ZARZĄDZENIE NR 133/ZK/2018
BURMISTRZA MIASTA SIERPCA

z dnia 29 października 2018 r.

w sprawie zatwierdzenia „Polityki Bezpieczeństwa Danych Osobowych"

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy Unii Europejskiej nr 119, poz. 1) zarządzam co następuje:

§ 1.

W celu zapewnienia bezpieczeństwa danych osobowych gromadzonych i przetwarzanych przez Administratora Danych Osobowych jakim jest Urząd Miejski w Sierpcu zatwierdzam Politykę Bezpieczeństwa Danych Osobowych stanowiącą załącznik nr 1 do zarządzenia.

§ 2.

Na stanowisko Inspektora Ochrony Danych Osobowych powołuję Pana Jakuba Kosmacińskiego

§ 3.

Traci moc Zarządzenie nr 149/ZK/2017 Burmistrza Miasta Sierpca z dnia 21 listopada 2017 r.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ
Jarosław Perzyński

zgodność:
INSPEKTOR
Artur Dudziński

Polityka bezpieczeństwa

Spis treści

_____

(data wejścia w życie i podpis osoby upoważnionej)

1. Wstęp

1.1 Słowniczek

Administrator (ADO) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Administratorem w rozumieniu Polityki jest **Burmistrz Miasta Sierpca (ul. Piastowska 11A, 09-200 Sierpc)**.

Administrator Systemów Informatycznych (ASI) – podmiot nadzorujący systemy informatyczne Administratora.

adekwatność – zasada, zgodnie z którą dane osobowe muszą być gromadzone tylko w zakresie niezbędnym do wykonania celu, w którym dane są przetwarzane (w szczególności oznacza to brak możliwości zbierania danych osobowych „na zapas"), w szczególności dla wypełniania ciążących na ADO obowiązków prawnych.

autoryzacja – proces, którego celem jest potwierdzenie czy użytkownik posiada uprawnienia do właściwego zakresu danych. Dla określenia uprawnień konieczne jest najpierw stwierdzenie tożsamości, dlatego autoryzacja następuje dopiero po pomyślnej weryfikacji tożsamości na podstawie loginu i hasła.

dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, takie jak imiona, nazwiska, adresy zamieszkania, numery dokumentów tożsamości itp.

dostępność – zasada, zgodnie z którą dostęp do danych osobowych i związanych z nimi aktywów mają osoby upoważnione tylko wtedy, gdy istnieje taka potrzeba.

hasło – ciąg znaków literowych, cyfrowych bądź innych znany jedynie uprawnionemu użytkownikowi zapewniający uwierzytelnienie i dostęp do systemu informatycznego.

Inspektor Ochrony Danych (IOD) – osoba wspierająca ADO w realizacji obowiązków, wynikających z przepisów o ochronie danych osobowych (w tym RODO i Ustawy).

integralność – zasada, zgodnie z którą dane osobowe są przechowywane w sposób bezpieczny (za pomocą odpowiednich środków technicznych lub organizacyjnych) i nie są zmieniane lub niszczone w sposób nieautoryzowany.

login/identyfikator – ciąg znaków literowych, cyfrowych bądź innych jednoznacznie identyfikujący użytkownika, zapewniający uwierzytelnienie i dostęp do systemu informatycznego.

minimalizacja – wykorzystanie danych osobowych tylko w zakresie niezbędnym dla celu, dla którego zostały zebrane.

naruszenie ochrony danych osobowych – przypadkowe lub niezgodne z prawem zniszczenie, utrata, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesłanych, przechowywanych lub w inny sposób wykorzystywanych.

ograniczenie przechowywania – zasada, zgodnie z którą dane są gromadzone przez okres nie dłuższy niż jest to niezbędne ze względu na cel, dla którego dane zostały zebrane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO.

Polityka bezpieczeństwa – ten dokument.

poufność – zasada, zgodnie z którą dane nie są udostępniane nieupoważnionym podmiotom.

prawidłowość – zasada, zgodnie z którą zbierane dane osobowe są prawidłowe, a w razie potrzeby uaktualniane.

przejrzystość – zasada, zgodnie z którą dane są zbierane w sposób jasny dla osoby, której dane dotyczą.

przepisy o ochronie danych osobowych – powszechnie obowiązujące przepisy prawa dotyczące ochrony danych osobowych i bezpieczeństwa informacji, w tym RODO i Ustawa.

przetwarzanie danych osobowych – wszystkie operacje wykonywane na danych osobowych (w formie papierowej lub elektronicznej), takie 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) – organ właściwy do spraw ochrony danych osobowych w Polsce.

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.

rozliczalność – zasada, zgodnie z którą działania osoby lub podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie lub temu podmiotowi.

rzetelność – zasada, zgodnie z którą dane są zbierane w sposób rzetelny od osoby, której dane dotyczą.

szczególne kategorie danych/dane wrażliwe – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby, której dane dotyczą.

Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

uwierzytelnianie – proces, którego celem jest weryfikacja tożsamości użytkownika.

zgodność z prawem – zasada, zgodnie z którą dane są zbierane na podstawie jednej z przesłanek wskazanych w art. 6 ust. 1 RODO lub art. 9 ust. 2 RODO oraz zgodnie z innymi przepisami o ochronie danych osobowych**.**

1.2 Cel Polityki

1. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO. Polityka została opracowana na podstawie przepisów RODO, Ustawy oraz innych powszechnie obowiązujących przepisów, dotyczących ochrony danych osobowych i bezpieczeństwa informacji.
2. Celem Polityki jest zapewnienie takiego poziomu bezpieczeństwa danych osobowych przetwarzanych przez ADO, który uchroni je przed:
    1) przetwarzaniem przez osoby nieuprawnione,
    2) nieuprawnionym dostępem, zmianą, uszkodzeniem lub zniszczeniem.
3. Realizując cel Polityki, ADO stosuje środki techniczne, organizacyjne i informatyczne.
4. ADO zapewnia przetwarzanym przez siebie danym osobowym poniższe właściwości:

1) poufność,
2) integralność,
3) dostępność,
4) rozliczalność,
5) zgodność z prawem.

5. ADO deklaruje pełne zaangażowanie i determinację celem:
   1) zapewnienia bezpieczeństwa przetwarzanych danych osobowych,
   2) prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych.
6. ADO na bieżąco dostosowuje systemy informatyczne służące do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w przepisach o ochronie danych osobowych.
7. W związku z realizacją celu Polityki ADO może wprowadzać dodatkowe wytyczne, regulaminy i instrukcje.
8. Niniejsza Polityka oraz dokumenty z nią powiązane są aktualizowane wraz ze zmieniającym się stanem faktycznym lub prawnym w celu zapewnienia, że zasady ochrony danych określone w Polityce lub dokumentach pozostają aktualne i adekwatne.
9. Do stosowania Polityki zobowiązane są wszystkie osoby zatrudnione u Administratora lub współpracujące z Administratorem (niezależnie od podstawy zatrudnienia lub współpracy), którym przyznano dostęp do danych osobowych.

1.3 Podstawowe zasady

1. ADO przetwarza dane osobowe z poszanowaniem następujących zasad:
   1) zgodność z prawem
   2) rzetelność i przejrzystość
   3) adekwatność
   4) minimalizacja
   5) prawidłowość
   6) ograniczenie przechowywania
   7) integralność i poufność
   8) rozliczalność
2. ADO jest odpowiedzialny za stosowanie zasad opisanych w Polityce i jest w stanie wykazać ich przestrzeganie.

2. Podmioty zaangażowane w ochronę danych osobowych i ich obowiązki

2.1 Administrator danych osobowych (ADO)

1. ADO realizuje zadania z zakresu ochrony danych osobowych.
2. ADO decyduje o celach i środkach przetwarzania danych.
3. ADO nadaje osobom zatrudnionym upoważnienia do przetwarzania danych osobowych.
4. ADO stosuje środki techniczne, organizacyjne i informatyczne zapewniające ochronę danych osobowych odpowiednią do zagrożeń, kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieuprawnioną.
5. ADO w szczególności zapewnia:
   1) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych osobowych w pomieszczeniach do tego przeznaczonych,

2) system i sprzęt informatyczny zapewniający bezpieczne przetwarzanie danych,
3) dopuszczenie do przetwarzania danych wyłącznie osób posiadających odpowiednie upoważnienie,
4) prowadzenie ewidencji osób upoważnionych,
5) kontrolę nad tym jakie dane, kiedy i przez kogo zostały wprowadzone, usunięte lub komu i przez kogo zostały przekazane,
6) osobom zatrudnionym możliwość zdobywania wiedzy dotyczącej ochrony danych osobowych.

6. W razie wykazania przez osobę, której dane dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany, bez zbędnej zwłoki do uzupełnienia, sprostowania, uaktualnienia, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.
7. ADO prowadzi rejestr czynności przetwarzania, zgodnie z art. 30 ust. 1 RODO. **Wzór stanowi załącznik do Polityki**.
8. Jeżeli ADO jest podmiotem przetwarzającym dane w stosunku do podmiotu zewnętrznego, prowadzi rejestr kategorii czynności przetwarzania, zgodnie z art. 30 ust. 2 RODO. **Wzór stanowi załącznik do Polityki**.
9. ADO dokonuje ogólnej analizy ryzyka przetwarzania danych osobowych, a jeżeli przetwarzanie danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – dodatkowo analizę oceny skutków. **Analizy są dokonywane zgodnie z procedurą stanowiącą załącznik do Polityki**.
10. W sytuacjach określonych w art. 32-33 RODO ADO zawiadamia o naruszeniu ochrony danych osobowych PUODO lub osoby, których dane dotyczą.
11. ADO prowadzi rejestr naruszeń ochrony danych osobowych. **Wzór rejestru stanowi załącznik do Polityki**.
12. ADO wyznacza inspektora ochrony danych (IOD).

2.2 Inspektor ochrony danych (IOD)

1. Do zadań IOD należy:
    1) informowanie ADO oraz osób zatrudnionych, które przetwarzają dane osobowe, o ich obowiązkach związanych z ochroną danych osobowych i doradzanie im w tych sprawach;
    2) monitorowanie przestrzegania Polityki i przepisów o ochronie danych osobowych, w tym w szczególności podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO
    4) współpraca z PUODO,
    5) pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach
2. IOD może być osoba, która posiada odpowiednie kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, wskazanych w ust. 1 powyżej.

3. Dane kontaktowe inspektora ochrony danych (imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu):
    1) są publikowane na stronie internetowej (lub w sposób ogólnie dostępny w miejscu prowadzenia działalności) ADO,
    2) są przekazywane PUODO zgodnie z art. 10 Ustawy.
4. W dokumencie powołującym IOD osoba powołana do pełnienia funkcji musi być wskazana z imienia i nazwiska.
5. ADO może powierzyć IOD wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania przez IOD zadań związanych z ochroną danych osobowych.
6. IOD podlega bezpośrednio najwyższemu kierownictwu ADO.
7. Administrator zapewnia IOD środki i organizacyjną odrębność, niezbędne do niezależnego wykonywania przez niego zadań.

2.3 Administrator systemów Informatycznych (ASI)

1. ADO może wyznaczyć na Administratora Systemów Informatycznych (ASI) osobę zatrudnioną u ADO lub powierzyć wykonywanie obowiązków ASI podmiotowi zewnętrznemu.
2. Do podstawowych zadań ASI należy zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych, określonych w Polityce bezpieczeństwa i załącznikach do niej.
3. ASI odpowiedzialny jest również za zarządzanie bezpieczeństwem przetwarzanej informacji.
4. ASI podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio najwyższemu kierownictwu ADO.
5. Jeżeli ADO nie wyznaczył ASI lub nie powierzył jego obowiązków podmiotowi zewnętrznemu, za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych odpowiada ADO.
6. Jeżeli treść Polityki bezpieczeństwa lub załączników do niej odwołuje się do praw lub obowiązków ASI, to w przypadku niewyznaczenia ASI wszystkie te prawa i obowiązki realizuje ADO.

2.4 Osoby upoważnione do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych są dopuszczone wyłącznie osoby, które upoważnił ADO.
2. Przed przystąpieniem do przetwarzania danych osobowych osobie mającej przetwarzać dane osobowe wydaje się upoważnienie, którego wzór stanowi **załącznik do Polityki**.
3. Przed przystąpieniem do przetwarzania danych osobowych osoba mająca przetwarzać dane osobowe podpisuje oświadczenie, zawarte w treści upoważnienia, o którym mowa w ust. 2 powyżej.
4. Osoby upoważnione są obowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.
5. Po nadaniu upoważnienia osobie upoważnionej nadawany jest dostęp do aplikacji, programów lub systemów. Dostęp jest uzależniony od:
    1) zakresu obowiązków użytkownika,
    2) zakresu upoważnienia do przetwarzania danych osobowych użytkownika, nadanego zgodnie z niniejszymi procedurami,
    3) zasady nadawania minimalnych uprawnień, wystarczających użytkownikowi do wykonywania powierzonych mu zadań
6. W przypadku zakończenia współpracy z osobą zatrudnioną:
    1) jej upoważnienie automatycznie wygasa,
    2) jej dostęp do aplikacji, programów lub systemów jest blokowany.

7. Osoby uprawnione do przebywania w pomieszczeniach, w których przetwarza się dane osobowe, ale niebędące osobami upoważnionymi (np. członkowie personelu sprzątającego), składają oświadczenie o zachowaniu poufności, zgodnie ze wzorem stanowiącym **załącznik do Polityki**.
8. Osoba upoważniona, podejrzewająca lub stwierdzająca zaistnienie zdarzenia mogącego doprowadzić do naruszenia bezpieczeństwa danych osobowych, zobowiązana jest do natychmiastowego poinformowania o tym zdarzeniu.

3. Przetwarzanie danych

1. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy jest spełniona jedna z przesłanek wskazanych:
    1) w art. 6 ust. 1 RODO (dotyczy danych osobowych zwykłych)
    2) art. 9 ust. 2 RODO (dotyczy szczególnych kategorii danych osobowych, w tym danych o stanie zdrowia).
2. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IOD z wnioskiem o rozstrzygnięcie wątpliwości.
3. Przed udzieleniem przez IOD odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotycz należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.
4. Wobec osób, których dotyczą przetwarzane dane osobowe, ADO realizuje obowiązek informacyjny na zasadach określonych w art. 13-14 RODO. ADO dba o to, by przekazywane w związku z tym informacje były łatwo dostępne, a także przekazywane w sposób jasny, czytelny i zrozumiały dla odbiorcy.
5. ADO realizuje również inne uprawnienia osób, których dane dotyczą, określone w art. 15-22 RODO. Wykonując te zadanie, ADO dba zwłaszcza o:
    1) potwierdzenie tożsamości osób składających wnioski,
    2) przekazywanie danych w sposób jasny, czytelny i zrozumiały,
    3) łatwość dostępu do danych,
    4) odpowiadanie na wnioski niezwłocznie, nie później niż w terminach wynikających z art. 12 ust. 3 RODO.
6. Realizowanie prawa do bycia zapomnianym opisuje **załącznik do Polityki**.
7. Realizowanie prawa dostępu do danych opisuje **załącznik do Polityki**.
8. ADO dokumentuje sposób realizacji praw osób, których dane dotyczą.

4. Powierzenie przetwarzania danych osobowych

1. ADO może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
2. Przed powierzeniem przetwarzania danych osobowych innemu podmiotowi ADO powinien zweryfikować, czy ten podmiot zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. Umowa powierzenia przetwarzania danych osobowych może być zawarta:
    1) **na wzorze, który stanowi załącznik do Polityki** lub

2) na wzorze przekazanym przez podmiot przetwarzający (zgodnym z wymaganiami, o których mowa w **załączniku do Polityki**).

