesora m.in. w zakresie polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa. Monitorowanie usług strony trzeciej powinno być udokumentowane i powinno zawierać informacje o: poziomie wykonania usługi, incydentach bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych, śladach audytowych, problemach operacyjnych, awariach, błędach i zakłóceniach

ADO może prowadzić dokument rejestru podmiotów, którym Podmiot powierza dane osobowe **(zał. nr 13)**.

PROCEDURA PRZYJMOWANIA DANYCH OSOBOWYCH W POWIERZENIE

Podmiot w charakterze podmiotu przetwarzającego (procesora) może przyjąć do przetwarzania dane osobowe powierzone przez ADO.

Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i ADO, określają w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Podmiot może posługiwać się szablonem umowy powierzenia danych osobowych **(zał. nr 15)**.

W przypadku, gdy stosowany jest inny wzorzec umowy, odmienny od wzorca umowy pozostającego w dyspozycji Podmiotu, konieczna jest szczegółowa weryfikacja zgodności tego innego wzorca z przepisami powszechnie obowiązującego prawa, w szczególności RODO.

Wyłączenie obowiązku prowadzenia rejestru kategorii czynności przetwarzania stosuje się w przypadkach określonych w art. 30 pkt 5 Rozporządzenia UE.

Powierzenie nie polega na udostępnieniu danych. Udostępnienie jest przekazaniem danych innemu podmiotowi (odbiorcy danych), który staje się ich ADO zaś powierzenie polega na przetwarzaniu danych przez podmiot, który nie jest ADO tych danych**.**

PROCEDURA UDOSTĘPNIANIA DANYCH OSOBOWYCH

Udostępnianie danych osobowych, jest jedną z form ich przetwarzania. Udostępnianie danych osobowych można określić, jako wszelkie działania umożliwiające innym niż ADO podmiotom, zapoznanie się z nimi, z wyłączeniem opisanych wcześniej powierzeń. Udostępnianie nie odnosi się do pracowników Podmiotu, który działają na podstawie udzielonych upoważnień.

1. Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.
2. Nie jest istotne, czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd., aby czynność była uznana za udostępnianie.
3. Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
4. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

ADO lub osoba przez niego upoważniona może prowadzić dokument rejestr podmiotów, którym Podmiot udostępnia dane osobowe **(zał. nr 14)**. Dokument zawiera informacje o udostępnieniu danych osobowych na rzecz wszystkich podmiotów, z wyłączeniem:

1. osób lub podmiotów, którym powierzono dane osobowe,
2. osób Upoważnionych do przetwarzania danych osobowych,
3. osób, których dane dotyczą.

PROCEDURA PRZETWARZANIA DANYCH W FORMIE PAPIEROWEJ

Ustanawia się poniższą procedurę przetwarzania danych osobowych w formie papierowej.

1. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.
2. Na biurku nie powinny znajdować się dokumenty zawierające dane osobowe innych osób niż w danej chwili obsługiwanej.
3. Odchodząc od biurka nie wolno pozostawiać dokumentów bez nadzoru.
4. Po zakończeniu pracy dokumenty należy zabezpieczyć w szafie.
5. Nie należy magazynować zbędnych wydruków.
6. Zbędne wydruki i inne dokumenty konwencjonalne (na nośnikach papierowych), zawierające dane osobowe, powinny być zniszczone w niszczarce dokumentów.
7. Za prawidłowe zniszczenie zbędnych dokumentów papierowych, zawierających dane osobowe, odpowiada osoba, która przetwarzała dane.
8. Nadzór nad prawidłowym niszczeniem dokumentów zawierających dane osobowe sprawuje ADO.

PROCEDURA POSTĘPOWANIA Z HASŁAMI I PLIKAMI DOSTĘPOWYMI

Ustanawia się poniższą procedurę postępowania z hasłami i plikami dostępowymi w Podmiocie.

