Załącznik nr 1 do Polityki Ochrony Danych

Wykaz osób zapoznanych z Polityką Ochrony Danych

L.p.	Imię i nazwisko pracownika	Podpis
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		

Załącznik nr 2 do Polityki Ochrony Danych

Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnie rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. I w celach:

.....

.....

(data, podpis)

Administratorem danych osobowych przetwarzanych ww. celach jest Gmina Krokowa, ul. Żarnowiecka 29 84 - 110 Krokowa. Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnie rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 osobie, której dane dotyczą przysługuje prawo:

- Żądania dostępu do danych osobowych;
- Sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych;
- Wniesienia sprzeciwu;
- Cofnięcia zgody w każdym momencie, jednak bez wpływu na zgodność z prawem przetwarzania danych osobowych, którego dokonano na podstawie zgody przed jej cofnięciem;
- Wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Zapoznałam/-em się z treścią powyższego.

.....

(data, podpis)

Załącznik nr 3 do Polityki Ochrony Danych

Wzór odwołania zgody na przetwarzanie danych osobowych

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnie rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. I odwołuję wyrażoną przeze mnie zgodę na przetwarzanie danych osobowych w celach

.....
.....

przez

.....
.....

.....
(data, podpis)

Załącznik nr 4 do Polityki Ochrony Danych

Na podstawie art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 informujemy, iż:

1.Administratorem Pani/Pana danych osobowych jest Gmina Krokowa, ul. Żarnowiecka 29, 84-110 Krokowa

2.W sprawach z zakresu ochrony danych osobowych mogą Państwo kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: iodo@krokowa.pl

3.Dane osobowe będą przetwarzane w celu realizacji obowiązków prawnych ciążących na Administratorze.

4.Dane osobowe będą przetwarzane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów przechowywania określonych w przepisach odrębnych, w tym przepisów archiwalnych.

5.Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia.

6.Odbiorcą Pani/Pana danych będą podmioty upoważnione na mocy przepisów prawa.

7.Osoba, której dane dotyczą ma prawo do:

- dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania oraz do przenoszenia swoich danych, a także - w przypadkach przewidzianych prawem - prawo do usunięcia danych i prawo do wniesienia sprzeciwu wobec przetwarzania Państwa danych.

- wniesienia skargi do organu nadzorczego w przypadku, gdy przetwarzanie danych odbywa się z naruszeniem przepisów powyższego rozporządzenia tj. Prezesa Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa

Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 ogólnego rozporządzenia o ochronie danych osobowych.

Załącznik nr 5 do Polityki Ochrony Danych

Procedura realizacji uprawnienia: prawo dostępu do danych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa dostępu do swoich danych przetwarzanych przez Administratora.

Każdej osobie fizycznej przysługuje prawo do uzyskania wyczerpujących informacji od Administratora, w postaci potwierdzenia, czy dane są faktycznie przetwarzane.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba fizyczna, której dane są przetwarzane ma prawo do uzyskania informacji o:
1) celach, w jakich przetwarzane są dane osobowe;
2) kategoriach danych osobowych, które podlegają przetwarzaniu;

3) odbiorcach lub kategoriach odbiorców;

4) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalania okresu przechowywania danych;

5) prawie do żądania sprostowania swoich danych osobowych;

6) prawie do usunięcia lub ograniczenia przetwarzania danych osobowych;

7) prawie do wniesienia sprzeciwu wobec konkretnego przetwarzania swoich danych;

8) prawie do wniesienia skargi do organu nadzorczego, na przetwarzanie swoich danych, jeśli są one przetwarzane niezgodnie z obowiązującymi przepisami;

9) w sytuacji, gdy dane osobowe nie zostały zebrane od osoby, której one dotyczą – wszelkich dostępnych informacje o źródle, z którego administrator pozyskał te dane

10) zautomatyzowanym podejmowaniu decyzji, jeżeli Administrator realizuje wobec konkretnej osoby fizycznej taki sposób przetwarzania, w tym informacji o profilowaniu (art. 22 ust. 1 i 4 RODO).