5. Środki bezpieczeństwa, stosowane u ADO

1. ADO zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zarówno w formie papierowej, jak i elektronicznej;
2. Do środków technicznych zalicza się:
   1) środki ochrony fizycznej,
   2) środki dotyczące infrastruktury informatycznej, w tym środki stosowane w ramach systemów informatycznych;
3. Zależność między środkami technicznymi a środkami organizacyjnymi wynikają z zastosowania urządzeń oraz technologii, które wpływają na funkcjonowanie organizacji, w szczególności koordynacji pracy.
4. Główną koncepcją mającą na celu efektywne podejście do ochrony przetwarzanych danych jest łączenie różnych zabezpieczeń, co ma na celu stworzenie kilku warstw ochronnych.
5. ADO w wymienionych powyżej obszarach wdrożył środki zapewniające jak najwyższe standardy bezpieczeństwa przy uwzględnieniu ryzyka, stanu wiedzy technicznej, kosztów ich wprowadzenia oraz zasobów organizacyjnych.
6. Poniżej wymienione środki ochrony zostały **szerzej opisane w załącznikach do Polityki** określających szczegółowe zasady dotyczące bezpieczeństwa przetwarzanych danych
7. **Każda upoważniona osoba ma obowiązek zapoznania się i stosowania zasad dotyczących ochrony danych osobowych przetwarzanych w sposób zarówno elektroniczny jak i papierowym. Z wyłączeniem części poufnych ADO udostępnia do treść dokumentu w wersji elektronicznej lub papierowej według własnego wyboru.**

5.1 Rozwiązania organizacyjne

ADO stosuje następujące środki organizacyjne:

1) została opracowana Polityka wraz z szeregiem szczegółowych uregulowań, stanowiących treść **załączników do Polityki**,
2) do przetwarzania danych osobowych zostają dopuszczone wyłącznie osoby posiadające ważne upoważnienie do ich przetwarzania,
3) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
4) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy,
5) osoby upoważnione do przetwarzania danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami ADO, odnoszącymi się do postępowania przy przetwarzaniu danych osobowych,
6) osoby posiadające upoważnienie do przetwarzania danych osobowych zostały przeszkolone w zakresie ochrony danych osobowych i zabezpieczeń systemu informatycznego, szczególności sytuacji związanych z postępowaniem w przypadku wystąpienia zdarzeń wskazujących na incydent bezpieczeństwa,
7) podjęto ustalenia dotyczące okresowych kontroli dotyczące przestrzegania przez użytkowników wprowadzonych regulacji,
8) osoby postronne mają dostęp do pomieszczeń, w których są przetwarzane dane osobowe, wyłącznie w obecności osoby upoważnionej lub za wiedzą i zgodą ADO.

5.2 Rozwiązania fizyczne

ADO stosuje następujące zabezpieczenia fizyczne:

1) system alarmowy (min. czujki ruchu zainstalowane w pomieszczeniach, gdzie przechowywane są dane osobowe),
2) zabezpieczenia przeciwpożarowe (min. gaśnica nadająca się do gaszenia sprzętu elektronicznego),
3) zamykanie pomieszczeń (np. drzwi zamykane na klucz, zamki szyfrowe, karty dostępu),
4) zabezpieczenie okien w miejscach narażonych na ryzyko włamania (np. kraty lub rolety antywłamaniowe),
5) dostęp osób upoważnionych do szafek, szaf lub szuflad zamykanych na klucz,
6) dostęp do niszczarek dokumentów papierowych.

5.3 Rozwiązania informatyczne

ADO stosuje następujące zabezpieczenia informatyczne:

1) mechanizmy uwierzytelniające w systemach informatycznych zorganizowane w sposób kaskadowy,
2) mechanizmy odpowiedzialne za autoryzację użytkowników w systemach informatycznych,
3) rozwiązania zapewniające nienaruszoną pracę w systemie min. aplikacje antywirusowe,
4) środki gwarantujące ciągłą pracę systemów informatycznych (min. zasilaczy UPS),
5) środki gwarantujące możliwość odtworzenia środowiska informatycznego w przypadku wystąpienia zdarzenia zakłócającego ciągłość działania (min. wykonywanie kopii zapasowych).
6) technologie ograniczające dostęp do infrastruktury informatycznej w szczególności usług sieciowych (min. zapora ogniowa chroniąca styk sieci),
7) środki zapewniające monitorowanie infrastruktury informatycznej w szczególności obszarów dotyczących bezpieczeństwa.

6. Naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych jest odpowiedzialna za ich bezpieczeństwo.
2. Osoba podejrzewająca lub stwierdzająca zdarzenie, mogące prowadzić do naruszenia ochrony danych osobowych, ma obowiązek zgłoszenia tego odpowiedniej osobie.
3. Przykładowa lista zdarzeń, o których mowa w ust. 2 powyżej ze wskazaniem osób, które mają być zawiadomione, **stanowi załącznik do Polityki**.
4. Zgłoszenie naruszenia lub podejrzenia naruszenia ochrony danych do IOD dokonuje się na formularzu, który **stanowi załącznik do Polityki**.
5. Po otrzymaniu zawiadomienia o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych IOD, we współpracy z ADO, dokonuje weryfikacji stanu danych osobowych i ich zabezpieczeń.
6. W razie stwierdzenia naruszenia ochrony danych osobowych ADO, we współpracy z IOD i ASI:
    1) podejmuje niezbędne czynności zmierzające do uniemożliwienia ponownego wystąpienia naruszeń,
    2) podejmuje niezbędne czynności, mające na celu uniemożliwienie lub ograniczenie dostępu do danych osobowych osób nieupoważnionych,
    3) gromadzi i zabezpiecza wszelkie informacje i dokumenty, mogące przyczynić się do ustalenia przyczyn i źródła naruszenia,
    4) niezwłocznie przywraca prawidłowe działanie systemu informatycznego,

5) dokonuje analizy stanu zabezpieczeń,
6) szacuje rozmiar szkód powstałych na skutek naruszenia,
7) dokonuje zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych lub odpowiednich osób fizycznych, zgodnie z art. 33-34 RODO.

7. ADO we współpracy z IOD oraz ASI podejmują niezbędne działania, mające na celu uniemożliwienie ponownego wystąpienia naruszeń. Wskazane działania mogą obejmować w szczególności:
   1) przeprowadzenie przeglądu i konserwacji komputerów, sprzętu komputerowego oraz oprogramowania komputerowego,
   2) przeprowadzenie szkoleń dla osób upoważnionych,
   3) wyciągnięcie przewidzianych przepisami prawa konsekwencji względem osób odpowiedzialnych za zaistniałe naruszenia,
   4) zawiadomienie odpowiednich organów (np. Policji), jeżeli do naruszenia doszło na skutek zachowania noszącego znamiona czynu sprzecznego z prawem.

7. Postanowienia końcowe

1. Polityka obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u ADO. Wszelkie zmiany niniejszego dokumentu obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u ADO.
2. Z dniem wprowadzenia w życie Polityki traci ważność wcześniej obowiązująca u ADO dokumentacja dotycząca ochrony danych osobowych. Zastrzeżenie to nie dotyczy upoważnień do przetwarzania danych osobowych, wystawionych przed dniem wprowadzenia w życie Polityki.
3. Każdy, kto przetwarza dane posiadane przez ADO, zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
5. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym przepisy o ochronie danych osobowych.

8. Załączniki

1. Analiza ryzyka – procedura postępowania
2. Dostęp do danych – procedura postępowania
3. Oświadczenie o poufności
4. Praca w systemach IT (wersja dla ADO)
5. Praca w systemach IT (wersja dla użytkowników)
6. Prawo do bycia zapomnianym – procedura postępowania
7. Protokół likwidacji
8. Rejestr czynności przetwarzania
9. Rejestr kategorii czynności przetwarzania
10. Rejestr naruszeń ochrony danych osobowych
11. Tabela form naruszenia
12. Upoważnienie do danych osobowych
13. Wymagania dotyczące umów powierzenia
14. Wzór umowy powierzenia
15. Zabezpieczenia fizyczne

16. Zgłoszenie naruszenia do IOD

Analiza ryzyka

1. Wstęp

1. ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu ADO:
    1) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
    2) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
    3) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.
    4) analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
2. ADO ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym celu ADO ustala przydatność i stosuje takie środki i podejście jak:
    1) pseudonimizacja,
    2) szyfrowanie danych osobowych,
    3) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
    4) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
3. ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. ADO stosuje przyjętą u siebie metodykę oceny skutków.

2. Procedura zarządzania ryzykiem

1. Celem analizy ryzyka jest ocena zagrożeń dla poprawnego i bezpiecznego przetwarzania danych oraz wybór i wdrożenie środków zmniejszających prawdopodobieństwo ich wystąpienia.
2. Ogólna analiza ryzyka przetwarzania danych osobowych jest przeprowadzana obowiązkowo.
3. Analiza oceny skutków (DPIA - Data Protection Impact Assessment) jest przeprowadzana obowiązkowo, jeżeli przetwarzanie danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
4. Analiza ryzyka polega na określeniu wielkości ryzyka, na zidentyfikowaniu grup informacji oraz obszarów jej przetwarzania, które wymagają zabezpieczenia.
5. Za realizację analizy ryzyka odpowiedzialny ADO, we współpracy z IOD, ASI i innym wskazanymi przez ADO osobami.
6. Podstawą przeprowadzenia analizy ryzyka jest:
    1) lista zagrożeń
    2) lista pytań uzupełniających

7. Lista zagrożeń:
    1) Ujawnienie haseł dostępu.
    2) Dostęp osób nieupoważnionych.
    3) Niemożność odtworzenia informacji.
    4) Działanie szkodliwego oprogramowania.
    5) Nielegalne wykorzystanie oprogramowania.
    6) Awaria usług świadczonych przez stronę trzecią.
    7) Awaria systemów IT.
    8) Awaria urządzeń.
    9) Przerwa w dostarczaniu mediów niezbędnych do funkcjonowania systemów IT.
    10) Włamanie do systemu IT
    11) Błąd użytkownika.
    12) Brak reakcji na naruszenia bezpieczeństwa.
    13) Zniszczenie lub nieuprawniona zmiana informacji.
    14) Naruszenie bezpieczeństwa przy współpracy ze stronami trzecimi.
    15) Naruszenie prawa.
    16) Oszustwa w transakcjach online.
    17) Ujawnienie informacji osobom nieuprawnionym.
    18) Kradzież.
    19) Zagrożenia środowiskowe (powódź, pożar).
    20) Włamanie do pomieszczenia/budynku lub inne nieuprawnione wejście.
    21) Błędy w zarządzaniu.
8. Etapy przeprowadzania analizy ryzyka w organizacji:
    1) określenie prawdopodobieństwa wystąpienia zagrożenia
    2) określenie skutków wystąpienia zagrożenia
    3) określenie poziomu ryzyka dla danego zagrożenia
    4) wypełnienie arkusza oceny ryzyka
9. Określenie prawdopodobieństwa wystąpienia zagrożenia:
    1) przy ocenie prawdopodobieństwa wystąpienia zagrożenia dla każdego zagrożenia należy:
        a) formułować pytania uzupełniające
        b) wskazywać liczbę incydentów
        c) wykorzystać wiedzę na temat ocenianego zagrożenia.
    2) prawdopodobieństwo wystąpienia zagrożenia określa się według następującej skali:
        a) małe (negatywna ocena na mniej niż 25% pytań),
        b) średnie (negatywna ocena na 25-50% pytań),
        c) duże (negatywna ocena na 50-75% pytań),
        d) bardzo duże (negatywna ocena na więcej niż 75% pytań).
10. Ocena skutków wystąpienia zagrożenia:
    1) dla każdego zagrożeń wymienionych na liście zagrożeń wskazanych powyżej, należy określić skutek jego wystąpienia.
    2) skutek wystąpienia zagrożenia może przyjmować następujące wartości:
        a) mały;
        b) średni;
        c) duży;
        d) bardzo duży

Analiza ryzyka (załącznik do Polityki bezpieczeństwa)

11. Określenie poziomu ryzyka dla danego zagrożenia.
    1) uwzględniając ocenę prawdopodobieństwa wystąpienia zagrożenia oraz skutku wystąpienia zagrożenia, należy wskazać poziom ryzyka.

Prawdopodobieństwo wystąpienia/Skutek wystąpienia zagrożenia	1	2	3	4
1	N	N	Ś	Ś
2	N	Ś	Ś	W
3	N	Ś	W	W
4	Ś	W	W	W

12. Wypełnienie arkusza oceny ryzyka
    1) W arkuszu oceny ryzyka należy umieścić
        a) prawdopodobieństwo wystąpienia zagrożenia;
        b) skutek wystąpienia zagrożenia;
        c) ryzyko
    2) W ostatniej rubryce należy wskazać odpowiednie obszary wymagające poprawy oraz sugerowane sposoby zabezpieczeń.

ARKUSZ ANALIZY RYZYKA						
L.p.	Zagrożenie	Prawdopodobieństwo	Skutek	Ryzyko	Obszar wymagający poprawy	Proponowane zabezpieczenie
1						
2						
3						

Dostęp do danych

Jeżeli do ADO wpłynie żądanie dostępu do danych, **nie należy postępować pochopnie** – poniżej przedstawiamy kroki, według których należy postępować w przypadku wpłynięcia takiego wniosku, w tym wniosku o dostarczenie kopii danych osobowych:

1. **Sprawdzamy tożsamości osoby**, która zgłosiła żądanie – należy mieć pewność, że pod naszego klienta nie podszyła się osoba trzecia. Można to zrobić w bardzo prosty sposób: należy sprawdzić, czy żądanie zostało wysłane ze źródła, które znajduje się w naszej bazie danych, np. z adresu e-mail, który jest przypisany do wnioskującej osoby (np. czy p.nowak@abc.pl nie prosi o dostęp do danych j.nowak@abc.pl).
2. Należy podjąć wszelkie możliwe starania żeby tę tożsamość ustalić.
3. Jeżeli osoba zgłaszająca żądanie znajduje się w naszej bazie danych, **sprawdzamy jakiego rodzaju dane o tej osobie przetwarzamy**, np. imię, nazwisko, adres zamieszkania, adres e-mail, numer telefonu, itp.
4. **Sprawdzamy, na jakiej podstawie są przetwarzane dane osobowe**: takimi podstawami są w szczególności:

- umowy,
- zgody (np. na działania marketingowe) lub
- odrębne przepisy prawa (np. dotyczące podatków, ubezpieczeń, oświaty itp.).

5. **Realizujemy żądanie** o które prosi dana osoba – zgodnie z art. 15 RODO osoba, której dane są przetwarzane, ma prawo do otrzymania informacji na temat danych osobowych przetwarzanych na jej temat oraz do uzyskania kopii tych danych. Zgodnie z żądaniem Administrator powinien:

- umożliwić osobie zgłaszającej wniosek wgląd do bazy danych administratora danych (np. poprzez dedykowany kanał do pobierania danych – o ile istnieje);
- przekazać osobie zgłaszającej wniosek dokument zawierający dane eksportowane z bazy danych;

Jeżeli zapewnienie wglądu lub przekazanie wnioskującemu dokumentu z danymi eksportowanymi z systemu nie jest możliwe, można sporządzić dokument, który będzie zawierał wszystkie niezbędne informacje – wzór dokumentu stanowi załącznik do niniejszej instrukcji.

Dokumenty są przekazywane poprzez przesłanie do osoby wnioskującej kopii danych – zgodnie ze złożonym wnioskiem, np.:

- pocztą,
- kurierem,
- drogą elektroniczną w formie zahasłowanej (hasło do pliku musi być przekazane inną drogą – telefonicznie bądź esemesem na wskazany numer telefonu; nie ma potrzeby ewidencjonowania numeru telefonu, jest on wykorzystywany jedynie do wysłania hasła do pliku).

6. **Dokumentujemy realizację żądania** w sposób pozwalający na ustalenie komu (imię i nazwisko, adres e-mail z którego wysłano żądanie), kiedy, przez kogo, w jakiej formie i na jakie dane została przekazana odpowiedź na żądanie.