1. Każda osoba upoważniona jest zobowiązana do ochrony swoich danych dostępowych do systemów informatycznych służących do przetwarzania danych osobowych. W zakres danych dostępowych włącza się w szczególności
   a) hasła dostępowe,
   b) klucze softwareowe (pliki umożliwiające dostęp – np. certyfikaty do VPN),
   c) klucze sprzętowe,
   d) inne mechanizmy umożliwiające dostęp do systemów IT.
2. Zobowiązuje się pracowników do zmiany indywidualnych haseł do systemów informatycznych służących przetwarzaniu danych osobowych, co najmniej 1 raz na 3 miesiące.
3. Zobowiązuje się pracowników do zmiany haseł dostępowych sprzętu, na którym przetwarza się dane osobowe, co najmniej 1 raz na 3 miesiące.
4. Zmiany haseł powinny być odnotowane przez ADO w rejestrze czynności, w systemie informatycznym.
5. Podstawowe metody ochrony danych dostępowych:
   a) nieprzekazywanie danych dostępowych innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
   b) nieprzechowywanie danych dostępowych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
   c) ochrona danych dostępowych przed pozyskaniem przez osoby trzecie.

PROCEDURA KORZYSTANIA Z INTERNETU

Ustanawia się poniższą procedurę korzystania z internetu w Podmiocie.

1. Użytkownicy systemu informatycznego mają prawo korzystać z internetu wyłącznie w celu wykonywania obowiązków służbowych.
2. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
3. Zabrania się zgrywania na nośniki pamięci używane w urządzeniach informatycznych oraz uruchamia na nich jakichkolwiek programów lub aplikacji niezatwierdzonych do użytku przez ADO.
4. Zabrania się uruchamiania plików pobranych z pominięciem skanowania przez program antywirusowy lub oznaczonych przez ten program jako niebezpieczne lub potencjalnie niebezpieczne.
5. Zabrania się przesyłania danych osobowych przy użyciu nieszyfrowanych stron internetowych. W tym celu przed rozpoczęciem przesłania tych danych, należy sprawdzić czy w pasku adresu strony internetowej widoczna jest informacja o odpowiednim zabezpieczeniu (zielona kłódka, protokół https).

6. Przy korzystaniu z internetu, użytkownicy systemu informatycznego mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.

PROCEDURA KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

Ustanawia się poniższą procedurę korzystania z poczty elektronicznej w Podmiocie.

1. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę. Dopuszcza się taką możliwość wyłącznie po uprzedniej pozytywnej weryfikacji adresu e-mail nadawcy (gdy np. stwierdzimy, że jest to kontrahent Podmiotu). W innych przypadkach należy przesłać wiadomość do ADO, celem zweryfikowania bezpieczeństwa załącznika.
2. Przy rozsyłaniu wszelkiej korespondencji wielu adresatom należy używać funkcji UDW, pozwalającej na ukrycie adresów e-mail adresatów. W takim przypadku adresy e-mail adresatów należy wprowadzić w polu UDW, a jako jej odbiorcę wprowadzić np. własny adres e-mail.
3. Przed wysłaniem wiadomości zawierającej dane osobowe, należy przynajmniej jednokrotnie zweryfikować poprawność adresu e-mail adresata.
4. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania lub stwierdzenia zaburzeń w funkcjonowaniu systemu informatycznego, osoba upoważniona jest zobowiązana powiadomić o tym fakcie ADO.

PROCEDURA KORZYSTANIA Z URZĄDZEŃ PRZENOŚNYCH

Ustanawia się poniższą procedurę korzystania z urządzeń przenośnych (np. laptopów, smartfonów) w Podmiocie.

1. Przed rozpoczęciem przetwarzania danych osobowych osoba upoważniona powinna sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić ADO.
2. Osoba upoważniona jest zobowiązana powiadomić ADO o stwierdzonym usiłowaniu zalogowania się do systemu informatycznego służącego do przetwarzania danych osobowych przez osobę nieuprawnioną.
3. Przystępując do pracy z urządzeniem służącym do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana wprowadzić swoje hasło dostępu.
4. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora, hasła dostępu innej osoby upoważnionej.
5. Ustawienia wyświetlaczy lub monitorów urządzeń przenośnych muszą zapewniać ograniczenie możliwości podglądania wyświetlanych danych osobom trzecim.
6. Osoba upoważniona jest zobowiązana dochowywać należytej staranności w celu uniemożliwienia nieuprawnionym osobom trzecim wglądu w informacje obejmujące dane osobowe przetwarzane w ramach systemu, które wyświetlane są na ekranie urządzenia.
7. W przypadku konieczności przerwania lub zakończenia pracy na urządzeniu przenośnym służącym do przetwarzania danych osobowych, należy zablokować dostęp do tego urządzenia.
8. Komputery przenośne można wynosić z obszaru przetwarzania danych osobowych tylko w szczególnych przypadkach, po poinformowaniu ADO lub właściwej osoby upoważnionej.