3. Realizacja uprawnienia dostępu do danych

Osoba fizyczna otrzymuje dostęp do swoich danych osobowych poprzez uzyskanie kopii przetwarzanych danych osobowych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Pierwsza kopia i jej przekazanie odbywa się bezpłatnie, lecz za wszelkie kolejne kopie, o które zwróci się podmiot danych, Administrator będzie miał prawo pobrać „opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych" (art. 15 ust. 3 RODO) związanych z jej wytworzeniem (według stawek obowiązujących u Administratora).

Umożliwienie wglądu do danych konkretnej osobie fizycznej nie może powodować naruszenia praw innych osób lub też tajemnic prawnie chronionych. Uzyskując wgląd do

swoich danych osoba fizyczna nie może mieć nieuzasadnionego dostępu do danych innych osób fizycznych.

W przypadku, gdy przetwarzana jest duża ilość informacji o osobie, która chce skorzystać z prawa dostępu do swoich danych, Administrator kieruje do tej osoby zadanie sprecyzowania do jakich konkretnie danych lub też informacji o czynnościach przetwarzania jej danych chciałaby ona uzyskać dostęp.

Terminy na udzielenie odpowiedzi na żądanie:

1. Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie miesiąca od otrzymania tego żądania.
2. Jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi

o kolejne 2 miesiące, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

3. W przypadku, gdy administrator nie zamierza udzielić odpowiedzi oraz podjęcia działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sadu.

Wzór odpowiedzi na skierowany wniosek:

Na podstawie art. 15 ust. 1 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, Administrator potwierdza, że Pana/Pani dane osobowe są przetwarzane i jednocześnie informuje, że:

1) celem przetwarzania Pani/Pana danych osobowych jest ...;

2) (administrator) przetwarza Pani/Pana dane osobowe w zakresie ... (należy wskazać kategorię danych osobowych);

3) dane osobowe będą ujawniane ... (należy wskazać odbiorcę lub kategorie odbiorców);

4) dane osobowe będą przechowywane przez okres ...;

5) przysługuje Panu/Pani prawo do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, a także prawo do wniesienia sprzeciwu oraz skargi do organu nadzorczego;

6) (administrator) uzyskał Pani/Pana dane osobowe z ... (należy wskazać źródło, o ile dane nie zostały pozyskane od osoby, której dotyczą);

7) (należy dodać informacje dotyczące zautomatyzowanego podejmowania decyzji, w tym profilowania, o ile znajduje to zastosowanie).

_____

(data, podpis)

Załącznik nr 6 do Polityki Ochrony Danych

Procedura: prawo do sprostowania danych osobowych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej do sprostowania/uzupełnienia swoich danych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Jeżeli osoba fizyczna zażąda uzupełnienia katalogu dotyczących go danych osobowych o te, które nie są niezbędne Administratorowi do działania, to taki wniosek nie musi zostać pozytywnie rozpatrzony przez Administratora dla osoby, której dane dotyczą.

3. Procedura rozpatrywania żądań o sprostowanie danych osobowych

Komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i dostępnej formie.

Osoba składająca wniosek o sprostowanie/uzupełnienie danych osobowych oświadcza, że jest osobą możliwą do zidentyfikowania, na podstawie dobrowolnie podanych danych osobowych, umożliwiających jej jednoznaczną identyfikację.

W przypadku, gdy Administrator nie jest w stanie zidentyfikować osoby składającej wniosek o sprostowanie/uzupełnienie danych osobowych, ma prawo na podstawie obowiązujących przepisów prawa odmówić rozpatrzenia żądania, uprzednio podejmując wszelkie możliwe środki w celu zidentyfikowania osoby, która z nim wystąpiła.