Przy realizacji żądania dostępu do danych należy pamiętać o tym, że:

Dostęp do danych – procedura postępowania (załącznik do Polityki bezpieczeństwa)

1) Osobie zgłaszającej żądanie jesteśmy zobowiązani udzielić wszelkich informacji dotyczących jej danych osobowych, które podlegają przetwarzaniu oraz informacji o:

- celu przetwarzania danych,
- okresie, w którym dane będą przechowywane,
- fakcie przekazania danych współpracującym podmiotom (na podstawie umów powierzenia przetwarzania danych),
- przysługujących prawach.

2) Pierwsza kopia danych udzielana jest nieodpłatnie, za kolejne kopie administrator danych może pobierać opłatę, której wysokość musi być miarkowana (tzn. musi kształtować się w rozsądny sposób i nie może generować zysków dla administratora danych z tytułu wykonania żądania).

3) Odpowiedź na żądanie musi być zrealizowana w terminie **do jednego miesiąca**.

W razie wątpliwości należy skonsultować się z zarządem, Działem IT lub Inspektorem Ochrony Danych.

ZAŁĄCZNIKI:

1. Wzór odpowiedzi na żądanie
2. Wzór ewidencji realizacji żądania dostępu do danych osobowych
3. Wyjaśnienie zasad wynikających z artykułu 15 RODO

Dostęp do danych – procedura postępowania (załącznik do Polityki bezpieczeństwa)

Załącznik nr 1

WZÓR ODPOWIEDZI NA ŻĄDANIE

_____, dnia __.__.____ r.

Dane administratora:

_____

_____

Dane wnioskodawcy:

_____

_____

W odpowiedzi na żądanie dostępu do przetwarzanych danych z dnia __.__.____ r. poniżej przekazujemy informacje niezbędne do realizacji wniosku.

Rodzaj przetwarzanych danych	*Wpisujemy zgodnie ze stanem faktycznym: imię, nazwisko, adres zamieszkania, adres e-mail, numer telefonu*
Podstawa przetwarzania danych	*Podajemy zgodnie z obowiązkiem informacyjnym*
Cel przetwarzania danych	*Podajemy zgodnie z obowiązkiem informacyjnym*
Okres, w którym dane będą przechowywane	*Podajemy zgodnie z obowiązkiem informacyjnym*
Czy dane zostały przekazane podmiotom współpracującym z Administratorem?	TAK/NIE
Prawa osoby zgłaszającej żądanie	*Podajemy zgodnie z obowiązkiem informacyjnym*

_____

(podpis osoby upoważnionej przez administratora danych)

Załącznik nr 2

WZÓR EWIDENCJI REALIZACJI ŻĄDANIA DOSTĘPU DO DANYCH

Lp.	Data wpłynięcia żądania	Dane osoby zgłaszające żądanie	Forma żądania (e-mail, pismo, telefon, osobiście)	Data realizacji żądania	Forma realizacji żądania	Rodzaj przekazanych danych	Podpis osoby realizującej żądanie

Załącznik nr 3

WYJAŚNIENIE ZASAD WYNIKAJĄCYCH Z ARTYKUŁU 15 RODO

Jednym z filarów ochrony danych osobowych jest zagwarantowanie osobie fizycznej prawa dostępu do informacji o przetwarzanych przez administratora danych oraz uzyskania ich kopii. Zgodnie z art. 15 RODO, każda osoba ma prawo uzyskać potwierdzenie, czy jej dane są przetwarzane – jeżeli ma to miejsce administrator danych powinien poinformować daną osobę o:

- celu przetwarzania jej danych osobowych,
- kategorii przetwarzanych danych (np. imię i nazwisko, adres e-mail, informacje o stanie zdrowia),
- odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione (ze zwróceniem szczególnej uwagi na odbiorców w organizacjach międzynarodowych lub państwach trzecich – w tym przypadku należy również poinformować wnioskującego o zabezpieczeniach związanych z przekazaniem danych, zgodnie z art. 46 RODO[1]),
- planowanym okresie przechowywania danych osobowych (a w przypadku, kiedy nie będzie możliwe wskazanie konkretnego terminu przetwarzania danych, kryteriów niezbędnych do określenia tego okresu),
- przysługujących danej osobie uprawnieniach, tj. prawie do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz o możliwości wniesienia sprzeciwu wobec takiego przetwarzania i skargi do organu nadzorczego,
- źródle, z którego dane zostały pozyskane w przypadku, kiedy nie nastąpiło to bezpośrednio od osoby której dane dotyczą (w sytuacji, w której Administrator korzystał z wielu źródeł informacji, dopuszczalne jest przedstawienie ogólnych informacji o ich źródle pochodzenia, np. poprzez poinformowanie odbiorcy, że jego dane zostały pozyskane ze źródeł ogólnodostępnych)
- profilowaniu i automatycznym podejmowaniu decyzji wobec podmiotu danych – o ile takie działania są prowadzone. W tym przypadku należy powiadomić wnioskującą osobę o zasadach podejmowania wskazanych działań oraz o ich znaczeniu i przewidywanych konsekwencjach mających bezpośredni wpływ na osobę, której dane dotyczą. Poniżej przykłady obrazujące omawiane działania:
    - ✓ w przypadku monitorowania aktywności użytkownika na naszej stronie internetowej (czas spędzony na jej przeglądaniu oraz otwierane zakładki) musimy go o tym poinformować, ale nie musimy mieć na to odrębnej zgody. Jeżeli jednak wykorzystywany przez nas do monitorowania (profilowania) algorytm będzie wywoływał skutki prawne dla tej osoby lub podobnie na nią wpływał, użytkownik strony musi udzielić nam zgody na nasze działanie;
    - ✓ wykorzystując algorytm odrzucający z puli złożonych CV np. osoby po 30 roku życia, nie mające prawa jazdy, nie mające wykształcenia wyższego w stopniu magistra, na podjęcie opisanych działań wymagana jest zgoda osoby składającej dokumenty,

[1] *Art. 46 RODO: Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń* – artykuł ten określa w jakich sytuacjach i przy podjęciu jakich działań zabezpieczających, dane osobowe mogą być przekazane do państwa trzeciego lub organizacji międzynarodowych.

ponieważ działania te wykonywane są bez udziału człowieka i mają istotny wpływ na danego kandydata.

Treść Art. 15 RODO wskazuje również, że Administrator zobowiązany jest do **nieodpłatnego:**

- udostępnienia żądanych informacji oraz
- przekazania pierwszej kopii danych osobowych, które podlegają procesowi przetwarzania,

osobie, której te dane dotyczą. Kwestia pobieranych opłat za kolejne udostępnienie danych, zgodnie z omawianym artykułem RODO, pozostaje w gestii administratora danych: kolejne udostępnienia mogą również być bezpłatne lub może być za nie pobierana opłata, którą ustala adminiostrator danych, ale której wysokość jest miarkowana (tzn. musi kształtować się w rozsądny sposób i nie może generować zysków dla Administratora z tytułu wykonania żądania).

Do decyzji osoby zgłaszającej żądanie, choć w ramach zamkniętego katalogu określonego w omawianym art. 15 RODO, pozostaje zakres uzyskanych informacji czy danych, które są przekazywane w postaci kopii (podmiot danych może wnioskować o informacje na temat jednej z przetwarzanych danych bądź na temat całości, może również prosić o kopię lub wgląd do przetwarzanych danych).

Zasada ta nie ogranicza jednak prawa Administratora do przyjęcia takich rozwiązań organizacyjnych i technicznych, które skutkowałyby każdorazowym udostępnieniem osobie zgłaszającej żądanie całości jej danych, które podlegają procesowi przetwarzania. Należy również pamiętać, że w przypadku wątpliwości Administrator ma prawo zwrócić się do osoby występującej z żądaniem z prośbą o doprecyzowanie wnioskowanego zakresu.

Istotną kwestią jest również to, że udzielenie odpowiedzi na żądanie osoby, której dane są przetwarzane, nie stanowi podstawy do usunięcia danych czy skrócenia okresu ich archiwizowania, wynikającego z przepisów prawa. Prawo dostępu do danych nie jest również jednoznaczne z prawem do przenoszenia danych (które wynika z art. 20 RODO) oraz nie wyczerpuje żądania podmiotu danych dotyczącego przesłania jego danych innemu podmiotowi.

OŚWIADCZENIE O POUFNOŚCI[1]

W związku z wykonywanymi przeze mnie czynnościami, związanymi bezpośrednio z dostępem do pomieszczeń Urzędu Miejskiego w Sierpcu, w których odbywa się przetwarzanie danych osobowych

ja, niżej podpisana/podpisany: Ewa Krydzińska

- oświadczam, iż jestem świadoma/świadomy tego, że nie przysługuje mi prawo do przetwarzania danych osobowych administrowanych przez Administratora, w szczególności prawo wglądu do dokumentów papierowych ani dostępu do systemu informatycznego służącego do przetwarzania danych osobowych,
- zobowiązuję się do niedokonywania przetwarzania danych osobowych,
- zobowiązuję się do niezwłocznego informowania Administratora (Burmistrza Miasta Sierpca lub osób jego reprezentujących) o stwierdzonych naruszeniach bezpieczeństwa danych osobowych,
- zobowiązuję się do tego, że w przypadku wejścia w posiadanie danych osobowych w związku z zaistniałym naruszeniem bezpieczeństwa danych zachowam te dane w poufności.

Oświadczam także, że znane mi są przepisy prawa dotyczące ochrony danych osobowych oraz że jestem świadoma/świadomy odpowiedzialności prawnej (w tym karnej) związanej z naruszeniem tych przepisów. Przyjmuję ponadto do wiadomości, że naruszenie tych przepisów może stanowić ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu pracy lub natychmiastowego rozwiązania umowy cywilnoprawnej, bez zachowania okresu wypowiedzenia.

_____

(data i podpis osoby składającej oświadczenie)

[1] Niniejsze oświadczenie wypełniają osoby, które w ramach obowiązków służbowych NIE PRZETWARZAJĄ DANYCH OSOBOWYCH. Osoby, które w ramach obowiązków służbowych przetwarzają dane osobowe, otrzymują JEDYNIE upoważnienie do przetwarzania danych osobowych.

Zasady dotyczące używania urządzeń mobilnych

1. W przypadku dopuszczenia do użytku urządzeń typu telefon komórkowy, tablet, iPad itp., należy zabezpieczyć je:
    1) kodem PIN – używanym w celu rozpoczęcia pracy na urządzeniu po jego włączeniu;
    2) kodem PIN, gestem lub hasłem – używanym w celu wznowienia pracy na urządzeniu po jego zablokowaniu lub przerwaniu pracy.
2. Kod PIN oraz dodatkowe zabezpieczenie urządzenia przenośnego, są znane tylko jego użytkownikowi. Użytkownik nie może ujawniać tych danych osobą postronnym.
3. W razie zapomnienia kodu PIN lub dodatkowego zabezpieczenia, użytkownik informuje o tym ASI i postępuje zgodnie z jego wskazówkami.
4. Kod PIN oraz informacje dotyczące dodatkowego zabezpieczenia, nie powinny być zapisywane przez użytkownika na kartkach, w notesach itp., pozostawianych w miejscu pracy lub poza nim.
5. Użytkownik urządzenia przenośnego nie doprowadza do sytuacji, w których urządzenie to mogłoby zostać zgubione lub skradzione (np. nie pozostawia go w samochodzie, kieszeni kurtki oddawanej do szatni itp.)
6. W przypadku zgubienia lub kradzieży urządzenia przenośnego użytkownik informuje o tym ASI i postępuje zgodnie z jego wskazówkami
7. Użytkownik komputera przenośnego, używający go poza biurem, korzysta wyłącznie z bezpiecznych sieci wi-fi, oferowanych przez hotele, restauracje, lotniska itp. miejsca, np. zabezpieczonych hasłem dostarczonym przez te miejsca.
8. ADO może podjąć decyzję o obowiązkowej instalacji na urządzeniach przenośnych programów antywirusowych lub innego oprogramowania służącego bezpieczeństwu danych.

Praca w systemach IT (wersja dla ADO)

Spis treści

1. Zasady uwierzytelniania w systemach IT

1. Podczas wpisywania hasła w formatce logowania nie powinno ujawniać się znaków – znaki te powinny być ukryte lub zamaskowane znakami specjalnymi.
2. Liczba błędnych prób logowania powinna być ograniczona (minimum do pięciu prób), a po przekroczeniu dozwolonej liczby prób logowania, dostęp do systemu powinien być zablokowany.
3. Wskazane jest, żeby systemy wymuszały zmianę hasła w regularnych odstępach czasu. Okres zmiany hasła nie powinien być mniejszy niż 90 dni.
4. Jeśli w systemie informatycznym występuje możliwość ustawienia ponownego użycia historycznego hasła, wartość parametru musi blokować przynajmniej pięć ostatnich haseł użytkownika.
5. Hasła nie mogą być zapisywane w systemie informatycznym w postaci jawnej – hasła muszą być przechowywane w systemach w zaszyfrowanej formie.
6. Podczas zmiany hasła system powinien wymagać potwierdzenia zmiany starym hasłem oraz dwukrotnego wprowadzenia nowego hasła.
7. Nowe hasła powinny być udostępniane w sposób gwarantujący poufność, po przeprowadzaniu jednoznacznej identyfikacji użytkownika.
8. Login każdego użytkownika, zdefiniowany w systemie informatycznym, musi być unikalny i musi identyfikować tylko jednego użytkownika.
9. Login użytkownika umożliwiający zalogowanie do systemu informatycznego nie podlega zmianie.
10. Login pracownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być ponownie nadany innemu użytkownikowi.
11. Wszelkie dostępy użytkowników, z którymi umowa ulegnie rozwiązaniu, powinny być zablokowane niezwłocznie po zakończeniu współpracy.

12. Wszelki dostęp do systemów informatycznych pracownika, w przypadku postępowania dyscyplinarnego, powinien zostać prewencyjnie zablokowany.
13. Wskazane powyżej czynności, związane z blokowaniem dostępu, powinny zostać udokumentowane.
14. Bez względu na przyczyny odebrania lub nadania dostępu, historia czynności wynikających z działań na kontach nie może zostać usunięta.
15. Dostępy użytkowników do systemów informatycznych powinny podlegać okresowemu przeglądowi i weryfikacji ze stanem faktycznym.
16. Tworzenie kont grupowych jest zabronione o ile ADO nie wyrazi na to zgody.
17. Konta typu "gość" oraz inne konta, które nie są przypisane do konkretnej osoby i nie są wymagane do prawidłowego działania systemu czy procesów wspomagających przetwarzanie, są niedozwolone. ADO może jednak w uzasadnionych przypadkach wyrazić zgodę na wykorzystywanie takich kont. Utworzenie konta przeznaczonego dla zewnętrznych użytkowników, m.in. pracowników dostawcy oprogramowania czy bezpośredniego wsparcia informatycznego, powinny wynikać z zapisów umowy.
18. Konta zewnętrznych użytkowników powinny być specjalnie oznaczone – najlepiej, żeby były aktywne tylko na czas wykonywanych prac, a ich uprawnienia powinny być ograniczone do minimum.
19. W szczególnych wypadkach dopuszcza się użycie kont, które nie podlegają wymogom czasowej zmiany hasła. Konta takie mogą być tworzone tylko do właściwego funkcjonowania procesów systemowych.
20. Wszystkie hasła domyślne należy zmienić przed wprowadzeniem rozwiązania do środowiska produkcyjnego.
21. Konta administratorskie oraz konta użytkowników z uprawnieniami wykraczającymi poza użytkową obsługę systemów informatycznych, powinny być szczególnie kontrolowane pod względem nadawania i zmiany uprawnień.
22. Wszelkie czynności wykonywane przez administratora i użytkowników z uprawnieniami wykraczającymi poza użytkową obsługę aplikacji, powinny być przypisane do indywidualnego konta takiego użytkownika.
23. ADO powinien położyć szczególny nacisk na odpowiednie rejestrowanie czynności wykonywanych przy wykorzystaniu kont niestandardowych. Rejestr powinien być przechowywany nie krócej niż jeden rok, o ile ADO nie zatwierdzi innych okresów przechowywania dla konkretnych logów lub nie zostanie to uregulowane ustawowo. Rejestr może mieć postać logu wykonywanego automatycznie przez zastosowany system monitorujący.