Niniejszy punkt nie dotyczy osób upoważnionych, które w ramach czynności służbowych wykonują czynności poza lokalizacją Podmiotu.

9. Osoba użytkująca urządzenie przenośne służące do przetwarzania danych osobowych, zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza lokalizacją Podmiotu.
10. Zabrania się pozostawiania urządzeń przenośnych służących do przetwarzania danych osobowych bez nadzoru, poza lokalizacją Podmiotu.
11. Zabrania się logowania do otwartych sieci (hotspotów, otwartych Wi-Fi) przy użyciu urządzeń przenośnych służących do przetwarzania danych osobowych.
12. Zabrania się wywożenia urządzeń przenośnych służących do przetwarzania danych osobowych do krajów spoza EOG (Europejskiego Obszaru Gospodarczego, w zakres którego wchodzą wszystkie kraje Unii Europejskiej, Islandia, Liechtenstein oraz Norwegia) bez uprzedniej zgody ADO.
13. Zabrania się wyłączania programów antywirusowych oraz uniemożliwiania wykonania kopii zapasowych przez system informatyczny.
14. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania lub stwierdzenia zaburzeń w funkcjonowaniu systemu informatycznego służącego do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana powiadomić o tym fakcie ADO.
15. Kopie zapasowe danych osobowych w systemie informatycznym wykonuje wyłącznie ADO lub uprawniony do tego operator hostingu.

PROCEDURA KORZYSTANIA Z KOMPUTERÓW STACJONARNYCH

Ustanawia się poniższą procedurę korzystania z komputerów stacjonarnych w Podmiocie.

1. Przed rozpoczęciem przetwarzania danych osobowych osoba upoważniona powinna sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić ADO.
2. Osoba upoważniona jest zobowiązana powiadomić ADO o stwierdzonym usiłowaniu zalogowania się do systemu informatycznego służącego do przetwarzania danych osobowych przez osobę nieuprawnioną.
3. Przystępując do pracy z komputerem służącym do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana wprowadzić swoje hasło dostępu.
4. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora, hasła dostępu innej osoby upoważnionej.
5. Ustawienia monitorów komputerów stacjonarnych muszą zapewniać ograniczenie możliwości podglądania wyświetlanych danych osobom trzecim.
6. Osoba upoważniona jest zobowiązana dochowywać należytej staranności w celu uniemożliwienia nieuprawnionym osobom trzecim wglądu w informacje obejmujące dane osobowe przetwarzane w ramach systemu, które wyświetlane są na ekranie komputera.
7. W przypadku konieczności przerwania lub zakończenia pracy na komputerze stacjonarnym służącym do przetwarzania danych osobowych, należy zablokować dostęp do tego komputera.
8. Zabrania się wynoszenia komputerów stacjonarnych z lokalizacji Podmiotu.

9. Zabrania się wyłączania programów antywirusowych oraz uniemożliwiania wykonania kopii zapasowych przez system informatyczny.
10. Kopie zapasowe danych osobowych w systemie informatycznym wykonuje ADO lub uprawniony do tego operator hostingu.

PROCEDURA PRZEGLĄDÓW I KONSERWACJI

Ustanawia się poniższe wymogi dotyczące realizacji przeglądów, napraw i konserwacji systemu informatycznego, służącego do przetwarzania danych osobowych.