Każdej osobie fizycznej przysługuje jednakowe prawo do niezwłocznego sprostowania/uzupełnienia dotyczących go danych osobowych, które są nieprawidłowe lub nieaktualne. Uwzględniając cele przetwarzania, osoba, której dane dotyczą ma prawo do żądania od Administratora uzupełnienia niekompletnych danych osobowych, poprzez przedstawienie odpowiedniego oświadczenia Administratorowi.

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) Administratorowi przysługują dwa uprawnienia:

1) pobranie rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań (według stawek obowiązujących u Administratora),

2) odmowa podejmowania działań.

Administrator, w przypadku podjęcia decyzji, o nieuzasadnionym lub nadmiernym charakterze żądania ma obowiązek wykazania takich cech żądania (wniosku) w ewentualnym postepowaniu przed organem nadzorczym.

Administrator jest zobowiązany po dokonaniu sprostowania/ uzupełnienia danych osobowych poinformować wszystkich odbiorców, którym ujawniono dane podlegające uzupełnieniu/sprostowaniu o fakcie ich uzupełnienia/sprostowania.

W przypadku braku możliwości wykonania powyższego, lub gdy działanie takie wymagałoby niewspółmiernie dużego wysiłku ze strony Administratora, może on podjąć decyzję o nieudzieleniu stosownej informacji odbiorcom, jednakże ma obowiązek wykazania braku tej możliwości lub niewspółmiernie dużego wysiłku w ewentualnym postepowaniu przed organem nadzorczym.

4. Terminy rozpatrywania żądań o sprostowanie/uzupełnienie danych osobowych.

Na podstawie art. 12 ust. 3 RODO, Administrator podejmuje decyzję o przyjęciu/odrzuceniu oświadczenia/wniosku o sprostowanie/uzupełnienie danych osobowych bez zbędnej zwłoki.

Terminy na udzielenie odpowiedzi na żądanie:

1) Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie **miesiąca** od otrzymania tego żądania;

2) jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne **2 miesiące**, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

W przypadku, gdy Administrator nie zamierza udzielić odpowiedzi i działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sadu.

Załącznik nr 7 do Polityki Ochrony Danych

Procedura: prawo do sprostowania danych osobowych („prawo do bycia zapomnianym")

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa usunięcia swoich danych osobowych („prawo do bycia zapomnianym") przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje prawo żądania usunięcia jej danych osobowych przetwarzanych przez Administratora. Prawo to składa się z następujących uprawnień:

1) Możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez Administratora danych,
2) Możliwości żądania, aby Administrator danych poinformował innych Administratorów, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, czy ich replikacje.

Obowiązek poinformowania innych Administratorów może być ograniczony przez: dostępną technologię, koszy, konieczność ograniczenia się Administratora do „rozsądnych działań".

Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych Administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

Każdej osobie fizycznej przysługuje prawo do „bycia zapomnianym". Prawo to można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

1. Dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2. Osoba, której dane dotyczą, wycofa zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;
3. Osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych do celów marketingowych;

4. Dane osobowe były przetwarzane w sposób „niezgodny z prawem",
5. Dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator";
6. Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W przypadku wykonania prawa do bycia zapomnianym, Administrator zaprzestanie przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowne oświadczenie/ wniosek, chyba że zachodzą szczególne przypadku ograniczające prawo do bycia zapomnianym:

1. Istnieje przepis prawa, który nakazuje przetwarzanie danych osobowych,
2. Istnieje sytuacja, w której przetwarzanie jest niezbędne do ustalenia dochodzenia lub obrony roszczeń.

Załącznik nr 8 do Polityki Ochrony Danych

Procedura: prawo do przenoszenia danych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do przeniesienia swoich danych osobowych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy osoba, której dane dotyczą uprzednio dostarczyła Administratorowi dane jej dotyczące, lub wyraziła zgodę na pozyskanie przez Administratora tych danych, w inny sposób, określony uprzednio odpowiednim oświadczeniem.