2. Zasady autoryzacji w systemach IT

1. Użytkownicy, po zalogowaniu, powinni mieć dostęp tylko do tych funkcji, które wynikają z przyznanych uprawnień.
2. Przyznane pracownikom uprawnienia powinny być adekwatne do wykonywanych obowiązków służbowych.
3. Zmiana uprawnień do systemów informatycznych może nastąpić tylko na podstawie wniosków zatwierdzonych przez ADO.
4. Wszelkie uprawnienia użytkowników, z którymi umowa ulegnie rozwiązaniu, powinny być zablokowane niezwłocznie po zakończeniu współpracy.
5. Przed czynnościami związanymi z odbieraniem uprawnień powinny zostać wystawione stosowne dokumenty. Historia związana z nadaniem, zmianą i odebraniem uprawnień nie może zostać usunięta.

6. Uprawnienia użytkowników w systemach informatycznych powinny podlegać okresowemu przeglądowi.

3. Zasady konfiguracji i wykorzystywania stacji roboczych

1. Wygaszacz ekranu komputera powinien być skonfigurowany w taki sposób, by uruchamiał się automatycznie. Czas uruchomienia wygaszacza uwarunkowany jest od dostępu osób postronnych do pomieszczenia, w którym znajduje się komputer.
2. Wyłączenie wygaszacza ekranu musi wymagać od użytkownika podania loginu i hasła do systemu operacyjnego.
3. Wszystkie stacje robocze podłączone do sieci ADO muszą być objęte ochroną systemu zabezpieczającego oraz podlegać regularnej aktualizacji zabezpieczeń.
4. O ile ADO nie udzielił na to zgody, żadna zewnętrzna stacja robocza nie może być połączona do jego środowiska informatycznego.
5. W przypadku wyrażenia zgody na podłączenie stacji zewnętrznej, np. należącej do pracownika firmy zewnętrznej, ADO powinien zwrócić szczególną uwagę na to, czy stacja taka posiada min. aktualny system ochrony przed szkodliwym oprogramowaniem.

4. Zasady dostępu zdalnego do infrastruktury ADO

1. Zdalny dostęp do infrastruktury informatycznej ADO może zostać przyznany, jeśli będzie realizowany przy użyciu konta określonego w umowie. Do jego realizacji użyte zostaną mechanizmy zapewniające silne uwierzytelniania.
2. W celu uzyskania dostępu do sieci wewnętrznej ADO, podmioty zewnętrzne muszą chronić swoją infrastrukturę zgodne z ogólnie przyjętymi standardami zabezpieczeń.
3. W celu udostępnienia zdalnej obsługi konkretnemu użytkownikowi, należy nadać mu indywidualny identyfikator i ograniczyć możliwość działania jedynie do konkretnych komputerów i/lub aplikacji wymagających wsparcia.
4. W miarę możliwości konto pracownika zewnętrznego, umożliwiające skorzystanie ze zdalnego dostępu do infrastruktury informatycznej, powinno być uruchamiane wyłącznie na żądanie i aktywne w przedziale czasu niezbędnym do wykonania zadania. Jeśli to możliwe, działanie użytkownika powinno być monitorowane przez pracownika ADO uczestniczącego w prowadzonych pracach.

5. Zasady konfiguracji i wykorzystywania elementów sieciowych u ADO

1. Wszystkie połączenia pomiędzy sieciami muszą zostać zatwierdzone przez ADO i muszą być zabezpieczone przez zaporę sieciową oraz właściwą kontrolę dostępu.
2. Zabronione jest korzystanie, bez wiedzy ADO, z rozwiązań umożliwiających jednoczesny bezpośredni dostęp do sieci zewnętrznej oraz wewnętrznej.
3. Wszelkie połączenia pomiędzy sieciami, urządzeniami lub aplikacjami muszą być przeprowadzane w sposób, który nie zagraża bezpieczeństwu sieci wewnętrznej ADO. W miarę możliwości takie połączenie powinny być zabezpieczone poprzez szyfrowanie.
4. ADO utrzymuje listy urządzeń podłączonych do sieci ich adresy MAC oraz informację do jakich portów w przełącznikach sieciowych zostały podłączone.
5. Wewnętrzna konfiguracja infrastruktury sieciowej, np. adresy IP, architektura sieci oraz infrastruktura systemów informatycznych ADO, mogą być udostępniane wyłącznie upoważnionym osobom.

6. Zasady postępowania z nośnikami danych

1. Z nośników danych może korzystać tylko ograniczona grupa użytkowników – możliwość korzystania z nośników danych mogą mieć użytkownicy, którzy muszą odczytywać udostępniane im informacje na nośnikach oraz muszą wykonywać kopie zapasowe.
2. W wyjątkowych sytuacjach, za zgodą ADO oraz przy zastosowaniu szczególnych środków bezpieczeństwa, dopuszczalne jest korzystanie z nośników danych dostarczonych przez osoby z zewnątrz.
3. Nośniki danych wykorzystywane przez pracowników, powinny zostać specjalnie oznaczone tak, aby doszło do pomyłki z innym urządzeniem tego typu.
4. W przypadku decyzji ADO o zniszczeniu nośników albo przekazaniu/sprzedaży urządzeń podmiotom zewnętrznym, należy uruchomić działania zapewniające, że z tych nośników lub urządzeń nie będzie można w żaden sposób odzyskać przetwarzanych na nich danych osobowych.
5. W przypadku elektronicznych nośników informacji przeznaczonych do likwidacji, w pierwszej kolejności usuwa się dane osobowe, a w przypadku gdy nie jest to możliwe, uszkadza się nośnik fizycznie w sposób uniemożliwiający odczytanie zapisanych na nim treści.
6. ADO, w celu usunięcia danych, może korzystać z zakontraktowanych zewnętrznych firm specjalizujących się w niszczeniu informacji. W celu zapewnienia właściwego wykasowania danych osobowych, czynności związane z usuwaniem powinny być przeprowadzone lub nadzorowane przez upoważniony personel ADO.

7. Zasady dotyczące zabezpieczeń infrastruktury informatycznej ADO

1. Systemy zabezpieczające infrastrukturę sieciową muszą zapewniać ochronę zarówno przed próbami włamania od wewnątrz, jak i z zewnątrz. Dostęp do takich systemów musi być ograniczony.
2. Wykrywanie i blokowanie złośliwego oprogramowania lub nieautoryzowanego ruchu sieciowego musi być zapewnione przez instalację oprogramowania na wszystkich rodzajach urządzeń wchodzących w skład infrastruktury informatycznej, w sposób zapewniający odpowiednie bezpieczeństwo na każdym poziomie środowiska informatycznego.
3. Wskazane jest, aby systemy zapewniające ochronę pochodziły od różnych producentów, korzystały z różnych mechanizmów wyszukiwania oraz wzajemnie się uzupełniały.
4. Wykorzystywane oprogramowania zabezpieczającego wraz z sygnaturami złośliwego kodu, muszą być regularnie aktualizowane.
5. Aplikacje chroniące zasoby komputera powinny być skonfigurowane tak, żeby naprawiały zainfekowane pliki. W przypadku braku możliwości naprawy pliku muszą go odseparować, poddać kwarantannie i poinformować użytkownika lub wysłać stosowna informację do osób odpowiedzialnych za monitorowanie.
6. Szczególną uwagę należy przywiązywać do aktualizacji zastosowanych zabezpieczeń. Standardowo systematyczność aktualizacji powinna zostać określona w oparciu o częstotliwość aktualizacji udostępnianych przez producenta. Termin wykonania aktualizacji powinien być uzależniony od poziomu jej krytyczności. Każdorazowo należy zachować ostrożności podczas instalacji aktualizacji.

8. Zasady dotyczące monitorowania infrastruktury informatycznej ADO

1. Monitorowanie infrastruktury informatycznej pod kątem zgodności ze standardami bezpieczeństwa, jest procesem polegającym na analizie zdarzeń przechowywanych w dziennikach zdarzeń.

2. ADO powinien dążyć do tego, żeby proces monitorowania był w jak największym stopniu scentralizowany – działanie to ma na celu osiągnięcie odpowiednio szybkiego wyszukiwania powiązań pomiędzy zdarzeniami bezpieczeństwa.
3. Proces monitorowania powinien być wspierany przez szereg rozwiązań zapewniających, w szczególności, wykrywanie złośliwego kodu, wykrywanie włamań, wykrywanie podatności.
4. Wszystkie systemy informatyczne, biorące udział w przetwarzaniu danych osobowych, powinny umożliwiać logowanie zdarzeń w dziennikach zdarzeń.
5. Rejestrowanie powinno obejmować w szczególności anomalie, zachowania nieuprawnione oraz działania niezgodne z przyjętymi zasadami bezpieczeństwa. W miarę możliwości zapisywane powinny być również połączeń z sieciami zewnętrznymi.
6. Dzienniki zdarzeń powinny być odpowiednio zabezpieczone, przechowywane w bezpieczny sposób oraz być dostępne tylko dla upoważnionych osób.
7. W miarę możliwości wszelkie problemy w rejestracji zdarzeń dziennika powinny spowodować wygenerowanie ostrzeżenia.
8. Należy zapewnić środki umożliwiające informowanie o wszelkich zmianach nieautoryzowanej zmiany konfiguracji, w szczególności elementów infrastruktury informatycznej biorących udział w przetwarzaniu danych osobowych.

9. Zasady dotyczące postępowania w przypadku procesu odtworzenia i wykonywania kopii zapasowych

1. ADO powinien dysponować planem reakcji w momencie wystąpienia zakłócenia o dużym znaczeniu, prowadzącego do sytuacji, w której konieczne będzie odbudowanie swojej infrastruktury informatycznej.
2. Plan powinien zakładać zdefiniowanie zadań oraz głównych etapów, a także przydzielenie odpowiedzialności w zakresie ich wykonania.
3. W działaniach zmierzających do odtworzenia funkcjonalności odpowiedzialnych za przetwarzanie danych osobowych, mogą brać udział pracownicy firm zewnętrznych. W tym wypadku ADO powinien posiadać stosowne umowy serwisowe ustalające ten obszar działania.
4. Podstawą procesu odtworzenia są regularnie wykonywane kopie zapasowe baz danych, w których są przechowywane dane osobowe.
5. W skład kopii zapasowych powinny wchodzić również wszelkie elementy związane z konfiguracją infrastruktury informatycznej. W miarę możliwości kopie zapasowe mogą obejmować również aplikacje wykorzystywane do przetwarzania danych.
6. W zależności od możliwości, ADO może magazynować kilka jednakowych kopii zapasowych. W celu podwyższenia standardów bezpieczeństwa jedna z nich powinna być zapisywana na nośniku zewnętrznym podłączanym tylko na czas wykonywania czynności kopiowania.
7. Kopie zapasowe mogą być przechowywane na innych serwerach, jednakże wówczas powinny być zabezpieczone przy wykorzystaniu środków kryptograficznych.
8. Należy zapewnić wykonywanie regularnych kopii danych przechowywanych na zewnętrznych nośnikach, kopie powinny zostać zaszyfrowane.
9. Nośniki danych, na których znajdują się kopie zapasowe powinny być przechowywane w bezpiecznym miejscu, do którego nie maja dostępu osoby postronne.
10. Bezwzględnie powinno się przestrzegać ustalonych terminów sporządzania kopii zapasowych oraz dokonywać okresowych kontroli odczytu danych zapisanych na tych dyskach. W miarę możliwości powinno się dokonywać weryfikacji wykonywanych kopii zapasowych podczas testów odtworzeniowych.

Praca w systemach IT (wersja dla użytkowników)

Niniejsze reguły, dotyczące uwierzytelniania i autoryzacji, stosuje się przy pracy w systemach informatycznych, do których możliwy jest dostęp zarówno z komputerów stacjonarnych, laptopów lub pozostałych urządzeń przenośnych.

Spis treści

1. Zasady uwierzytelniania w systemach IT

1. Każdy użytkownik jest odpowiedzialny za działania związane z przypisanymi mu kontami wykorzystywanym w systemach informatycznych.
2. Każdy pracownik musi przestrzegać zasad dotyczących stosowania mechanizmów uwierzytelniania w systemach informatycznych.
3. Hasło użytkownika do systemu informatycznego musi być zmieniane przez użytkownika regularnie, nie rzadziej niż co 90 dni. Użytkownik musi zmieniać hasło, niezależnie od tego, czy system informatyczny wymusza zmianę automatycznie.
4. Zmieniając hasło dostępu na nowe, użytkownikowi nie wolno wybrać pięciu ostatnio używanych haseł.
5. Hasło używane do logowania się musi spełniać następujące wymogi:
    1) długość: nie krótsze niż 8 znaków,
    2) stopień skomplikowania: minimum jedna mała litera, minimum jedna duża litera, minimum jedna cyfra lub znak specjalny,
6. Użytkownik musi posługiwać się hasłem spełniającym powyższe wymogi, niezależnie od tego, czy system informatyczny wymusza ich przestrzeganie.
7. Tworząc hasła użytkownik nie powinien stosować kombinacji znaków prowadzącej do łatwego ustalenia hasła przez osoby nieupoważnione. Szczególnie powinno zwracać się uwagę na niewykorzystywanie jako jedynego składnika hasła imion, nazwisk, numeru swojego telefonu, numeru rejestracyjnego swojego pojazdu itp. Wykluczone są także hasła w rodzaju 123456, qwerty, zaq12wsx itp.
8. Login lub hasło nie może być zapisywane przez użytkownika na kartkach, w notesach itp.

9. Jeżeli użytkownik będzie miał podejrzenie, że jego hasło mogło zostać odczytane lub przechwycone przez inną osobę, powinien zgłosić ten fakt do odpowiedniej jednostki.
10. Wielokrotne wprowadzenie błędnego hasła oznacza zablokowanie dostępu do systemu informatycznego.
11. Hasło użytkownika do systemu informatycznego jest znane tylko jemu. Użytkownik nie może ujawniać swojego hasła w klientom, współpracownikom lub innym osobom.
12. Niedopuszczalna jest sytuacja, w której jeden użytkownik loguje się do systemu informatycznego, korzystając z loginu lub hasła drugiego użytkownika, np. pod jego nieobecność w pracy.
13. W przypadku, gdy użytkownik zapomni swoje hasło lub zablokuje dostęp do systemu informatycznego w związku z wprowadzeniem błędnego hasła, powinien skontaktować się z osobą odpowiedzialną za zarządzanie dostępem do danego systemu informatycznego i postępować zgodnie z jego wskazówkami.
14. Nowo nadane hasło powinno zostać zmienione przez użytkownika przy pierwszym logowaniu.
15. Dostęp do systemów informatycznych udostępnianych przez ADO może zostać ograniczony lub zablokowany w przypadku, gdy użytkownik postępuje niezgodnie z ustalonymi zasadami.
16. Wobec użytkownika, który nie stosuje się do ustalonych zasad, ADO może zastosować konsekwencje dyscyplinarne.
17. ADO zastrzega sobie prawo do monitorowania dostępu użytkowników do systemów, jeżeli ma powody sądzić, że informacje z systemów są wykorzystywane w sposób zagrażający przetwarzaniu danych osobowych, prowadzący do wystąpienia incydentu bezpieczeństwa związanego z wyciekiem informacji. Użytkownicy są o takim monitorowaniu uprzednio informowani.

2. Zasady autoryzacji w systemach IT

1. Użytkownicy, po zalogowaniu, powinni mieć dostęp tylko do funkcji lub modułów, które wynikają z przyznanych uprawnień.
2. Zabronione jest wykonywanie czynności mających na celu nieautoryzowane zmiany uprawnień, wykorzystywanie ewentualnych luk lub przełamywanie zabezpieczeń w celu uzyskania szerszego dostępu do danych przetwarzanych w systemie.
3. Wszelkie zaobserwowane zmiany w przyznanych uprawnieniach powinny zostać bezzwłocznie zgłoszone ADO lub osobie odpowiedzialnej za zarządzanie bezpieczeństwem.