1. Za przeglądy, naprawy i konserwacje urządzeń informatycznych służących do przetwarzania danych osobowych odpowiada ADO.
2. W przypadku wystąpienia zapotrzebowania na przeprowadzenie naprawy lub konserwacji urządzeń informatycznych służących do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana zgłosić ten fakt do ADO.
3. Osoba upoważniona jest zobowiązana udostępnić urządzenie informatyczne dla celu wykonania przeglądu, konserwacji lub naprawy przez ADO.
4. Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika bez polecenia ADO.
5. W przypadku przeprowadzania naprawy zdalnej, w szczególności przy użyciu środków teletransmisji podglądu ekranu osoby upoważnionej do przetwarzania danych przez ADO, przed rozpoczęciem tej czynności osoba upoważniona jest zobowiązana wyłączyć wszelkie programu służące do przetwarzania danych osobowych, których użycie nie jest niezbędne podczas wykonywania czynności.

PROCEDURA POSTĘPOWANIA Z NARUSZENIEM ZASAD OCHRONY DANYCH DLA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Naruszeniem ochrony danych osobowych jest 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. W przypadku wystąpienia naruszenia ochrony danych osobowych należy uruchomić procedurę postępowania z naruszeniem, opisaną poniżej.

W przypadku podejrzenia naruszenia zasad ochrony danych osobowych, każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana niezwłocznie:

1. poinformować o tym fakcie ADO poprzez wysłanie wiadomości e-mail pod adres abuczkowska@kursfoto.pl

2. do czasu otrzymania informacji zwrotnej, powstrzymać się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
3. w miarę możliwości zabezpieczyć elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych.

Wówczas należy oczekiwać udokumentowanej informacji zwrotnej od osoby poinformowanej.

IV POSTANOWIENIA KOŃCOWE

1. Polityka bezpieczeństwa jest dokumentem obowiązującym w Podmiocie w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
2. Polityka bezpieczeństwa jest dokumentem obowiązującym wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności Podmiotu.
3. Każda osoba dopuszczona do przetwarzania danych osobowych w ramach działalności Podmiotu ma obowiązek zapoznania się z niniejszą Polityką bezpieczeństwa.
4. Naruszenie zasad wynikających z Polityki bezpieczeństwa może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.
5. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki bezpieczeństwa nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.
6. Polityka bezpieczeństwa wraz z załącznikami wchodzi w życie z dniem jej podpisania przez ADO.
7. W przedmiocie spraw nieuregulowanych Polityką bezpieczeństwa, zastosowanie znajdują przepisy prawa powszechnie obowiązującego, w szczególności Rozporządzenia UE.

V ZAŁĄCZNIKI

Załączniki do niniejszej Polityki bezpieczeństwa stanowią jej część pod warunkiem uzupełnienia:

1. Szablon obowiązku informacyjnego (zał. nr 1.1 lub 1.2 lub 1.3),
2. Szablon analizy ryzyka (zał. nr 2),
3. Rejestr czynności przetwarzania danych osobowych (zał. nr 3),
4. Szablon upoważnień do przetwarzania danych osobowych przez pracowników (zał. nr 4),
5. Szablon upoważnień do przetwarzania danych osobowych przez osoby zatrudnione na podstawie umów cywilnoprawnych (zał. nr 5),
6. Rejestr pracowników upoważnionych do przetwarzania danych (zał. nr 6),
7. Rejestr osób zatrudnionych na podstawie umowy cywilnoprawnej, upoważnionych do przetwarzania danych (zał. nr 7),
8. Szablon zgłoszenia naruszenia ochrony danych do PUODO (zał. nr 8),
9. Szablon protokołu zdawczo – odbiorczego kluczy
10. Rejestr naruszeń bezpieczeństwa danych osobowych (zał. Nr 10),
11. Rejestr napraw, przeglądów i konserwacji systemu informatycznego (zał. Nr 11),
12. Rejestr urządzeń i nośników, służących do przetwarzania danych osobowych (zał. nr 12),
13. Rejestr podmiotów, którym powierzono dane osobowe (zał. Nr 13),
14. Rejestr podmiotów, którym udostępniono dane osobowe (zał. nr 14).

15. Szablon umowy powierzenia danych osobowych (zał. nr 15),

Podpis Administratora Danych Osobowych	Data