Prawo do przenoszenia danych to, w szczególności prawo do:

1) otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi;

2) prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych, o ile jest to technicznie możliwe.

Prawo do przeniesienia danych może zostać wykonane, gdy:

1) przetwarzanie danych odbywa się na podstawie zgody osoby, lub w celu wykonania umowy;

2) przetwarzanie danych odbywa się w sposób zautomatyzowany - prawo do przenoszenia danych obejmuje tylko te dane osobowe, które są przetwarzane przy użyciu systemów informatycznych i nie obejmuje ono tradycyjnych, manualnych papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła Administratorowi. Wykonywanie tego prawa nie może ono niekorzystnie wpływać na praw i wolności innych osób.

Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Załącznik nr 9 do Polityki Ochrony Danych

Procedura: prawo do sprzeciwu

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do sprzeciwu do przetwarzania swoich danych osobowych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, (w tym profilowania na podstawie tych przepisów), tj. sytuacji, w której:

1) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;

2) przetwarzanie jest niezbędne do celów, wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, do złożenia sprzeciwu wobec powyższego przetwarzania jej danych osobowych, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

W sytuacji, gdy Administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym również profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, to Administratorowi nie wolno już przetwarzać tych danych osobowych do takich celów.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania

dotyczących jej danych osobowych, chyba, że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo wnieść bezpłatnie sprzeciw do Administratora, w dowolnym momencie, wobec tego konkretnego przetwarzania, pierwotnego lub dalszego (w tym profilowania), o ile jest ono powiązane z marketingiem bezpośrednim.

Prawo do sprzeciwu musi zostać przez Administratora wyraźnie podane do wiadomości osobie, której dane dotyczą, jak również musi być przedstawione jasno i oddzielnie od wszelkich innych informacji.

3. Szczególne uprawnienia związane z procesami zautomatyzowanego przetwarzania danych - w tym z profilowaniem

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który odbywa się w sposób automatyczny, ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania.

Profilowanie zawsze wymaga poinformowania (w sposób możliwy do zweryfikowania) o nim osób, które są profilowane. Profilowanie może być wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji Administratora wobec osób, których dane dotyczą.

Jeżeli automatyczne podejmowanie decyzji wywołuje skutki prawne wobec osób, których dane dotyczą, lub w podobny istotny sposób wpływa na te osoby, Administrator może mechanizm ten stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

1. 1) osoba profilowana wyrazi na to wyraźną zgodę,
2. 2) profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
3. 3) profilowanie jest dopuszczalne przez szczególne przepisy prawa.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być szczególny przepis prawa. W przypadku, gdy zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.

Odwołanie zgody wywołuje wyłącznie skutki na przyszłość – oznacza to, że od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już opierać na zgodzie przetwarzania danych.

4. Realizacja prawa do sprzeciwu

Administrator, po wniesieniu sprzeciwu przez osobę, której dane przetwarzał, powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji.

Wykazanie zaistnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, jest obowiązkiem leżącym po stronie Administratora, i ma on obowiązek wykazania powyższego, w ewentualnym postepowaniu przed organem nadzorczym.

Wykorzystanie prawa do sprzeciwu nie prowadzi do automatycznego usunięcia wszystkich danych osobowych przez Administratora. Oznacza ono, że Administrator, z chwilą otrzymania sprzeciwu wobec przetwarzania danych osobowych, zaprzestaje z nich korzystać.

Załącznik nr 10 do Polityki Ochrony Danych

....., dnia.....

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), upoważniam:

Pana/ Panią.....

Zatrudnionego/ zatrudnioną w .....

na stanowisku .....

do przetwarzania danych osobowych zgodnie z zakresem obowiązków.

Rozwiązanie stosunku pracy/ umowy w przypadku zleceniobiorców/ skutkuje odwołaniem upoważnienia.

.....