3. Zasady dotyczące pracy w systemach IT

1. Niewłaściwe korzystanie z systemów informatycznych lub innych form komunikacji elektronicznej może prowadzić do powstania zagrożeń dla przetwarzanych danych osobowych.
2. Rozpoczynając pracę w systemie informatycznym użytkownik powinien zalogować się własnymi loginem i hasłem.
3. W przypadku konieczności przerwania pracy przy komputerze na krótki czas, użytkownik powinien zablokować stację roboczą lub wylogować się z systemu informatycznego (np. poprzez użycie kombinacji: [klawisz Windows] + [L] w systemie operacyjnym Windows).
4. Po zakończonej pracy użytkownik powinien wylogować się z systemów informatycznych oraz wyłączyć komputer

4. Zasady dotyczące pracy na stacjach roboczych

1. Na komputerach służbowych powinny być gromadzone i wykorzystywane tylko pliki i informacje związane z wykonywaniem obowiązków służbowych. Wykluczone jest przechowywanie na komputerach służbowych prywatnych plików muzycznych, wideo, zdjęć itp.
2. Każdy użytkownik jest odpowiedzialny za sposób korzystania ze stacji roboczych, a w szczególności za ewentualną instalację wszelkiego rodzaju złośliwego oprogramowania (np. wirusów, koni trojańskich), mającego wpływ na funkcjonowanie bądź monitorowanie infrastruktury informatycznej.
3. Użytkownikowi zabronione jest podejmowanie prób mających na celu:
    1) zmianę ustawień dotyczących bezpieczeństwa lub
    2) samowolną instalację lub usuwanie oprogramowania
4. Użytkownik, który stwierdzi, że oprogramowanie zabezpieczające komputer jest nieaktywne lub otrzymuje powiadomienia z takiej aplikacji, powinien natychmiast powiadomić ADO bądź osobę odpowiedzialną za zarządzanie bezpieczeństwem.
5. W przypadku podejrzenia, że stacja robocza została zainfekowana przez szkodliwe oprogramowanie, należy natychmiast odłączyć ją od sieci a o podejrzeniu infekcji powiadomić ADO bądź osobie odpowiedzialnej za zarządzanie bezpieczeństwem.
6. Powinno unikać się przechowywania danych osobowych, a w szczególności danych wrażliwych, na lokalnym dysku stacji roboczej.
7. Jeśli istnieje potrzeba przechowywania danych osobowych poza systemami informatycznymi, preferowanym miejscem przechowywania takich danych są zasoby sieciowe.
8. Z chwilą przeniesienia danych na komputer użytkownika, ponosi on odpowiedzialność za te dane, ich ochronę i dalsze wykorzystanie zgodnie z prawem.
9. Użytkownicy, pracujący na przenośnych komputerach, powinni zachować szczególną ostrożność w trakcie użytkowania ich w pomieszczeniach ogólnodostępnych, do których mają swobodny dostęp osoby z zewnątrz. O ile istnieje taka możliwość, komputer przenośny powinien zostać zabezpieczony przy użyciu specjalnej linki zabezpieczającej.
10. Po godzinach pracy użytkownik komputera przenośnego powinien umieścić go w bezpiecznym miejscu, np. szafie zamykanej na klucz.
11. Użytkownik komputera przenośnego, zabierający go poza obszar przetwarzania danych, transportuje go w specjalnej torbie i nie doprowadza do sytuacji, w których komputer mógłby zostać skradziony lub zgubiony (np. nie pozostawia go w samochodzie, przechowalniach bagażu itp.)
12. W przypadku zgubienia lub kradzieży komputera przenośnego, użytkownik niezwłocznie informuje o sprawie ADO lub osobę wyznaczoną do zarządzania bezpieczeństwem i postępuje zgodnie z jego wskazówkami.
13. Użytkownik komputera przenośnego, używający go poza biurem, korzysta wyłącznie z bezpiecznych sieci wi-fi, oferowanych przez hotele, restauracje, lotniska itp. miejsca, np. zabezpieczonych hasłem dostarczonym przez te miejsca.

5. Zasady dotyczące poczty elektronicznej

1. W celu zapewnienia poufności i bezpieczeństwa przesyłanych informacji, ADO zastrzega sobie prawo do monitorowania i kontrolowania treści przesyłanych wiadomości w możliwie największym, dozwolonym przez prawo zakresie. Użytkownicy są o takim monitorowaniu uprzednio informowani.
2. ADO zastrzega sobie prawo do przyznawania i odbierania dostępu do poczty elektronicznej, wykorzystywanej do celów służbowych.
3. Użytkownicy nie mogą korzystać z systemu pocztowego do realizacji celów osobistych oraz nie mogą przetrzymywać na skrzynce pocztowej informacji niezwiązanych z wykonywaniem obowiązków służbowych.

4. Wiadomości e-mail związane z działalnością ADO powinny być wysyłane tylko przy wykorzystaniu systemu poczty elektronicznej zarządzanej przez ADO.
5. Pracownik jest odpowiedzialny za wiadomości wysyłane z jego konta poczty elektronicznej.
6. Za zgodą ADO dopuszczalne jest korzystanie ze skrzynek współdzielonych, które może obsługiwać kilku pracowników. W takim wypadku należy jednak wyznaczyć osobę, która będzie odpowiedzialna m.in. za wiadomości wysyłane z takiej skrzynki pocztowej.
7. Otwieranie wiadomości e-mail powinno być wykonywane ostrożnie. Przed otworzeniem wiadomości, a w szczególności załączników, nadawca oraz temat powinny zostać zweryfikowane.
8. Niedozwolone jest otwieranie, a w szczególności pobieranie załączników oraz uruchamianie linków z wiadomości e-mail pochodzących od podejrzanych, niewiarygodnych nadawców, zawierających temat budzący wątpliwości lub inne podejrzane elementy, np. literówki w nazwach nadawców.
9. Każdorazowo, kiedy użytkownik otrzymuje wiadomość e-mail zawierającą załączone pliki, musi wykazać ostrożność. Jeśli są to pliki wykonywalne, np. programy (EXE) lub skrypty (VB lub JB), załączniki takie nie mogą być otwierane.
10. W przypadku zaobserwowania powyżej wymienionych symptomów oraz w przypadku, gdy treść e-maila wskazuje na cel wyłudzenia informacji, użytkownik powinien powiadomić ADO lub osobę odpowiedzialną za zarządzanie bezpieczeństwem.
11. Użytkownicy nie powinni przekazywać wiadomości zawierających dane osobowe, w szczególności dane wrażliwe, na adresy e-mail nie będące:
    1) własnością osób, których dane dotyczą;
    2) własnością ADO;
    3) adresami podmiotów, z którymi ADO współpracuje
12. ADO może wyrazić zgodę na wysłanie wiadomości zawierających dane osobowe w szczególności dane wrażliwe na inne adresy e-mail, niewskazane powyżej.
13. W razie konieczności wykorzystania poczty elektronicznej do przesłania danych osobowych, w szczególności danych wrażliwych, konieczne jest ich zabezpieczenie przy wykorzystaniu szyfrowania bądź innego sposobu zapewniającego odpowiednią poufność przesyłanych danych.
14. Jeśli wykorzystywany sposób zabezpieczenia przekazywanych danych wymaga przekazania hasła, w żadnym wypadku nie można przekazać go tym samym kanałem komunikacyjnym, którym zostały wysłane dane osobowe.
15. W miarę możliwości należy dążyć do stworzenia zaufanej listy adresów e-mail, na które będą wysyłane dane osobowe.
16. Zabronione jest wysyłanie wiadomości zawierających dane osobowe do wielu odbiorców, w szczególności niedopuszczalne jest korzystanie z opcji „Odpowiedz wszystkim”. W razie konieczności wysłania zawierających dane osobowe do wielu odbiorców należy używać opcji „Ukryte do wiadomości / UDW / BCC”.
17. Zabronione jest przesyłanie jakichkolwiek informacji służbowych na prywatne skrzynki pocztowe oraz ustawianie reguł systemu pocztowego, powodujących automatyczne przekierowanie wiadomości na prywatne skrzynki pocztowe.
18. Zabroniona jest rejestracja w serwisach internetowych (bądź listach mailingowych) przy użyciu służbowego adresu e-mail bez wiedzy i zgody bezpośredniego przełożonego lub ADO.

6. Zasady dotyczące korzystania z internetu

1. ADO traktuje Internet jako obszar prowadzenia swojej działalności, który udostępniony jest użytkownikowi w celu osiągania spodziewanych wyników pracy. Uzyskanie dostępu do Internetu nie jest równoznaczne ze zgodą na realizację prywatnych celów pracownika.
2. Dostęp do Internetu powinien zostać przyznany wyłącznie tym użytkownikom, którym jest niezbędny dla wykonywania obowiązków służbowych.
3. ADO zastrzega sobie prawo do przyznawania lub odbierania prawa dostępu do Internetu.
4. W celu ochrony działania systemów informacyjnych, ADO zastrzega sobie prawo do monitorowania, filtrowania i blokowania dostępu do Internetu w możliwie największym, dozwolonym przez prawo zakresie. Użytkownicy są o takim monitorowaniu uprzednio informowani.
5. Dostęp do Internetu nie powinien być używany w celu zakłócania systemów IT, a w szczególności nie może prowadzić do zagrożenia dla danych osobowych.
6. Użytkownik, transmitując dane osobowe, w szczególności dane wrażliwe poprzez Internet, ma obowiązek zachować zasady bezpieczeństwa podczas ich przesyłania, w szczególności zapewniając ich poufność.
7. Bez zgody ADO zabronione jest korzystanie z publicznych systemów peer-to-peer, czatów, komunikatorów internetowych, witryn internetowych ukrywających przeglądanie Internetu oraz usług internetowych umożliwiających przekazywanie plików.

7. Zasady dotyczące korzystania z nośników danych

1. Korzystanie z nośników danych jest domyślnie niedozwolone w związku z możliwością powodowania poważnych zagrożeń dla poufności oraz integralności przetwarzanych danych osobowych.
2. Pracownik upoważniony do korzystania z nośników danych, odpowiedzialny jest za ewentualne wprowadzenie złośliwego oprogramowania.
3. Zabrania się pracownikom korzystania z nośników danych nie będących własnością ADO (np. prywatnych pendrive'ów).
4. Każdorazowo w przypadku podłączenia nośnika danych, powinien on zostać sprawdzony przez program zabezpieczający (antywirus).
5. W miarę możliwości wszelkie dane osobowe, przechowywane na nośniku danych, powinny być szyfrowane.
6. Użytkownik musi zapewnić, żeby nośniki danych, na których znajdują się dane osobowe, przechowywane były w bezpiecznym miejscu.
7. Kradzież bądź utrata nośnika danych jest traktowana jako naruszenie bezpieczeństwa i powinna zostać natychmiast zgłaszana do ADO.

Prawo do bycia zapomnianym

Prawo do usunięcia danych to inaczej prawo do zapomnienia – jeżeli Burmistrz Miasta Sierpca (administrator danych) otrzyma żądanie dotyczące tego prawa, **trzeba postępować bardzo ostrożnie, żeby nie usunąć danych, które są przetwarzanie na podstawie przepisów prawa i które jesteśmy zobowiązani przechowywać przez czas określony w tych przepisach.**

Poniżej przedstawiamy kroki, według których należy postępować w przypadku wpłynięcia takiego wniosku:

1. **Sprawdzamy tożsamości osoby**, która zgłosiła żądanie – należy mieć pewność, że pod naszego klienta nie podszyła się osoba trzecia. Można to zrobić w bardzo prosty sposób: należy sprawdzić, czy żądanie zostało wysłane ze źródła, które znajduje się w naszej bazie danych, np. z adresu e-mail, który jest przypisany do wnioskującej osoby (np. czy p.nowak@abc.pl nie prosi o dostęp do danych j.nowak@abc.pl).
2. Jeżeli osoba zgłaszająca żądanie znajduje się w naszej bazie danych, **sprawdzamy jakiego rodzaju dane o tej osobie przetwarzamy**, np. imię, nazwisko, adres zamieszkania, adres e-mail, numer telefonu itp.
3. **Sprawdzamy, na jakiej podstawie są przetwarzane dane osobowe** – takimi podstawami są w szczególności:
    - umowy,
    - zgody (np. na działania marketingowe),
    - odrębne przepisy prawa (np. dotyczące prowadzenia dokumentacji kadrowej, dokonywania rozliczeń itp.).
4. **Realizujemy żądanie** o które prosi dana osoba – zgodnie z zapisami wynikającymi z RODO możemy usunąć tylko te dane, które nie będą nam potrzebne do realizacji obowiązku prawnego. W związku z tym **możemy usunąć wyłącznie te dane, które są przetwarzane na podstawie zgód, np. zgody na przesłanie newslettera.**

   Jeżeli dane, które mogą zostać usunięte, zostały udostępnione innym przedsiębiorstwom, należy poinformować również te przedsiębiorstwa o wpłynięciu danego żądania. Istotnym jest jednak fakt, że informujemy tych przedsiębiorców, o których wiemy, że mogą wykorzystywać dane osobowe osoby zgłaszającej żądanie oraz podejmujemy działanie, o ile nie jest ono dla nas trudne i kosztowne.

5. **Dokumentujemy realizację żądania** w sposób pozwalający na ustalenie komu (imię i nazwisko, adres e-mail z którego wysłano żądanie), kiedy, przez kogo, zostało wykonane żądanie (zasada rozliczalności).

Należy pamiętać o tym, że odpowiedź na żądanie musi być udzielona – zgodnie z art. 12 ust 3. RODO – bez zbędnej zwłoki, nie później niż w terminie jednego miesiąca.

W razie potrzeby termin ten może być przedłużony o kolejne dwa miesiące (ze względu na skomplikowany charakter żądania albo liczbę żądań kierowanych pod adresem Administratora). W takiej sytuacji osoba składająca żądanie musi o tym dowiedzieć się w ciągu miesiąca od przekazania żądania.

W razie wątpliwości należy skonsultować się z zarządem, ASI lub Inspektorem Ochrony Danych.

ZAŁĄCZNIKI:

1. Wzór ewidencji realizacji żądania dostępu do danych osobowych
2. Wzór wiadomości ws. przedłużenia terminu odpowiedzi na żądanie
3. Artykuł 17 RODO: Prawo do usunięcia danych („prawo do bycia zapomnianym”)

Załącznik nr 1

WZÓR EWIDENCJI REALIZACJI ŻĄDANIA

PRAWA DO USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM")

Lp.	Data wpłynięcia żądania	Dane osoby zgłaszające żądanie	Forma żądania (e-mail, pismo, telefon, osobiście)	Data realizacji żądania	Forma poinformowania o realizacji żądania (e-mail, pismo, telefon, osobiście)	Podpis osoby realizującej żądanie

Załącznik nr 2

Szanowna Pani / Szanowny Panie,

dziękujemy za wiadomość. Uprzejmie informujemy, że zgodnie z art. 12 ust. 3 ogólnego rozporządzenia o ochronie danych (RODO), ze względu dużą liczbę zgłoszeń dotyczących danych osobowych oraz skomplikowaną strukturę bazy danych, Pani / Pana wniosek znajduje się w dalszym ciągu w trakcie realizacji. Zapewniamy, że zrealizujemy Pani / Pana żądanie tak szybko jak to jest możliwe. Powrócimy z kolejnymi informacjami nie później niż 30 dni od dnia otrzymania tej wiadomości.

Przepraszamy za długi czas oczekiwania i prosimy o cierpliwość.

Załącznik nr 3

ARTYKUŁ 17 RODO
PRAWO DO USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM")

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;
c. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;
d. dane osobowe były przetwarzane niezgodnie z prawem;
e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego
w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane

osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a. do korzystania z prawa do wolności wypowiedzi i informacji;
b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;
d. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
e. do ustalenia, dochodzenia lub obrony roszczeń.

PROTOKÓŁ LIKWIDACJI ZNISZCZONYCH LUB ZBĘDNYCH DOKUMENTÓW PAPIEROWYCH LUB ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

Rodzaj i oznaczenie dokumentów lub nośników:

_____

_____

Uwagi:

_____

_____

Komisja w składzie[1]:

1. _____,
2. _____,
3. _____

oświadcza, że ww. dokumentu/nośniki zawierające dane osobowe zostały w dniu _____ komisyjnie zniszczone.

Opis procesu zniszczenia:

_____

_____

Podpisy członków komisji:

1. _____
2. _____
3. _____

[1] Wskazać imię, nazwisko i stanowisko członków komisji.

REJESTR CZYNNOŚCI PRZETWARZANIA

Lp.	Kategorie przetwarzanych danych	cele przetwarzania	opis kategorii osób, których dane dotyczą	opis kategorii danych osobowych	kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń	planowane terminy usunięcia poszczególnych kategorii danych	ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art.. 32 ust. 1 RODO
1	REKRUTACJA	Wyłonienie kandydatów do zatrudnienia w ramach procesu rekrutacyjnego	Kandydaci do pracy	Imię (imiona) i nazwisko, imiona rodziców, data urodzenia, adres do korespondencji, wykształcenie, przebieg dotychczasowego zatrudnienia, inne dane przekazane przez kandydata w treści dokumentów rekrutacyjnych	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane kandydatów, którzy nie wyrazili zgody na przetwarzanie ich danych w przyszłych celach rekrutacyjnych - jeden miesiąc od zakończenia procesu rekrutacji. Dane kandydatów niezatrudnionych, którzy wyrazili zgodę na przetwarzanie ich danych w przyszłych celach rekrutacyjnych - 5 dni roboczych od dnia otrzymania oświadczenia o wycofaniu zgody.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
2	PRACOWNICY i WSPÓŁPRACOWNICY	Realizacja obowiązków Administratora, dotyczących stosunku pracy lub współpracy w ramach umów cywilnoprawnych	Osoby zatrudnione u Administratora, niezależnie od podstawy zatrudnienia	Imię (imiona) i nazwisko, imiona rodziców, data urodzenia, adres do korespondencji, wykształcenie, przebieg dotychczasowego zatrudnienia, numer PESEL, adres e-mail, numer telefonu, numer rachunku bankowego	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów. Firmy zajmujące się doradztwem podatkowym. Firmy świadczące usługi z zakresu medycyny pracy. Firmy oferujące usługi brokerskie. Firmy oferujące ubezpieczenia.		Akta pracowników - 50 lat od zakończenia pracy u pracodawcy. Dokumenty osób zatrudnionych na podstawie umów cywilnoprawnych - 10 lat od zakończenia współpracy.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
3	KONTRAHENCI	Zakup lub sprzedaż towarów i usług w ramach działalności Administratora	Kontrahenci Administratora	imię, nazwisko, adres e-mail, numer telefonu, NIP, REGON, numer rachunku bankowego, adres do korespondencji	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		5 lat od daty zakończenia współpracy	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
4	WYDZIAŁ ORGANIZACYJNY	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
5	BIURO SPRAW OBYWATELSKICH	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
6	WYDZIAŁ FINANSOWY	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów. Firmy zajmujące się doradztwem podatkowym.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.

7	BIURO PODATKOWE	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów. Firmy zajmujące się doradztwem podatkowym.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
8	WYDZIAŁ ARCHITEKTURY I GOSPODARKI GRUNTAMI	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
9	WYDZIAŁ INWESTYCJI, REMONTÓW I POZYSKIWANIA FUNDUSZY ZEWNĘTRZNYCH	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
10	WYDZIAŁ OŚWIATY, KULTURY I PROMOCJI	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
11	WYDZIAŁ SPRAW PUBLICZNYCH I KOMUNALNYCH	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
12	URZĄD STANU CYWILNEGO	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.

13	STRAŻ MIEJSKA	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
14	MIEJSKA KOMISJA ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.
15	SPOŁECZNY ZESPÓŁ DO SPRAW ROZDZIAŁU MIESZKAŃ	Realizacja zadań komórki organizacyjnej, zgodnie z Regulaminem Organizacyjnym Urzędu Miejskiego w Sierpcu	Osoby, których dotyczą sprawy znajdujące się w zakresie zadań komórki organizacyjnej	Imię, nazwisko, adres e-mail, telefon kontaktowy, adres zamieszkania, inne dane osobowe niezbędne dla zrealizowania obowiązku prawnego lub zawarcia umowy	Firmy świadczące usługi informatyczne. Firmy zajmujące się niszczeniem dokumentów.		Dane zebrane na podstawie przepisów prawa, dotyczących komórki organizacyjnej - zgodnie z tymi przepisami. Dane zebrane w związku z realizacją umów - po dokonaniu rozliczeń związanych z umową.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczństwa i jej załączników.

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

Lp.	Dane administratora, w imieniu którego działa podmiot przetwarzający	Kategorie przetwarzanych danych	przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń	ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art.. 32 ust. 1 RODO
1.				
2.				
3.				
4.				

L.p.	Naruszenie (stypizowany opis naruszenia)	Data i godzina zgłoszenia podejrzenia naruszenia
1.	Np. zalanie archiwum z dokumentacją pracowników	
2.	Np. Wyciek danych z systemu X	

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Data oraz godzina stwierdzenia naruszenia	Data naruszenia/okres, którego dotyczy

Kategoria i ilość osób, których dotyczy naruszenie

Np. Pracownicy; 50 osób

Np. Klienci, ok. 1000 osób

Zakres danych i/lub kategorie danych, których dotyczy naruszenie

Np. Imię, nazwisko, PESEL, data urodzenia, data zatrudnienia

Np. Imię, nazwisko, adres e-mail, adres dostawy, numer telefonu

Osoba/źródło informacji o zdarzeniu	Miejsce naruszenia
	Np. siedziba administratora

Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia

Opis skutków/konsekwencji naruszenia	Osoba/jednostka odpowiedzialna za naruszenie

Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków

Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych

Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (Jeśli tak - data i godzina zgłoszenia; w przypadku wystąpienia opóźnienia w powiadomieniu - wyjasnienie przyczyn opóźnienia)

Czy poinformowano organy ścigania (data zawiadomienia)

Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy oraz sposób przekazania informacji wraz opisem zaleceń dla podmiotów danych

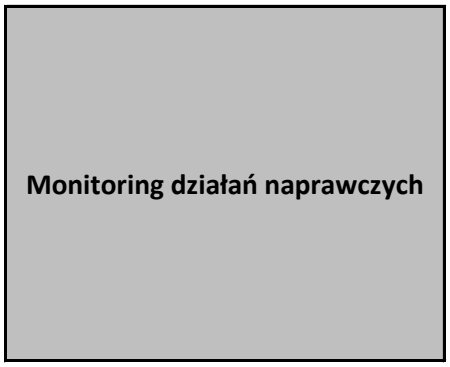
Monitoring działań naprawczych

TABELA FORM NARUSZENIA BEZPIECZEŃSTWA DANYCH

Inspektor ochrony danych (IOD)	kontakt@dpo24.pl
Administrator systemów informatycznych (ASI)	

Formy naruszeń	**Przykład naruszeń**	**Sposoby postępowania**
W zakresie wiedzy		
Ujawnienie sposobu działania oprogramowania komputerowego lub systemu informatycznego (w szczególności ich zabezpieczeń) osobom nieuprawnionym.	Ujawnienie osobie podającej się za serwisanta komputerowego (bez sprawdzenia, czy rzeczywiście nim jest) informacji o wykorzystywanej wersji programu antywirusowego.	Należy natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Należy powiadomić o zaistniałej sytuacji ASI. Po konsultacji z ASI oraz potwierdzeniu, że istnieje ryzyko naruszenia, należy wypełnić formularz „Zgłoszenie naruszenia do IOD" i przekazać go inspektorowi ochrony danych.
Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej (w szczególności ich zabezpieczeń) osobom nieuprawnionym.	Rozmowa w publicznym miejscu o sposobie rozbrojenia systemu alarmowego.	
Dopuszczenie lub stworzenie warunków umożliwiających osobie nieuprawnionej pozyskanie wiedzy na temat sposobu działania oprogramowania komputerowego lub systemu informatycznego (np. udostępnienie dokumentacji, umożliwienie dostępu do serwerowni)	Wpuszczenie do serwerowni osoby podającej się za serwisanta (bez zweryfikowania, czy rzeczywiście nim jest).	
W zakresie sprzętu i oprogramowania		
Dopuszczenie do korzystania z oprogramowania komputerowego lub sprzętu umożliwiającego dostęp do danych osobowych przez osoby inne niż osoba, której został przydzielony indywidualny login.	Korzystanie przez klienta z komputera pracownika, w sytuacji kiedy pracownik tymczasowo opuścił gabinet i zostawił w nim klienta samego.	Należy wezwać osobę nieuprawnioną do opuszczenia stanowiska. W porozumieniu z ASI należy ustalić, jakie czynności zostały wykonane przez osoby nieuprawnione.

		Należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w widocznym miejscu, zapisanego loginu lub hasła do systemu IT.	Login i hasło do systemu IT, zapisane na żółtej karteczce i przyklejone do monitora, ściany lub kontuaru w sposób umożliwiający osobom postronnym (np. osobom czekającym przy ladzie lub pracownikom serwisu sprzątającego) swobodny dostęp do tej informacji	Należy natychmiast usunąć zapisane login lub hasło z miejsca, w którym się znajdowały Należy powiadomić ASI i w porozumieniu z nim dokonać zmiany hasła. W razie podejrzenia, że z systemu IT korzystała osoba nieupoważniona, należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Samodzielne instalowanie jakiegokolwiek oprogramowania komputerowego lub pobieranie plików audio, wideo itp.	Pobieranie plików MP3 ze strony internetowej rozprowadzającej złośliwe oprogramowanie (np. wirusy).	Należy pouczyć osobę dokonującą wskazanych czynności o konieczności zaprzestania tego rodzaju działań. Należy powiadomić ASI. W razie stwierdzenia przez ASI, że w związku z nieuprawnioną instalacją oprogramowania lub pobraniem plików mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Modyfikowanie parametrów systemu Informatycznego lub oprogramowania komputerowego bez wiedzy i zgody ASI.	Wyłączenie programu antywirusowego.	Należy pouczyć osobę dokonującą wskazanej czynności o konieczności zaprzestania tego rodzaju działań. Należy wezwać ASI w celu przywrócenia pierwotnych parametrów.

		W razie stwierdzenia przez ASI, że w związku z modyfikacją parametrów mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD" i przekazać go inspektorowi ochrony danych.
Ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w systemie informatycznym lub uprawnienia poszerzone w stosunku do normalnej sytuacji.	Brak możliwości zarejestrowania nowej osoby w systemie IT	Należy wezwać ASI w celu przywrócenia pierwotnych uprawnień. W razie stwierdzenia przez ASI, że w związku ze zmianą uprawnień mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD" i przekazać go inspektorowi ochrony danych.
Brak możliwości uruchomienia oprogramowania komputerowego lub brak możliwości zalogowania się do systemu.	Brak możliwości zalogowania się do systemu Windows.	Należy powstrzymać się od dalszego użytkowania komputera. Należy powiadomić ASI. W razie stwierdzenia przez ASI, że w związku z brakiem możliwości uruchomienia oprogramowania lub zalogowania się mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD" i przekazać go inspektorowi ochrony danych.
Wygląd interfejsu oprogramowania komputerowego odbiegający od standardowego, znanego użytkownikowi.	Brak możliwości podglądu karty osoby w systemie informatycznym.	Należy powstrzymać się od dalszego użytkowania oprogramowania komputerowego. Należy powiadomić ASI. W razie stwierdzenia przez ASI, że zmiana wyglądu interfejsu może być skutkiem naruszenia ochrony danych osobowych, należy wypełnić formularz

		„Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Błędy w funkcjonowaniu systemu informatycznego (np. komunikaty informujące o niespójności i błędach w danych, brak dostępu do standardowych funkcji oprogramowania komputerowego, nieprawidłowości w wykonywanych operacjach).	Wyświetlenie na ekranie komputera informacji o uszkodzeniu bazy danych.	Należy powstrzymać się od dalszego użytkowania komputera. Należy powiadomić ASI. W razie stwierdzenia przez ASI, że błąd w funkcjonowaniu systemu może być skutkiem naruszenia ochrony danych osobowych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Instalowanie i odczytywanie nośników informacji przed sprawdzeniem ich programem antywirusowym	Umieszczenie w komputerze pendrive’a lub płyty otrzymanej od klienta bez wcześniejszego sprawdzenia nośnika za pomocą programu antywirusowego	Należy pouczyć osobę dokonującą wskazanej czynności o szkodliwości takiego działania. Należy wezwać ASI w celu sprawdzenia sprzętu lub systemu pod kątem złośliwego oprogramowania. W razie stwierdzenia przez ASI, że doszło do zainfekowania sprzętu lub systemu IT złośliwym oprogramowaniem, należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Utrata kontroli nad nośnikiem informacji, na którym zapisane są dane osobowe (np. zgubienie lub kradzież).	Zgubienie pendrive’a, na który wykonywana jest codziennie kopia zapasowa serwera.	Należy podjąć próbę odzyskania nośnika informacji. Należy powiadomić ASI. Należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Utrata kontroli nad sprzętem komputerowym, na którego dysku twardym przechowywane są dane osobowe (np. zgubienie lub kradzież).	Kradzież laptopa z działu kadr.	Należy podjąć próbę odzyskania sprzętu. Należy powiadomić ASI.

		Należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
W zakresie dokumentów i obrazów zawierających dane osobowe		
Przechowywanie dokumentów zawierających dane osobowe w sposób, który nie zapewnia właściwego zabezpieczenia przed dostępem osób nieuprawnionych.	Przechowywanie dokumentacji (np. umów) w stojącej na korytarzu szafie, która nie jest zamykana na klucz.	Należy wprowadzić odpowiednie zabezpieczenia. W razie stwierdzenia, że w związku z niewłaściwym przechowywaniem dokumentów doszło do naruszenia ochrony danych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Wyrzucanie dokumentów zawierających dane osobowe, niezniszczonych w stopniu uniemożliwiającym odczyt tych danych osobowych lub stwierdzenie, że w koszu znajduje się taki dokument.	Wyrzucenie do kosza na śmieci zawierającej błędy umowy.	Należy zabezpieczyć niewłaściwie zniszczone dokumenty i zniszczyć je w sposób trwały, uniemożliwiający ich odczytanie (np. za pomocą niszczarki).
Utrata kontroli nad dokumentacją papierową zawierającą dane osobowe (np. nieprawidłowe udostępnienie, zgubienie lub kradzież).	Zgubienie dokumentacji zawierającej dane osobowe, wykorzystywane przez pracownika w trakcie podróży służbowej.	Należy podjąć próbę odzyskania dokumentacji. Należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Dopuszczanie do kopiowania dokumentów zawierających dane osobowe i utraty kontroli nad kopią	Wysłanie pocztą (na adres klienta A) dokumentów dotyczących klienta B.	Należy zaprzestać kopiowania. Należy podjąć próbę odzyskania i zabezpieczenia wykonanej kopii. Należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Sporządzanie kopii danych osobowych na nośnikach informacji w sytuacjach nieprzewidzianych wewnętrznymi procedurami	Samodzielne wykonywanie przez pracownika kopii zapasowych plików bez konsultacji z informatykiem	Należy zaprzestać kopiowania danych osobowych na nośnik informacji. Należy zabezpieczyć wykonaną kopię i powiadomić ASI.