(pieczęć i podpis Administratora)

Załącznik nr 11 do Polityki Ochrony Danych

Wzór ewidencji osób upoważnionych do przetwarzania danych

Lp.	Imię i nazwisko	Stanowisko	Data nadania	Data ustania	Zakres upoważnienia

Załącznik nr 12 do Polityki Ochrony Danych

Opis środków technicznych i organizacyjnych

Siedziba główna Administratora mieści się w Gminie Krokowa ul. Żarnowiecka 29, 84-110 Krokowa. Na w/w obszary przetwarzania danych składają się następujące pomieszczenia urzędu.

Środki zabezpieczające budynek:
Każdy z budynków posiada system alarmowy, w związku z tym został oznakowany stosownymi tablicami informującymi o funkcjonowaniu tego typu zabezpieczeń.

Kopie zapasowe
Dane osobowe przetwarzane w formie elektronicznej, w szczególności w systemach informatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada pracownik zatrudniony na stanowisku ds. informatyzacji.

Kopie zapasowe objęte są:

	Częstotliwość wykonywania kopii zapasowej	Rodzaj nośnika na jakim wykonano kopię zapasową	Sposób wykonywania kopii	Miejsce przechowywania nośnika na którym zapisano kopię
Baza danych	Dni robocze	Dysk HDD	Automatyczny	Budynek Urzędu Gminy
Serwery				
Pliki z dysków wspólnych	Raz w tygodniu	Dysk HDD	Automatyczny	Budynek Urzędu Gminy

Sposób postępowania z kluczami do pomieszczeń biurowych
Administrator wyznaczył pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy jednostki. Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do nie udostępniania kluczy oraz kodu cyfrowego do systemu alarmowego osobom trzecim.

Klucze do poszczególnych pomieszczeń pracowniku pobierają i zdają po zakończonym dniu pracy do sekretariatu. Od momentu pobrania kluczy do momentu ich zdania na pracownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń. W

przypadku stwierdzenia nieprawidłowości należy postępować zgodnie z procedurą naruszeń **załącznik nr 17 do niniejszej polityki.**

Zabrania się pozostawienia kluczy do pomieszczeń obszaru przetwarzania danych lub w miejscach ogólnie dostępnych, pomieszczenia zamyka się na czas nieobecności wszystkich pracowników w sposób uniemożliwiający dostęp osobom nieupoważnionym.

Pracownicy po godzinach pracy jednostki mogą w nim przebywać jedynie za zgodą Administratora. W przypadkach przebywania pracowników w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.

Załącznik nr 13 do Polityki Ochrony Danych

Oświadczenie o zachowaniu poufności

Ja niżej podpisany/a ..... zobowiązuje się do zachowania w tajemnicy danych osobowych, do których mam lub będę miał/ miała dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych, zarówno w trakcie obowiązującego stosunku pracy, jak i bezterminowo po ustaniu zatrudnienia.

.....

(podpis pracownika)

Załącznik nr 14 do Polityki Ochrony Danych

Oświadczenie o monitorowaniu komputerów służbowych

Oświadczam, iż zostałam/ zostałem zaznajomiona/ zaznajomiony z faktem, iż systemy informatyczne, do których mam dostęp na komputerze służbowych i na których wykonuję obowiązki pracownicze, są monitorowane w zakresie ilościowego i jakościowego wykorzystania tych systemów.

Oświadczam, że monitoring obejmuje również sposób wykorzystania służbowej poczty elektronicznej. Zobowiązuje się do wykorzystywania jej jedynie w celu realizacji zadań pracowniczych, wynikających ze stosunku pracy.

.....

(podpis osoby składającej oświadczenie)

Załącznik nr 15 do Polityki Ochrony Danych

Wzór umowy powierzenia danych

UMOWA POWIERZENIA

przetwarzania danych osobowych

zawarta w ..... w dniu ..... r. pomiędzy:

.....

zwanym dalej **„Zleceniodawcą"**

reprezentowaną przez:

..... – .....

..... z siedzibą przy ....., ..., kod pocztowy .....

(NIP: ....., REGON: ..... zwanym dalej **„Zleceniobiorcą"**

reprezentowaną przez:

..... - .....

§ 1

Oświadczenia stron

1. Zleceniodawca oświadcza, że jest Administratorem Danych Osobowych w rozumieniu ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych w stosunku do danych powierzonych Zleceniobiorcy.

2. Zleceniobiorca oświadcza, iż dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

3. Zleceniobiorca oświadcza, iż przygotował stosowną dokumentację wymaganą od podmiotu, któremu powierzono przetwarzanie danych osobowych, zgodnie z postanowieniami ustawy z dnia 10 maja 2018 r. o ochronie danych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych.

§ 2

Zakres i cel przetwarzania danych osobowych

1. W związku z realizacją umowy pomiędzy Stronami, o ..... Zleceniodawca powierza Zleceniobiorcy w trybie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych przetwarzanie danych osobowych.
2. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych/:
   1) imię i nazwisko,
   2), adres
   3), numer telefonu
   4) inne dane osobowe .
3. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Zleceniobiorcę wyłącznie w celu wykonywania przez Zleceniobiorcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie, o której mowa w § 2 ust. 1 i w sposób zgodny z niniejszą Umową.

§ 3

Zobowiązania podmiotu, któremu powierzono przetwarzanie danych osobowych (zobowiązania Zleceniobiorcy)

1. Zleceniobiorca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 2, do ich zabezpieczenia poprzez podjęcie następujących środków:
   1) Środki organizacyjne: (*została opracowana i wdrożona Polityka bezpieczeństwa. została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym, do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Bezpieczeństwa Informacji)*
   2) Środki ochrony fizycznej danych:

Dokumenty zawierające dane osobowe znajdują się w szafach zamykanych, w pomieszczeniach zamkniętych na klucz

3) Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
Komputery zabezpieczone są hasłami, zawierają programy antywirusowe.

4) Środki ochrony w ramach narzędzi programowych i baz danych
Pliki zawierające dane osobowe zabezpieczone są hasłami dostępu.

2. Zleceniobiorca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

3. Zleceniobiorca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:

1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia lub śledztwa,

2) każdym nieupoważnionym dostępie do danych osobowych,

3) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.

4. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Zleceniobiorca oraz żądania składania przez niego pisemnych wyjaśnień.

5. Na zakończenie kontroli, o których mowa w ust. 4, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Zleceniobiorca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.

6. Zleceniobiorca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.

7. Zleceniobiorca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.

8. Zleceniobiorca może „podpowierzyć" usługi objęte umową, o której mowa w § 2 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą Zleceniodawcy. Zleceniobiorca informuje Zleceniodawcę o każdym podwykonawcy oraz każdej ewentualnej zmianie w tym zakresie.

§ 4

Odpowiedzialność Zleceniobiorcy

1. Zleceniobiorca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako Administrator Danych Osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Zleceniobiorca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§ 5

Warunki wypowiedzenia Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
   1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
   3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 2 ust. 1.

§ 6

Rozwiązanie Umowy

Zleceniobiorca, w przypadku wygaśnięcia umowy, o której mowa §2 ust.1 i niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym

skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§7

Postanowienia końcowe

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują przepisy ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz innych przepisów.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....

Zleceniodawca

.....

Zleceniobiorca

Załącznik nr 16 do Polityki Ochrony Danych

Wzór rejestru umów powierzenia przetwarzania danych osobowych

Lp.	Numer umowy	Data zawarcia umowy	Strona umowy	Zakres powierzenia
1				
2				
3				
4				
5				

Załącznik nr 17 do Polityki Ochrony Danych

Procedura zgłaszania naruszeń ochrony danych osobowych

1. Cel procedury

Celem procedury jest zminimalizowanie mogących wystąpić nieprawidłowości w funkcjonowaniu Zakładu, spowodowanych nieuprawnionym ujawnieniem danych osobowych, udostępnieniem lub umożliwieniem dostępu do nich osobom nieupoważnionym, zabraniem danych przez osobę nieupoważnioną, uszkodzeniem lub usunięciem, a w szczególności:

a. Nieautoryzowany dostęp do danych,
b. Nieautoryzowane modyfikacje lub zniszczenie danych,
c. Udostępnienie danych nieautoryzowanym podmiotom,
d. Nielegalne ujawnienie danych,
e. Pozyskanie danych z nielegalnych źródeł.

2. Klasyfikacja naruszeń

Naruszenia ze względu na ich występowanie możemy podzielić na:

1. Zdarzenia losowe **zewnętrzne**, których występowanie może doprowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, zakłócenia ciągłości pracy systemów (np. klęski żywiołowe, przerwy w zasilaniu);
2. Zdarzenia losowe wewnętrzne, których występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu, może nastąpić naruszenie poufności danych (np. niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu);
3. Zdarzenia zamierzone, celowe i świadome, niepowodujące uszkodzenia infrastruktury technicznej i zakłóceń ciągłości pracy możemy podzielić na:
   a. Nieuprawniony dostęp do bazy danych z zewnątrz,
   b. Nieuprawniony dostęp do bazy danych z sieci wewnętrznych,
   c. Nieuprawniony transfer danych,
   d. Pogorszenie funkcjonowania sprzętu i oprogramowania, np. działania wirusów
   e. Bezpośrednie zagrożenie materialnych składników systemu np. kradzieży sprzętu

3.Zgłaszanie naruszeń związanych z bezpieczeństwem informacji

W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik

przetwarzający dane osobowe zobowiązany jest przerwać czynności i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, a następnie postępować stosownie do podjętej przez niego decyzji.

Pracownicy jednostki mają obowiązek zgłaszać zauważone przez siebie naruszenia oraz notować wszystkie szczegóły związane z naruszeniami.

Zgłoszenie powinno zawierać:

a. Imię i nazwisko zgłaszającego,
b. Określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych;
c. Określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
d. Określenie znanych zgłaszającemu sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

Osoba zgłaszająca naruszenie w miarę możliwości powinna zabezpieczyć materiał dowodowy np.: zrobić zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że działanie odbiega od normy. Osobą odpowiedzialną za przyjmowanie zgłoszeń naruszeń w jednostce jest Sekretarz Gminy.

Postępowanie z naruszeniami

Osoba, która otrzymała zgłoszenie dokonuje wstępnej identyfikacji zdarzenia i po konsultacji z Inspektorem Ochrony Danych Osobowych dokonuje jego kwalifikacji jako naruszenie niskie lub wysokie. W przypadku kwalifikacji naruszenia jako niskie należy dokonać wpisu do rejestru naruszeń, którego wzór stanowi ***załącznik nr 1*** do niniejszej procedury. Naruszenie zakwalifikowane jako wysokie podlegają zgłoszeniu do organu nadzorczego niezwłocznie, jednak nie później niż po upływie 72 godzin po stwierdzeniu naruszenia.

a. Charakter incydentu i jest znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
b. Miejsce wystąpienia incydentu – identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
c. Liczba referatów/ komórek organizacyjnych dotkniętych incydentem,

d. Identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji,
e. Możliwości rozszerzenia się incydentu i sposoby jego ograniczania,
f. Szacowany poziom szkód,
g. Szacunkowy czas, po którym skutki naruszenia zostaną zlokalizowane, jeżeli nie ma możliwości natychmiastowego usunięcia naruszenia bezpieczeństwa informacji,
h. Skutki organizacyjne i prawne (wstępny szacunek).

Po dokonanej analizie Administrator zgłasza naruszenie do organu nadzorczego (wzór zgłoszenia stanowi ***załącznik nr 2*** do niniejszej Procedury),oraz jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (wzór zawiadomienia stanowi ***załącznik nr 3*** do niniejszej Procedury). Zawiadomienie osoby nie jest wymagane jeśli Administrator wdrożył odpowiednie techniczne i organizacyjne środki, które umożliwiają osobom nieuprawnionym dostęp do danych, zastosował następnie środki, które uniemożliwią osobom nieuprawnionym dostęp do danych, zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą. Z zawiadomienia, o którym mowa nie należy stosować, gdy wymagałoby to niewspółmiernie dużego wysiłku. W takim jednak wypadku należy opublikować ogłoszenie, zastosować inny, równie skuteczny środek.

Jeżeli z jakiegokolwiek powodu nie uda się przekazać zgłoszenia w tym terminie, do zgłoszenia należy dołączyć wyjaśnienie przyczyn opóźnienia. Jeżeli Administrator niw zawiadomił jeszcze o naruszeniu osób, których ono dotyczy, organ nadzorczy może mu to nakazać.

Dodatkowo naruszenia mogą być wykorzystane przez Inspektora Ochrony Danych podczas szkoleń pracowniczych jako przykład tego, co może się wydarzyć, jak unikać ich w przyszłości i jak reagować jak się wydarzą. Podczas wykorzystania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowywania poufności.

Załącznik nr 1:

Lp.	Data naruszenia	Kategoria osób, których dane zostały naruszone	Kwalifikacja naruszenia (niskie lub wysokie)	Zastosowane środki zaradcze	Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)	Zawiadomienie osoby której dane dotyczą (dotyczy lub nie dotyczy)
1						
2						
3						
4						
5						
6						
7						

Załącznik nr 2 – Procedura zgłaszania naruszeń ochrony danych osobowych

..... dnia.....

Urząd Ochrony Danych Osobowych

.....

Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu

Na podstawie obowiązku wynikającego z art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Data Naruszenia	
Liczba osób których dane dotyczą	
Liczba wpisów danych osobowych i kategoria danych	
Dane Inspektora Danych Osobowych	
Dane Organu Nadzorczego	
Charakter Naruszenia	
Konsekwencje naruszenia	
Zastosowane i proponowane środki zaradcze	

Załącznik nr 18 do Polityki Ochrony Danych

Wzór notatki z kontroli uprawnień

..... dnia .....roku

W związku z kontrolą uprawnień i kont użytkowników z dnia ..... stwierdzam co następuje:

1. Użytkownicy pracują na systemach zgodnych z ich uprawnieniami
   TAK/ NIE
   Jeśli NIE, należy wskazać pracowników którym należy nadać lub zabrać upoważnienia:
   .....
   .....
2. Użytkownicy posiadają na stacjach roboczych oprogramowanie na które jednostka posiada licencje
   TAK/ NIE
   Jeśli NIE, należy wykazać to oprogramowania oraz nazwy stacji roboczych, na których się ono znajduje
   .....
   .....
3. Na stacjach roboczych pracowników znajduje się oprogramowanie nie związane z pracą służbową np. komunikatory społecznościowe, aplikacje służące do wymiany lub pobierania plików, czytniki prywatnej poczty, oprogramowanie umożliwiające dostęp do prywatnej chmury z danymi itp. Portalami społecznościowymi
   TAK/ NIE
   Jeśli TAK należy wskazać pracowników oraz stacje robocze, na których zostało zidentyfikowane wyżej wymienione oprogramowanie:
   .....
   .....
4. Czy na stacjach roboczych pracowników znajdują się dokumenty i korespondencja nie związana z czynnościami służbowymi
   TAK/ NIE
   Jeśli TAK należy wskazać pracowników oraz stacje robocze na której niezgodności występują:
   .....
   .....
5. Wnioski i zalecenia pokontrolne:
   .....

.....
(podpis pracownika zatrudnionego
na stanowisku ds. informatyzacji)