		W razie stwierdzenia, że w związku z wykonaniem nieautoryzowanej kopii danych doszło do naruszenia ochrony danych osobowych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD" i przekazać go inspektorowi ochrony danych.
Przesłanie wiadomości mailowej, zawierającej dane osobowe, do nieprawidłowego adresata (do podmiotu lub osoby nieuprawnionej do przetwarzania tych danych) lub wysłanie wiadomości do wielu adresatów w polu DO lub DW.	Wysłanie odpowiedzi na pismo klienta A na adres e-mail, podany przez klienta B.	Należy skontaktować się z osobą do której omyłkowo dotarła wiadomość mailowa, poinformować o zaistniałym zdarzeniu i zobowiązać do niezwłocznego usunięcia wiadomości mailowej. Należy powiadomić ASI. Należy wypełnić formularz „Zgłoszenie naruszenia do IOD" i przekazać go inspektorowi ochrony danych.
W zakresie obszaru, w którym przetwarzane są dane osobowe oraz systemu informatycznego służącego do przetwarzania danych osobowych		
Ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych lub do szafek, w których przechowywane są dokumenty papierowe, nośniki informacji lub sprzęt komputerowy zawierający dane osobowe.	Zamek w drzwiach działu kadr lub księgowości noszący ślady ingerencji.	Należy powstrzymać się przed dokonywaniem jakichkolwiek czynności mogących zatrzeć ślady włamania (np. odciski palców). Należy powiadomić odpowiednie służby (np. policję). Należy wypełnić formularz „Zgłoszenie naruszenia do IOD" i przekazać go inspektorowi ochrony danych.
Wpuszczanie do pomieszczeń osób nieuprawnionych i dopuszczanie do ich kontaktu ze sprzętem komputerowym służącym do przetwarzania danych osobowych.	Wpuszczenie do serwerowni osoby podającej się za serwisanta (bez zweryfikowania, czy rzeczywiście nim jest) lub umożliwienie dostępu do komputera osobie podającej się za pracownika firmy informatycznej bez wcześniejszego sprawdzenia tożsamości takiej osoby.	Należy wezwać osoby nieuprawnione do zaprzestania kontaktu ze sprzętem komputerowym. Należy podjąć próbę ustalenia tożsamości tych osób. W razie stwierdzenia, że działania osób nieuprawnionych mogły doprowadzić do naruszenia ochrony danych osobowych, należy wypełnić formularz

		„Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek innych manipulacji.	Zezwolenie osobie podającej się za pracownika firmy informatycznej (bez sprawdzenia, czy jest im rzeczywiście) podłączenie dysku do komputera w rejestracji.	Należy wezwać osoby dokonujące wskazanych czynności do ich zaprzestania. Należy podjąć próbę ustalenia tożsamości tych osób. W razie stwierdzenia, że działania osób nieuprawnionych mogły doprowadzić do naruszenia ochrony danych osobowych, należy wypełnić formularz „Zgłoszenie naruszenia do IOD” i przekazać go inspektorowi ochrony danych.

UPOWAŻNIENIE
do przetwarzania danych osobowych

Burmistrz Miasta Sierpca, jako administrator danych osobowych (**Administrator**), niniejszym upoważnia:

Imię i nazwisko	
Stanowisko	

do przetwarzania danych osobowych w zakresie zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania, archiwizowania oraz usuwania danych osobowych w związku z zajmowanym stanowiskiem.

Upoważnienie zostaje udzielone na okres od dnia _____ r. do odwołania lub zakończenia świadczenia pracy bądź usług na rzecz Administratora.

_____
(data i podpis Administratora[1])

Niniejszym oświadczam, że zapoznałem/zapoznałam* się z treścią obowiązujących u Administratora regulacji dotyczących ochrony danych osobowych, w tym polityki bezpieczeństwa i zobowiązuję się do ich przestrzegania. Zobowiązuję się zachować w tajemnicy dane osobowe, do których będę mieć dostęp oraz sposoby ich zabezpieczenia, także po wygaśnięciu niniejszego upoważnienia. Przyjmuję do wiadomości, że udostępnienie danych osobowych lub umożliwienie dostępu do tych danych osobom nieupoważnionym może podlegać odpowiedzialności, szczególnie odpowiedzialności karnej, zgodnie z powszechnie obowiązującymi przepisami.

_____
(data i podpis osoby upoważnionej[2])

[1] Osoba uprawniona do reprezentowania podmiotu.
[2] Osobą upoważnioną jest osoba współpracująca z Administratorem, niezależnie od podstawy współpracy.

Wymagania dotyczące umów powierzenia

Zgodnie z obowiązującą Polityką Bezpieczeństwa w sytuacji, gdy konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych, powinna ona być zawarta na wzorze, który stanowi załącznik do Polityki Bezpieczeństwa.

Jeżeli jednak zawarcie umowy na wzorze ADO nie jest możliwe, należy dokonać weryfikacji umowy przekazanej przez kontrahenta ADO pod kątem sprawdzenia, czy spełnia ona wymogi wskazane w art. 28 RODO.

W treści umowy powierzenia musi wynikać, że podmiot przetwarzający:

1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3) podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO;
5) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
7) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
8) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Umowa powierzenia

zawarta w … dnia … pomiędzy:

… z siedzibą w … przy ul. …, KRS…, NIP: …, w dalszej części umowy zwaną „Administratorem”

reprezentowaną przez

……

……

a

… z siedzibą w … przy ul. …, KRS …, NIP: …, w dalszej części umowy zwaną „Podmiotem przetwarzającym”

reprezentowaną przez

……

……

§ 1
Postanowienia ogólne

1. Administrator, na podstawie art. 28 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 (zwanego dalej „RODO”) powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie i na zasadach określonych w niniejszej umowie.
2. Powierzenie następuje w celu prawidłowej realizacji umowy o _____ z dnia __.__.2018 r., zwanej dalej „Umową główną”. Okres powierzenia danych osobowych jest równy okresowi obowiązywania Umowy głównej.
3. Powierzenie obejmuje kategorie osób, których dane dotyczą oraz rodzaje danych osobowych wynikające z Umowy Głównej.
4. Podmiot przetwarzający może wykorzystywać dane osobowe, o których mowa w ust. 3 powyżej:
    a. wyłącznie w celach związanych z realizacją usług, świadczonych na podstawie Umowy głównej,
    b. wyłącznie w zakresie wskazanym w ust. 3 powyżej.

§ 2
Obowiązki Stron

1. Podmiot przetwarzający, w celu zabezpieczenia powierzonych do przetwarzania danych osobowych, zobowiązuje się podjąć środki techniczne i organizacyjne, by przetwarzanie spełniało wymogi RODO oraz niniejszej Umowy i chroniło prawa osób, których dane dotyczą. W szczególności obejmuje to środki, o których mowa w artykułach 24 oraz 32 RODO, w szczególności:
    a. wdrożenie odpowiednich polityk ochrony danych,

b. wdrożenie środków technicznych i organizacyjnych aby zabezpieczenie danych pozwalało spełnić wymagania RODO,
c. dokumentowanie spełnienia wymagań dotyczących zabezpieczeń w celu wykazania zgodności z RODO.

2. Podmiot przetwarzający zobowiązuje się do zapewnienia, by osoby mające po stronie Podmiotu przetwarzającego dostęp do powierzonych danych osobowych:
   a. były upoważnione do ich przetwarzania przez Podmiot przetwarzający,
   b. zachowały je w tajemnicy zarówno w okresie współpracy z Podmiotem przetwarzającym, jak i po jej zakończeniu.
3. Podmiot przetwarzający wspiera Administratora – w zakresie uzgodnionym przez Strony – w realizacji:
   a. obowiązku odpowiadania na żądania osób, których dane osobowe są wykorzystywane w ramach powierzenia, w zakresie ich praw określonych w rozdziale III RODO,
   b. obowiązków określonych w art. 32–36 RODO.
4. Podmiot przetwarzający niezwłocznie, jednak nie później niż w ciągu 24 godzin, informuje Administratora o stwierdzonych naruszeniach danych osobowych, wykorzystywanych w ramach powierzenia. Informacja dla Administratora zawiera:
   a. charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych Podmiotu przetwarzającego lub oznaczenie innej osoby po stronie Podmiotu przetwarzającego, od której można uzyskać więcej informacji;
   c. możliwe konsekwencje naruszenia ochrony danych osobowych;
   d. opis środków zastosowanych lub proponowanych przez Podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym – w stosownych przypadkach – środki, których celem jest zminimalizowanie ewentualnych negatywnych skutków naruszenia.
5. Podmiot przetwarzający rejestruje kategorie czynności przetwarzania zgodnie z art. 30 RODO.
6. Podmiot przetwarzający wyznacza u siebie inspektora ochrony danych (IOD) w sytuacji, w której wymagają tego przepisy art. 37 RODO.

§ 3

Dalsze powierzenie danych osobowych

1. Administrator zezwala Podmiotowi przetwarzającemu na powierzanie danych osobowych innym podmiotom przetwarzającym w zakresie niezbędnym do realizacji Umowy Głównej.
2. Podmiot przetwarzający informuje Administratora o wszelkich zmianach dotyczących dodania lub zastąpienia podmiotów, o których mowa w ust. 1 powyżej. Administrator zastrzega sobie prawo wyrażenia sprzeciwu wobec zmian, o których mowa w zdaniu pierwszym. Na wyrażenie zgody lub sprzeciwu Administrator ma 3 dni od dnia powiadomienia. Akceptacja jest dokonywana drogą elektroniczną. W przypadku braku odpowiedzi w terminie 3 dni od dnia powiadomienia uznaje się, że Administrator nie wyraził sprzeciwu wobec dalszego powierzenia przetwarzania danych osobowych.
3. Podmiot przetwarzający gwarantuje, iż inny podmiot przetwarzający, z którego usług zamierza korzystać przy przetwarzaniu danych osobowych, będzie dawał te same gwarancje i spełniał obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej umowie, w

szczególności daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

4. Podmiot przetwarzający ponosi wobec Administratora pełną odpowiedzialność za niewywiązanie się innego podmiotu przetwarzającego, któremu powierzył przetwarzanie danych osobowych, ze spoczywających na nim obowiązków ochrony danych. W takim przypadku Administrator ma prawo żądać natychmiastowego zaprzestania korzystania przez Podmiot przetwarzający z usług tego podmiotu w procesie przetwarzania danych osobowych.

§ 4

Współpraca Stron

1. W czasie trwania umowy, Administrator jest uprawniony do żądania od Podmiotu przetwarzającego informacji związanych z przetwarzaniem powierzonych danych osobowych, a Podmiot przetwarzający zobowiązany jest udzielić takich informacji niezwłocznie. Na żądanie Administratora Podmiot przetwarzający udzieli odpowiedzi na piśmie.
2. Podmiot przetwarzający niezwłocznie zawiadomi Administratora o zgłoszeniu przez jakąkolwiek osobę lub organ władzy publicznej uwag, zastrzeżeń, wniosków lub o wszczęciu postępowania w odniesieniu do danych osobowych powierzonych na podstawie niniejszej umowy, w szczególności wszelkich czynnościach kontrolnych podjętych wobec niego przez organ nadzorczy oraz o wynikach takiej kontroli, jeżeli jej zakresem objęto dane osobowe powierzone Podmiotowi przetwarzającemu na podstawie niniejszej umowy.
3. Administrator lub audytor upoważniony przez Administratora może przeprowadzać u Podmiotu przetwarzającego audyty, w tym inspekcje, w celu ustalenia, czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej umowy.
4. Audyt może polegać na:
    a. udostępnieniu przez Podmiot przetwarzający dokumentów lub informacji dotyczących przetwarzania powierzonych danych osobowych lub na
    b. czynnościach kontrolnych prowadzonych w miejscu przetwarzania powierzonych danych osobowych przez Podmiot przetwarzający
5. Czynności kontrolne mogą być prowadzone w godzinach 10:00 – 16:00 w dni robocze (rozumiane jako dni od poniedziałku do piątku, z wyłączeniem sobót, niedziel i dni ustawowo wolnych od pracy), po uprzednim pisemnym lub elektronicznym poinformowaniu Podmiotu przetwarzającego o terminie czynności i ich zakresie, co najmniej na 10 dni roboczych przed rozpoczęciem czynności kontrolnych.
6. Czynności kontrolne mogą polegać w szczególności na:
    a. sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
    b. odebraniu wyjaśnień osób przetwarzających powierzone dane osobowe;
    c. sporządzeniu kopii otrzymanych dokumentów;
    d. sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania powierzonych danych osobowych;
    e. sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania powierzonych danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu
7. Koszty audytu ponosi Administrator.

8. Ze sporządzonego audytu Administrator sporządza raport i przekazuje jego kopię Podmiotowi przetwarzającemu. W treści raportu umieszcza się w szczególności działania lub zaniechania Podmiotu przetwarzającego, skutkujące naruszeniem niniejszej umowy lub powszechnie obowiązujących przepisów dotyczących ochrony danych osobowych, w tym RODO.
9. Podmiot przetwarzający, w terminie uzgodnionym z Administratorem, usuwa naruszenia, wskazane w raporcie, o którym mowa w ust. 6 powyżej.

§ 5
Zakończenie współpracy

1. W terminie do 14 dni po zakończeniu współpracy na gruncie Umowy głównej, Podmiot przetwarzający - zależnie od decyzji Administratora – protokolarnie usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, a jeden z podpisanych egzemplarzy protokołu przekazuje Administratorowi, chyba że przepisy powszechnie obowiązujące nakazują przechowywanie danych osobowych.
2. Podmiot przetwarzający odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z niniejszą umową przetwarzania przez Podmiot przetwarzający danych osobowych lub nieprzestrzegania przepisów obowiązującego prawa w zakresie ochrony danych osobowych.
3. W przypadkach, o których mowa w ust. 2 powyżej, Podmiot przetwarzający zobowiązuje się do zapłaty odszkodowania na zasadach ogólnych.

§ 6
Postanowienia końcowe

1. Strony dopuszczają zmianę niniejszej umowy w formie elektronicznej, w szczególności poprzez wymianę korespondencji e-mailowej.
2. Osobami do kontaktu w sprawach dotyczących niniejszej umowy, w tym zawiadomień, o których mowa w § 2 ust. 3-4, § 3 ust. 2, § 4 ust. 5 Umowy, są:
    a. po stronie Administratora: _____
    b. po stronie Podmiotu przetwarzającego: _____
3. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy RODO oraz Kodeksu cywilnego.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
5. Umowa wchodzi w życie z dniem podpisania i zastępuje wszelkie obowiązujące przed tą datą umowy powierzenia przetwarzania danych osobowych oraz postanowienia umowne dotyczące powierzenia przetwarzania danych osobowych, na mocy których Administrator powierzał Podmiotowi przetwarzającemu przetwarzanie danych osobowych w związku z realizacją Umowy głównej.

_____	_____
Administrator	Podmiot przetwarzający

Zabezpieczenia fizyczne

Spis treści

1. Dostęp do budynku ADO

Po godzinach pracy Urzędu Miejskiego w Sierpcu, gdy w budynku nie przebywają żadne osoby z personelu ADO, konieczne jest zabezpieczenie budynku przed dostępem osób nieupoważnionych. Zabezpieczenie budynku może nastąpić w szczególności poprzez:

1. zamknięcie wszystkich wejść do budynku (głównych, bocznych, dla pracowników itp.) na klucz i zabieranie tych kluczy przez wyznaczoną osobę lub osoby,
2. montaż systemu alarmowego (czujek ruchu),
3. montaż systemu alarmowego automatycznie informującego o uruchomieniu czujki wybraną osobę z personelu ADO i firmę ochroniarską, z którą ADO współpracuje.

1.1 System alarmowy (czujki ruchu)

1. W przypadku wykorzystywania przez ADO systemu alarmowego, możliwość uruchomienia/wyłączenia systemu alarmowego powinna mieć jak najmniejsza liczba osób.
2. W przypadku zakończenia współpracy ADO z osobą znającą kod do alarmu, należy dokonać zmiany kodu (jeżeli wszystkie osoby używały tego samego kodu) lub dezaktywacji kodu byłego pracownika (jeżeli były pracownik miał własny kod).
3. Czujki alarmu muszą być umieszczone w miejscach, przez które na teren placówki mogą dostać się osoby nieupoważnione. Czujki nie mogą być zasłaniane przez parawany, kartony stojące na szafach itp. przeszkody.

1.2 Okna

Okna znajdujące się na parterze lub w miejscach, do których mogą mieć łatwy dostęp osoby nieupoważnione, powinny zostać zabezpieczone np. poprzez:

1) montaż krat w oknach,
2) montaż rolet antywłamaniowych,
3) montaż folii antywłamaniowych.

2. Dostęp do pomieszczeń ADO

1. Wszystkie pomieszczenia, w których przechowuje się na stałe:
    a) papierową dokumentację zawierającą dane osobowe (np. umowy, akta osobowe pracowników itp.)
    lub
    b) urządzenia, z pomocą których przetwarza się dane osobowe (np. komputery, na których zainstalowano system IT zawierające dane klientów)
    powinny być zabezpieczone przez dostępem osób nieupoważnionych.
2. Zabezpieczenie pomieszczenia może nastąpić w szczególności poprzez:
    a) zamykanie pomieszczenia na klucz,
    b) zamykanie pomieszczenia w inny sposób (np. kartą dostępu),
    c) stałą obecność w pomieszczeniu osoby upoważnionej przez ADO (np. pracownika ochrony).
3. Osoba zamykająca pomieszczenie na klucz nie może zostawiać klucza w zamku – musi zabrać go ze sobą lub umieścić w bezpiecznym miejscu (np. na recepcji).
4. Po godzinach pracy klucze do pomieszczeń powinny być składowane w jednym miejscu, do którego dostęp będą miały jedynie osoby, którym taki dostęp jest potrzebny (np. pracownicy, osoby sprzątające budynek). Takim miejscem może być np. klucznik umieszczony na recepcji.
5. Osoby nieupoważnione przebywają w pomieszczeniach, o których mowa w ust. 1, jedynie w obecności osób upoważnionych przez ADO (np. klient przebywa w gabinecie wyłącznie w obecności pracownika zajmującego ten gabinet). Pozostawienie osoby nieupoważnionej samej w pomieszczeniu, w którym przechowywane są (okresowo lub na stałe) dokumenty zawierające dane osobowe, jest niedopuszczalne. Należy wówczas grzecznie poprosić osobę nieupoważnioną o wyjście na korytarz, zamknąć drzwi do pomieszczenia i zabrać klucz ze sobą.
6. Ust. 5 powyżej nie dotyczy osób, które mają prawo przebywać w pomieszczeniach zawierających dane osobowe za wiedzą i zgodą ADO (np. osób sprzątających, wykonujących swoje obowiązki po godzinach pracy biura).

3. Sprzątanie pomieszczeń ADO

1. Osoby należące do personelu sprzątającego do wykonywania swoich obowiązków nie potrzebują dostępu do danych osobowych, przetwarzanych w formie papierowej lub elektronicznej.
2. Sprzątanie powinno odbywać się:
    a) w godzinach pracy biura, pod nadzorem osoby z personelu ADO
    lub
    b) poza godzinami pracy biura, przy zachowaniu przez pracowników ADO zasady czystego biurka.
3. Osoby należące do personelu sprzątającego zobowiązują się do zachowania danych osobowych (na które ewentualnie mogłyby się natknąć w trakcie wykonywania swoich

obowiązków służbowych), jak i sposobu ich zabezpieczenia w tajemnicy. W tym celu ADO odbiera od tych osób oświadczenia o poufności, których wzór stanowi załącznik do Polityki Bezpieczeństwa.

4. Sposób przechowywania dokumentacji papierowej

1. Osoby zatrudnione przez ADO są zobowiązane do zachowania zasady czystego biurka: po godzinach pracy wszystkie dokumenty, zawierające dane osobowe, muszą być przechowywane w szafach, szafkach lub szufladach zamykanych na klucz.
2. Po zakończeniu pracy klucze do szaf, szafek lub szuflad muszą być przechowywane w miejscach dostępnych jedynie dla członków upoważnionego personelu ADO. Takim miejscem może być np. klucznik szyfrowany, do którego kod znają jedynie ww. upoważnione osoby.
3. Klucze do szaf, szafek lub szuflad nie mogą być przechowywane w tzw. miejscach wiadomych (za doniczkami, w puszkach, w szufladach itp. miejscach), ponieważ istnieje ryzyko przypadkowego lub celowego odnalezienia tych kluczy przez osoby nieupoważnione.
4. Dokumentacja zawierająca dane osobowe nie może być przechowywana w miejscach, do których swobodny dostęp mają osoby nieupoważnione (np. na otwartym regale stojącym na korytarzu, na kontuarze recepcji itp. miejscach).

5. Przenoszenie dokumentacji papierowej

1. W trakcie przewożenia dokumentacji zawierającej dane osobowe powinna ona być przechowywana w taki sposób, aby zminimalizować ryzyko jej utracenia, np. w wyniku kradzieży lub zgubienia. Dokumentacja nie powinna być przewożona luzem. Transport środkami transportu publicznego jest bardziej ryzykowny niż transport samochodowy z uwagi na niebezpieczeństwo kradzieży lub zagubienia, dlatego też ta pierwsza forma transportu powinna zostać ograniczona do minimum.
2. Dokumentacja wykorzystywana poza biurem powinna przez cały czas znajdować się pod opieką osoby przewożącej – nie powinna być pozostawiana w samochodzie, przechowalniach, szatniach itp. miejscach.

6. Dokumentacja archiwalna

6.1 Zalecenia ogólne

1. Miejsce przechowywania archiwalnej dokumentacji powinno być, w miarę możliwości ADO, dodatkowo zabezpieczone przed dostępem osób nieupoważnionych, np. poprzez:
    a) zamontowanie czujki ruchu,
    b) założenie drzwi antywłamaniowych,
    c) przeniesienie dokumentacji do zamykanej na klucz szafy metalowej (w przypadku, gdy nie ma w biurze oddzielnego pomieszczenia, przeznaczonego na dokumentację archiwalną).
2. Dokumentacja powinna być regularnie sprawdzana pod kątem ewentualnych infekcji, grzybów pleśniowych, niszczenia przez owady, gryzonie, wilgoć lub kurz.
3. Dokumentacja powinna być regularnie przeglądana w celu ustalenia, czy nie upłynął termin ustawowego jej przechowywania (przechowywanie dokumentacji archiwalnej dłużej niż wymagają tego przepisy może być rozpatrywane jako naruszenie zasad przetwarzania danych osobowych).
4. Dokumenty, w stosunku do których termin obowiązkowego przechowywania już minął, należy przeznaczyć do utylizacji, najlepiej korzystając z usług zewnętrznej firmy. Jeżeli taka utylizacja nastąpi:

   a) siłami własnymi – należy powołać komisję likwidacyjną oraz sporządzić protokół zniszczenia wraz z opisem niszczonej dokumentacji (wzór protokołu stanowi załącznik do Polityki Bezpieczeństwa),
   b) z pomocą zewnętrznej firmy – konieczne jest zawarcie z tą firmą umowy powierzenia przetwarzania danych osobowych.
5. W przypadku, gdyby np. na skutek zalania część dokumentacji uległa zniszczeniu, należy sporządzić notatkę opisującą:
   a) datę wystąpienia zniszczenia lub stwierdzenia zniszczenia przez personel placówki,
   b) opis przyczyny zniszczenia (np. podtopienie, zalanie, pożar),
   c) opis podjętych czynności: osuszanie i sortowanie dokumentacji, odtwarzanie treści uszkodzonej dokumentacji (o ile jest taka możliwość, np. gdy dane pracowników będą jednocześnie utrwalone w programie komputerowym).

6.2 Zalecenia dotyczące pomieszczenia pełniącego rolę archiwum

1. W pomieszczeniu pełniącym rolę archiwum należy, w miarę możliwości, utrzymywać parametry, które pozwolą na przechowywanie papierowej dokumentacji przez okres wymagany przepisami prawa:
   a) temperatura: 14°C-20°C (± 2°C wahania w ciągu 24 godzin),
   b) wilgotność względna: 45%-60% (± 5% wahania w ciągu 24 godzin).
2. Sprzątanie archiwum powinno odbywać się wyłącznie w obecności i pod nadzorem pracownika biura.
3. W przypadku, gdy w pomieszczeniu pełniącym funkcję archiwum biegną rury wodno-kanalizacyjne lub z innego względu istnieje ryzyko zalania pomieszczenia, dokumentacja nie może być umieszczana bezpośrednio na podłodze – półki, na których umieszczona jest dokumentacja, powinny znajdować się na wysokości przynajmniej kilku centymetrów nad podłogą (w celu zminimalizowania ewentualnych strat w razie zalania). Ponadto dokumentacja archiwalna nie powinna być przechowywana bezpośrednio pod wspomnianymi rurami.

7. Zabezpieczenie serwera

1. Serwer/komputer główny (jednostka centralna) nie powinien być wykorzystywany do codziennej pracy (np. odbierania poczty e-mail, przeglądania stron www).
2. Serwer/komputer główny powinien być, w miarę możliwości, przechowywany w wydzielonym pomieszczeniu, do którego dostęp będą miały wyłącznie osoby upoważnione (dobrą praktyką jest autoryzowanie dostępu np. poprzez wykorzystanie zamka kodowanego lub karty magnetycznej).
3. Pomieszczenie, w którym przechowywany jest serwer/komputer główny, musi być odpowiednio zabezpieczone pod względem technicznym i organizacyjnym.
4. W przypadku, gdy ADO dysponuje oddzielnym pomieszczeniem, pełniącym rolę serwerowni, powinna ona spełniać m.in. następujące wymogi:
   a) jeżeli w pomieszczeniu znajdują się okna
      - należy je zabezpieczyć kratami lub roletami antywłamaniowymi przed dostaniem się osób z zewnątrz,
      - należy je zabezpieczyć żaluzjami/roletami przed promieniami słonecznymi;
   b) pomieszczenie klimatyzowane (temperatura, wilgotność i wentylacja zgodnie ze specyfikacją producenta urządzenia);
   c) pomieszczenie powinno mieć odpowiednią instalację elektryczną (podzieloną na kilka faz), która wytrzyma duże obciążenie);

d) pomieszczenie powinno być wyposażone w UPS i filtry antyprzepięciowe, odpowiednie do obciążenia serwerów i innych urządzeń aktywnych;
e) pomieszczenie powinno być wyposażone gaśnicę odpowiednią do gaszenia sprzętu elektronicznego, na przykład gaśnicę GH-2x przeznaczoną do gaszenia czułych urządzeń elektronicznych i elektrycznych, niepozostawiającą zanieczyszczeń po środku gaśniczym;
f) wskazanym działaniem będzie również montaż czujek dymu;
g) serwery powinny być umieszczone w odpowiednich szafach, najlepiej obudowach typu RACK.

8. Niszczenie dokumentacji papierowej

1. Zbędna dokumentacja papierowa (np. błędne wydruki zawierające dane osobowe klientów lub dokumentacja, której ustawowy okres przechowywania minął) musi być niszczona w sposób uniemożliwiający identyfikację osoby, której dotyczyła.
2. Jeżeli dokumentacja jest niszczona w większej liczbie:
    a) na własną rękę – ADO powołuje komisję likwidacyjną oraz sporządza protokół zniszczenia wraz z opisem niszczonej dokumentacji (wzór protokołu stanowi załącznik do Polityki Bezpieczeństwa),
    b) z pomocą zewnętrznej firmy – konieczne jest zawarcie z tą firmą umowy powierzenia przetwarzania danych osobowych.
3. Niszczenie na własną rękę powinno odbywać się z pomocą niszczarek, spełniających minimum poziom P-3 normy DIN 66399 (szerokość ścinka ≤ 2 mm; powierzchnia ścinka ≤ 320 mm²).
4. ADO powinien zapewnić osobom zatrudnionym liczbę niszczarek gwarantującą, że zbędna dokumentacja będzie niszczona na bieżąco.

ZGŁOSZENIE NARUSZENIA/PODEJRZENIA NARUSZENIA BEZPIECZEŃSTWA DANYCH

Dane osoby zgłaszającej

Imię		Nazwisko	
Email		Nr telefonu	

Miejsce i data	Podpis osoby zgłaszającej

Dane naruszenia	Data	Godzina
Kiedy stwierdzono naruszenie? Kiedy dowiedzieli się Państwo o naruszeniu. Gdy dokładna data jest nieznana przybliżony czas.		
Kiedy faktycznie zaistniało naruszenie? Kiedy doszło do naruszenia? Jeżeli dokładna data nie jest znana - podać przybliżony czas.		
Kiedy naruszenie zostało usunięte? Proszę podać godzinę, jeżeli jest Państwu znana.		

Sposób stwierdzenia naruszenia Np. zgłoszenie osoby, której dane dotyczą/cykliczny przegląd logów systemów zgodnie z wdrożoną polityką bezpieczeństwa	

Charakter naruszenia

Wypełnia osoba zatrudniona u Administratora, która zauważyła działanie lub zachowanie, mogące prowadzić do naruszenia bezpieczeństwa danych osobowych.

- ☐ Naruszenie poufności danych (nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych)
- ☐ Naruszenie integralności danych (wprowadzenie nieuprawnionych zmian podczas odczytu, transmisji lub przechowywania)
- ☐ Naruszenie dostępności danych (brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną)

Na czym polegało naruszenie?

Wypełnia osoba zatrudniona u Administratora, która zauważyła działanie lub zachowanie, mogące prowadzić do naruszenia bezpieczeństwa danych osobowych.

- ☐ Zgubienie lub kradzież nośnika/urządzenia
- ☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
- ☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej nadawcy
- ☐ Nieuprawnione uzyskanie dostępu do informacji
- ☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
- ☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych
- ☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)
- ☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie
- ☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
- ☐ Niezamierzona publikacja
- ☐ Dane osobowe wysłane do niewłaściwego odbiorcy
- ☐ Ujawnienie danych niewłaściwej osoby
- ☐ Ustne ujawnienie danych osobowych

Opis słowny naruszenia

Kategorie danych osobowych

Bez podawania danych konkretnych osób, których dotyczy naruszenie

Wymień szczegółowo, jakie kategorie danych osobowych uległy naruszeniu (np. imiona, nazwiska, adresy e-mail)

Dane podstawowe

- ☐ Dane identyfikacyjne (imię, nazwisko, nr dowodu osobistego, adres IP)
- ☐ Krajowy numer identyfikacyjny (np. PESEL, SSN)

- ☐ Dane kontaktowe (np. e-mail, numer telefonu, adres korespondencyjny)
- ☐ Dane ekonomiczne i finansowe (np. historie transakcji, wnioski o wsparcie finansowe)
- ☐ Oficjalne dokumenty (np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu)
- ☐ Dane lokalizacyjne (np. GPS, dane o przemieszczaniu się, miejsce zamieszkania)
- ☐ inne: _____

Dane szczególnej kategorii

- ☐ dane o pochodzeniu rasowym lub etnicznym
- ☐ dane o poglądach politycznych
- ☐ dane o przekonaniach religijnych lub światopoglądowych
- ☐ dane o przynależności do związków zawodowych
- ☐ dane dotyczące seksualności lub orientacji seksualnej
- ☐ dane dotyczące zdrowia
- ☐ dane genetyczne
- ☐ dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

Dane, o których mowa w art. 10 RODO

- ☐ dane dotyczące wyroków skazujących
- ☐ dane dotyczące czynów zabronionych
- ☐ inne:

Liczba osób, których mogło dotyczyć naruszenie	

Kategoria osób

np. klienci, pracownicy, kontrahenci, etc

Środki bezpieczeństwa

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez administratora przed naruszeniem wobec danych, będących przedmiotem naruszenia

Możliwe konsekwencje

USZCZERBEK FIZYCZNY, MAJĄTKOWY, NIEMAJĄTKOWY LUB INNE ZNACZĄCEKONSEKWENCJE DLA OSOBY, KTÓREJ DANE DOTYCZĄ (np. kradzież tożsamości, strata finansowa, naruszenie dobrego imienia)

Środki zaradcze

Opis zastosowanych środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia)