ZARZĄDZENIE NR 45/ 2018

Wójta Gminy Sieciechów

z dnia 9 sierpnia 2018r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Urzędzie Gminy Sieciechów

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2018 r. poz. 994) w związku z art. 24 ust.1 i 2 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 ,

zarządzam, co następuje:

§ 1

Wprowadzam w Urzędzie Gminy Sieciechów „Politykę ochrony danych osobowych", stanowiącą załącznik nr 1 i 4,5,6,7,8,9 do niniejszego zarządzenia.

§ 2

Zobowiązuję wszystkich pracowników Urzędu Gminy Sieciechów do zapoznania się z „Politykę ochrony danych osobowych", oraz do przestrzegania jej postanowień.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

Mariusz Zbigniew Czerski

Załącznik Nr 1 do Zarządzenia Wójta Gminy Sieciechów

Nr 45/2018 z dnia 09.08.2018r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

URZĄD GMINY SIECIECHÓW

Spis treści

I. Wstęp

Polityka ochrony danych osobowych zwana dalej „Polityką" określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych zawartych w systemie informatycznym w wewnętrznej sieci intranetowej oraz zbiorach danych zapisanych w postaci dokumentacji papierowej w Urzędzie Gminy Sieciechów.

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).

Wdrożenie polityki bezpieczeństwa danych osobowych Urzędu Gminy Sieciechów ma na celu zabezpieczenie danych osobowych przetwarzanych w formie papierowej i w systemie informatycznym.

II. Postanowienia ogólne

1. Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z Polityką:

1) **Administrator (danych)** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W Urzędzie Gminy Sieciechów Administratorem Danych Osobowych (ADO) jest Wójt Gminy Sieciechów.

2) **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.

3) **Dane osobowe** – wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników

określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

4) **Przetwarzanie danych osobowych** – dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

5) **Ograniczenie przetwarzania** – polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

6) **Anonimizacja** – zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych.

7) **Zgoda osoby, której dane dotyczą** – oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

8) **Ocena skutków w ochronie danych** – proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

9) **Podmiotem danych** jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

10) **Odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

11) **Podmiot przetwarzający (Procesor)** – osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

12) **Inspektor Ochrony Danych (IOD)** - osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych

i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

13) **Pseudonimizacja** – oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

14) **Szczególne kategorie danych osobowych (dane wrażliwe)** – ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych i obejmują przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

15) **Profilowanie** – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

16) **Naruszenie ochrony danych osobowych** – jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, wszelkiego zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu (włamania) do danych osobowych. W szczególności oznacza nieujawniony dostęp lub próbę dostępu do danych przetwarzanych w formie informatycznej lub papierowej lub pomieszczeń, w których się one znajdują, naruszenie lub próby naruszania integralności systemu, poufności danych lub ich części. Zniszczenie, uszkodzenie lub wszelką ingerencję w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony danych zawartych w systemach informatycznych lub poza nimi.

2. Filary ochrony danych osobowych w Urzędzie Gminy Sieciechów:

1) Legalność – ADO dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

2) Bezpieczeństwo – ADO zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

3) Prawa Jednostki – ADO umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

4) Rozliczalność – ADO dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

3. Zasady ochrony danych:

1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

2) rzetelnie i uczciwie (rzetelność);

3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

4) w konkretnych celach i nie "na zapas" (minimalizacja);

5) nie więcej niż potrzeba (adekwatność);

6) z dbałością o prawidłowość danych (prawidłowość);

7) nie dłużej niż potrzeba (czasowość);

8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

4. Rejestr czynności przetwarzania (RCP)

Administrator jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Administrator prowadzi rejestr zgodnie z załącznikiem nr 1. W celu monitorowania Polityki przez Inspektora Ochrony Danych osoba przetwarzająca dane osobowe z upoważnienia Administratora przekazuje informacje o czynnościach przetwarzania Inspektorowi Ochrony Danych.

5. Analiza ryzyka

Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administratora. Administrator 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. Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania i dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Arkusz analizy ryzyka stanowi załącznik nr 2.

6. Zarządzanie przetwarzaniem danych / Upoważnienia

1. Obowiązki Administratora zostały określone w RODO i wydanych na jego podstawie przepisach krajowych.

2. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w postaci papierowej oraz w systemach informatycznych.

3. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

4. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie. Upoważnienie do przetwarzania danych osobowych stanowi załącznik nr 3.

5. Administrator prowadzi rejestr osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja osób upoważnionych ma charakter pomocniczy i jest prowadzona zgodnie z załącznikiem nr 4.

6. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego.

7. Administrator wyznacza Inspektora Ochrony Danych (IOD) oraz osobę odpowiedzialną za zabezpieczenie technologiczne przetwarzania danych osobowych – Administratora Systemu Informatycznego (Informatyka).

8. Obowiązki IOD zostały określone w RODO. W szczególności do obowiązków IOD należy:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

- monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

- współpraca z organem nadzorczym;

– pełnienie funkcji punktu kontaktowego dla organu nadzorczego 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.

9. Administrator Systemu Informatycznego (Informatyk) odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu Gminy Sieciechów.

10. Administrator Systemu Informatycznego (Informatyk) pełni rolę zarządzającego oprogramowaniem w Urzędzie Gminy Sieciechów, przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.

11. Do obowiązków Administratora Systemu Informatycznego (Informatyka) w zakresie ochrony danych osobowych należy w szczególności:

– bieżący nadzór oraz zapewnienie optymalnej ciągłości działania systemu informatycznego;

– przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;

– analiza raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem przetwarzania danych w systemach informatycznych;

– zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych zgodnie z przepisami RODO oraz niniejszej Polityki oraz Instrukcji zarządzania RODO;

– instalacja i konfiguracja oprogramowania i sprzętu sieciowego oraz serwerowego używanego do przetwarzania danych osobowych;

– konfiguracja i administrowanie oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem;

– do nadzoru nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;

– przyznawanie za zgodą Administratora i za wiedzą Inspektora Ochrony Danych ściśle określonych praw dostępu do danych osobowych w danym systemie;

– świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu Gminy Sieciechów, służącego do przetwarzania danych osobowych.

12. W procesie przetwarzania danych osobowych uczestniczy każdy pracownik Urzędu Gminy Fajsławice i powinien przestrzegać zasad przetwarzania i ochrony danych osobowych przetwarzanych w Urzędzie Gminy Sieciechów. Każda upoważniona do przetwarzania danych osoba jest osobiście odpowiedzialna za bezpieczeństwo powierzonych jej danych.

13. Administrator zobowiązany jest ponadto do poinformowania osób, których dane osobowe przetwarzają, o ich uprawnieniach wynikających z art. 13 ust 1 i 2 RODO.

14. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art.14 i art. 15 RODO.

7. Środki techniczne i organizacyjne zabezpieczające dane osobowe / minimalizacja

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych. Instrukcja zarządzania RODO stanowi załącznik nr 5.

2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.

3. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.

4. Administrator dba o minimalizację przetwarzania danych pod kątem: adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych oraz czasu przechowywania danych.

5. Administrator zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

6. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

7. Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

8. Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

9. Administrator stosuje kontrolę dostępu fizycznego.

10. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających, jeżeli takie wystąpi.

8. Regulamin ochrony danych osobowych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Załącznik nr 6 zawiera Regulamin ochrony danych osobowych.

9. Instrukcja postępowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości. Niniejsze zapisy mają zastosowanie do danych osobowych przetwarzanych w systemach informatycznych i papierowych.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu Inspektora Ochrony Danych. Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

2. Do typowych podatności bezpieczeństwa danych osobowych należą:

a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),

c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia incydentu należy bezzwłocznie powiadomić Inspektora Ochrony Danych. IOD prowadzi postępowanie wyjaśniające w toku, którego:

a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,

b) wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem,

c) inicjuje ewentualne działania dyscyplinarne,

d) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,

e) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Formularz rejestru naruszeń stanowi załącznik nr 7.

7. Inspektor Ochrony Danych po opanowaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu końcowego stanowi załącznik nr 8 – Raport ze stwierdzenia naruszenia.

8. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

9. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

III. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Tabela 1. Wykazu budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych.	
Adres: Urząd Gminy Sieciechów 26-922 Sieciechów ul. Rynek 16	Pomieszczenia: budynek przy ul. 11 Listopada 2 GBP 1,2(biura)pokoje nr: GOPS 3,4,GK 6,KsOś 10 Budynek Urzędu: ul. Rynek 16 – Archiwum – Pokoje nr: 1,2,3,4,5,6,7,8,9,10,11,12

	Serwerownia: I piętro

2. Zbiory danych

Tabela 2. Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w jednostce

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych w Urzędzie Gminy Fajsławice.				
Lp.	Zbiór danych	Programy zastosowane do przetwarzania / Nazwa zasobu	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
1.	Gospodarka odpadami komunalnymi	Przetwarzany sposób papierowy i w systemie informatycznym – Odpady w Gminie firma PROFEKO	Pokój nr 6	Pokój nr 6
2.	Dzienniki korespondencji	Przetwarzany w sposób papierowy	Pokój nr 1	Pokój nr 1
3.	Pocztowe książki nadawcze	Przetwarzany w sposób papierowy	Pokój nr 1 Archiwum	Pokój nr 1
4.	Akta osobowe	Przetwarzany w sposób papierowy	Pokój nr 7	Pokój nr 7
5.	Aplikacje kandydatów na stanowiska w Urzędzie Gminy Sieciechów /w tym dokumentacja konkursowa/	Przetwarzany w sposób papierowy	Pokój nr 7	Pokój nr 7

6.			Pokój nr 4	Pokój nr 4
7.	Umowy o dostawę wody, ścieków, czynszowe i dzierżawne	Przetwarzany w sposób papierowy	Pokój nr 8	Pokój nr 8
8.	Rejestry VAT	Przetwarzany w sposób papierowy i w systemie informatycznym – Macrologic-ERP	Pokój nr 8 Serwerownia	Pokój nr 8
9.	Faktury VAT	Przetwarzany w sposób papierowy i w systemie informatycznym Macrologic-Bens	Pokój nr 4	Pokój nr 4
10.	Wykaz osób podłączonych do kanalizacji i wodociągu	Przetwarzany w sposób papierowy i w systemie informatycznym – COMARCH- ERP Optima -księgowość GW- MAX- faktury	Pokój nr 8	Pokój nr 8
11.	Dodatki mieszkaniowe	Przetwarzany w sposób papierowy i w systemie informatycznym – Microbit	Pokój nr 3,4	Pokój nr 3,4
12.	Deklaracje na podatek rolny, leśny i od nieruchomości osób prawnych	Zbiór przetwarzany w sposób papierowy oraz w systemie informatycznym (XPERTIS)	Pokój nr 6	Pokój nr 6
13.	Podatek od środków transportowych	Zbiór przetwarzany w sposób papierowy i w systemie	Pokój nr 5	Pokój nr 5

		informatycznym – ręczny papierowy		
14.	Projekty finansowe ze źródeł zewnętrznych	Przetwarzany w sposób papierowy i w systemie informatycznym	Pokój nr 5	Pokój nr 5
15.	Informacje na podatek rolny, leśny i od nieruchomości osób fizycznych	Zbiór przetwarzany w sposób papierowy i w systemie informatycznym -	Pokój nr 6 Serwerownia	Pokój nr 6
16.	Tytuły wykonawcze	Przetwarzany w sposób papierowy i w systemie informatycznym – XSPERTIS	Pokój nr 6,5	Pokój nr 6,5
17.	Zaświadczenia o stanie posiadania	Przetwarzany w sposób papierowy i w systemie informatycznym – XSPERTIS	Pokój nr 6	Pokój nr 6
18.	Kwitariusze przychodowe	Przetwarzany w sposób papierowy	Pokój nr 8	Pokój nr 8
19.	Zmiany geodezyjne	Przetwarzany w sposób papierowy	Pokój nr 6	Pokój nr 6
20.	Umowy dzierżawy	Przetwarzany w sposób papierowy	Pokój nr 2	Pokój nr 2
21.	Numeracja porządkowa budynków	Przetwarzany w sposób papierowy i w systemie informatycznym – punkty adresowe	Pokój nr 2	Pokój nr 2
22.	Ewidencja gruntów i budynków	Przetwarzany w sposób papierowy i w systemie	Pokój nr 2	Pokój nr 2

		informatycznym – Geoportal 2		
23.	Warunki podłączenia do sieci wodociągowej	Przetwarzany w sposób papierowy	Pokój nr 6	Pokój nr 6
24.	Protokoły odbioru przyłączy wodociągowych i kanalizacyjnych	Przetwarzany w sposób papierowy	Pokój nr 6	Pokój nr 6
25.	Pozwolenia, zezwolenia i zgłoszenia	Przetwarzany w sposób papierowy	Pokój nr 6	Pokój nr 6
26.	Planowanie budżetu	Przetwarzany w sposób papierowy i w systemie informatycznym – BeSTi@	Pokój nr 9, 10	Pokój nr 9, 10
27.	Płace	Przetwarzany w sposób papierowy i w systemie informatycznym – CALI(ONT Systemy Informatyczne), ASSECO	Pokój nr 12	Pokój nr 12
28.	Rejestracja przedpoborowych	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
29.	Kwalifikacja wojskowa	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
30.	Struktury organizacyjne formacji obrony cywilnej	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
31.	Listy imienne strażaków i kierowców OSP	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
32.	Urząd Stanu Cywilnego w Sieciechowie	Przetwarzany w sposób papierowy i w systemie	Pokój nr 5	Pokój nr 5

		informatycznym – Źródło		
33.	Ewidencja ludności i dowody osobiste	Przetwarzany w sposób papierowy i w systemie informatycznym – Źródło ,PESEL ,RDE, rejestr dowodów osobistych, BUSC	Pokój nr 5	Pokój nr 5
34.	Płatnik	Przetwarzany w sposób papierowy i w systemie informatycznym – Asseco Poland S.A.	Pokój nr 9	Pokój nr 9
35.	Program Finansowo-Księgowy	Przetwarzany w sposób papierowy i w systemie informatycznym – System finansowo-księgowy (Vendis)	Pokój nr 10, 9 Serwerownia	Pokój nr 10, 9
36.	Obsługa Rady Gminy	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
37.	Awanse zawodowe nauczycieli, cząstkowa ocena pracy dyrektorów szkół, organizacja konkursów na stanowisko dyrektora szkoły	Przetwarzany w sposób papierowy KALI ,Qwark ,Płatnik	Pokój nr 10	Pokój nr 10
38.	Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	Przetwarzany w sposób papierowy i w systemie informatycznym – XPERTIS	Pokój nr 5	Pokój nr 5

39.	Zezwolenie na usuwanie drzew i krzewów z zadrzewień	Przetwarzany w sposób papierowy	Pokój nr 6	Pokój nr 6
40.	Zezwolenia na sprzedaż napojów alkoholowych	Przetwarzany w sposób papierowy	Pokój nr 1	Pokój nr 1
41.	Usuwanie wyrobów azbestowych	Przetwarzany w sposób papierowy	Pokój nr 2	Pokój nr 2
42.	Zwrot kosztów kształcenia młodocianych pracowników	Przetwarzany w sposób papierowy	Pokój nr 10	Pokój nr 10
43.	Dodatki energetyczne	Przetwarzany w sposób papierowy	Pokój nr 4	Pokój nr 4
44.	Szacowanie strat w uprawach rolnych	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
45.	Decyzje o środowiskowych uwarunkowaniach	Przetwarzany w sposób papierowy	Pokój nr 2	Pokój nr 2
46.	Kontrola spełniania obowiązku nauki	Przetwarzany w sposób papierowy	Pokój nr 10	Pokój nr 10
47.	Zwrot kosztów wychowania przedszkolnego dzieci zamieszkałych poza Gminą Sieciechów	Przetwarzany w sposób papierowy	Pokój nr 10	Pokój nr 10

48.	Świadczenia osobiste i rzeczowe na rzecz obrony	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
49.	Listy płac ekwiwalentu za udział w akcjach ratowniczych	Przetwarzany w sposób papierowy	Pokój nr 14	Pokój nr 14
50.	BHP	Przetwarzany w sposób papierowy	Pokój nr 1	Pokój nr 1
51.	Archiwizacja	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr 5
52.	Sporządzanie list wyborczych	Przetwarzany w sposób papierowy i w systemie informatycznym	Pokój nr 3	Pokój nr 3
53.	Oświadczenie o wyrażeniu zgody na dysponowanie działką na cele budowlane	Przetwarzany w sposób papierowy	Pokój nr 2	Pokój nr 2
54.	Nieodpłatna kontrolowana praca fizyczna na cele społeczne	Przetwarzany w sposób papierowy	Pokój nr 5	Pokój nr
55.	Zamówienia publiczne	Przetwarzany w sposób papierowy	Pokój nr 1	Pokój nr 1

3. System informatyczny

System informatyczny Administratora Danych obsługiwany jest przez rozproszone serwery (logiczne - posadowione bazy danych SQL na stacjach roboczych i fizyczne - dedykowane maszyny z oprogramowaniem serwerowym). System ten ma bezpieczne połączenie z Internetem. W systemie informatycznym przetwarzane są dane ze zbiorów danych Administratora Danych, tj.:

1. Opłaty ryczałtowe i licznikowe

2. Deklaracje na podatek rolny, leśny i od nieruchomości osób prawnych
3. Informacje na podatek rolny, leśny i od nieruchomości osób fizycznych
4. Ewidencja gruntów i budynków
5. Planowanie budżetu
6. Płace
7. Urząd Stanu Cywilnego w Sieciechowie
8. Ewidencja ludności i dowody osobiste
9. Płatnik
10. Program Finansowo – Księgowy
11. Gospodarka odpadami komunalnymi
12. Zwrot podatku akcyzowego
13. Dodatki mieszkaniowe
14. Deklaracje na podatek od środków transportowych

4. Struktura zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania danych

Wykaz zbiorów danych wraz ze wskazaniem ich struktury.		
Lp.	Zbiór danych	Struktura zbioru
1.	Gospodarka odpadami komunalnymi	Imię i nazwisko, Adres zamieszkania, PESEL, Imiona rodziców, Data urodzenia, Nr telefonu, Adres poczty elektronicznej, Stan posiadania
2.	Dzienniki korespondencji	Imię i nazwisko Adres zamieszkania
3.	Pocztowe książki nadawcze	Imię i nazwisko Adres zamieszkania
4.	Akta osobowe	imię i nazwisko, adres zamieszkania, numer telefonu, wysokość wynagrodzenia, podstawowe, niezbędne do ustalenia wysokości wynagrodzenia, dane dotyczące stażu pracy, wykształcenia, urlopów i zwolnień, numer dowodu osobistego, numer NIP i PESEL, imiona rodziców, datę i miejsce urodzenia, informacje o odbytych szkoleniach, urlopach, dokładne dane dotyczące wykształcenia, ewentualnie zainteresowań i hobby, informacje o

		posiadanych dzieciach, zawartych związkach małżeńskich, dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych zwłaszcza w wyniku badań profilaktycznych (wstępnych, Okresowych i kontrolnych)
5.	Aplikacje kandydatów na stanowiska w Urzędzie Gminy Sieciechów (w tym dokumentacja konkursowa)	Imiona i nazwiska, Adres zamieszkania, Data i miejsce urodzenia, Wykształcenie, Kwalifikacje zawodowe Przebieg kariery zawodowej, Informacje o zainteresowaniach, Załączniki (np. zaświadczenia o niekaralności kandydata, zaświadczenia lekarskie)
6.	Opłaty ryczałtowe i licznikowe	Imię i nazwisko, Adres zamieszkania, Imiona rodziców, Numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej
7.	Umowy o dostawę wody, ścieków, czynszowe i dzierżawne	Imię i nazwisko, Adres zamieszkania, Numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej
8.	Rejestry VAT	Imię i nazwisko, Adres zamieszkania, Numer Identyfikacji Podatkowej, Numer ewidencyjny PESEL
9.	Faktury VAT	Imię i nazwisko Adres zamieszkania Numer Identyfikacji Podatkowej Numer ewidencyjny PESEL
10.	Wykaz osób podłączonych do kanalizacji i wodociągu	Imię i nazwisko Adres zamieszkania
11.	Dodatki mieszkaniowe	Imię i nazwisko Adres zamieszkania Data urodzenia Numer ewidencyjny PESEL Informacja nt. dochodów Zaświadczenia o wynagrodzeniu
12.	Deklaracje na podatek rolny, leśny i od nieruchomości osób prawnych	Imię i nazwisko/ Nazwa Adres zamieszkania/ Siedziby Imiona rodziców Data i miejsce urodzenia Stan posiadania
13.	Podatek od środków	Imiona i nazwiska Adres zamieszkania

	transportowych	Data urodzenia Imię ojca Numer identyfikacyjny PESEL Numer Identyfikacji Podatkowej Dane dot. pojazdu
14.	Projekty finansowe ze źródeł zewnętrznych	Imię i nazwisko Adres zamieszkania Data i miejsce urodzenia Numer ewidencyjny PESEL Imiona rodziców Seria i numer dowodu osobistego Telefon
15.	Informacje na podatek rolny, leśny i od nieruchomości osób fizycznych	Imię i nazwisko Adres zamieszkania Imiona rodziców Data i miejsce urodzenia Numer Identyfikacji Podatkowej PESEL Stan posiadania
16.	Tytuły wykonawcze	Imię i nazwisko Adres zamieszkania Imiona rodziców Numer ewidencyjny PESEL Stan zaległości
17.	Zaświadczenia o stanie posiadania	Imię i nazwisko Adres zamieszkania Stan majątkowy
18.	Kwitariusze przychodowe	Imię i nazwisko Adres zamieszkania Numer Identyfikacji Podatkowej
19.	Zmiany geodezyjne	Imię i nazwisko Adres zamieszkania Imiona rodziców Numer ewidencyjny PESEL Numer Identyfikacji Podatkowej Informacje nt. nabywanych i zbywanych gruntów
20.	Umowy dzierżawy	Imię i nazwisko Adres zamieszkania Imiona rodziców Numer ewidencyjny PESEL

		Numer Identyfikacji Podatkowej Seria i numer dowodu osobistego
21.	Numeracja porządkowa budynków	Imię i nazwisko Adres zamieszkania Stan posiadania
22.	Ewidencja gruntów i budynków	Imię i nazwisko Adres zamieszkania Imiona rodziców Numer ewidencyjny PESEL Numer Identyfikacji Podatkowej Seria i numer dowodu osobistego
23.	Warunki podłączenia do sieci wodociągowej	Imię i nazwisko Adres zamieszkania
24.	Protokoły odbioru przyłączy wodociągowych i kanalizacyjnych	Imię i nazwisko Adres zamieszkania
25.	Pozwolenia, zezwolenia i zgłoszenia	Imię i nazwisko Adres zamieszkania
26.	Planowanie budżetu	Imię i nazwisko Adres zamieszkania Data urodzenia
27.	Płace	Imię i nazwisko Nazwisko rodowe Adres zamieszkania Data i miejsce urodzenia PESEL/NIP Dane nt. członków rodziny pracownika Angaże z umów Przebieg zatrudnienia Numer konta bankowego Imiona rodziców Wykształcenie, stopień awansu zawodowego Seria i numer dowodu osobistego Nr renty/emerytury/świadczeń kompensacyjnych
28.	Rejestracja przedpoborowych	Imię i nazwisko Imiona rodziców Data urodzenia

		Adres zamieszkania Seria i numer dowodu osobistego Miejsce urodzenia Numer ewidencyjny PESEL
29.	Kwalifikacja wojskowa	Imię i nazwisko Imiona rodziców Data urodzenia Numer ewidencyjny PESEL Adres zamieszkania Seria i numer dowodu osobistego Miejsce urodzenia Stosunek do powszechnego obowiązku obrony (książeczka wojskowa) Poprzednie miejsca pobytu czasowego i stałego
30.	Struktury organizacyjne formacji obrony cywilnej	Imię i nazwisko Adres zamieszkania Imię ojca Data i miejsce urodzenia Numer ewidencyjny PESEL Stosunek do powszechnego obowiązku obrony (książeczka wojskowa)
31.	Listy imienne strażaków i kierowców OSP	Imię i nazwisko Adres zamieszkania Data urodzenia Numer identyfikacyjny PESEL Imię ojca
32.	Urząd Stanu Cywilnego w Sieciechowie	Nazwiska i imiona Imiona rodziców Data urodzenia Adres zamieszkania lub pobytu PESEL Wykształcenie Seria i numer dowodu osobistego Płeć Stan cywilny Nazwisko z poprzedniego małżeństwa i rodowe Nazwisko i imię: ojca, matki, współmałżonka Nazwisko po zawarciu małżeństwa Miejsce i godzina urodzenia Data zdarzenia i numer aktu: urodzenia, małżeństwa, zgonu Data i miejsce zawarcia małżeństwa

		Miejsce wystawienia i numer aktu urodzenia współmałżonka Data, godzina, miejsce odnalezienia zwłok i zgonu Nazwisko, imię i adres osoby zgłaszającej zgon Adnotacje o rozwodzie i separacji Numer i seria oraz miejsce wydania dowodu osobistego Data unieważnienia aktu: urodzenia, małżeństwa, zgonu Imię nadane z urzędu Data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko Imię i nazwisko osoby przysposabiającej dziecko Zmiana nazwiska dziecka Numer aktu zgonu współmałżonka i data Nazwisko, nazwisko rodowe i imię współmałżonka Nazwisko rodowe matki i ojca Data rozwiązania poprzedniego małżeństwa Data i miejsce urodzenia matki dziecka i mężczyzny uznającego ojcostwo Kraj urodzenia Nazwiska rodowe rodziców dziecka Data i miejsce urodzenia rodziców dziecka Obywatelstwo dziecka, matki i ojca Miejsce zamieszkania rodziców Nazwisko i imię osoby zgłaszającej urodzenie Nazwiska i imiona, nazwiska rodowe, data i miejsce urodzenia Nazwiska rodowe i imiona rodziców osób zawierających małżeństwo Nazwiska rodziców i dzieci zrodzonych z małżeństwa Adnotacje o ustaniu, unieważnieniu, ustaleniu nieistnienia małżeństwa, separacji, zniesienia separacji, orzeczeń sądu, sygnatura akt sprawy, data uprawomocnienia orzeczenia. Godzina urodzenia i zgonu Nazwisko i imię biegłego lub tłumacza Adres do korespondencji
33.	Ewidencja ludności i dowody osobiste	Nazwiska i imiona Imiona i nazwiska rodziców Data i kraj urodzenia Adres zamieszkania lub pobytu oraz data zameldowania i wymeldowania na pobyt stały i czasowy PESEL Seria i numer dowodu osobistego

		Obywatelstwo Płeć Stan cywilny, data zawarcia związku małżeńskiego, oznaczenie aktu, data rozwiązania związku małżeńskiego, sygnatura akt i oznaczenie sądu Miejsce urodzenia Wystawca dokumentu tożsamości Poprzednie adresy Nazwisko rodowe Nazwisko rodowe matki Dane współmałżonka Właściwy USC i numer aktu urodzenia Stosunek do powszechnego obowiązku obrony Dane o poprzednich stanach cywilnych Oznaczenie aktu i Urząd Stanu Cywilnego sporządzenia Data wyjazdu, powrotu Kraj poprzedniego miejsca zamieszkania i zamieszkanie Adres elektroniczny do doręczeń Nazwisko i imię pełnomocnika Data wydania i ważności dowodu osobistego Oznaczenie organu wydającego dowód osobisty Adres do korespondencji(opcjonalnie adres poczty elektronicznej lub numer telefonu)
34.	Płatnik	NIP płatnika REGON płatnika PESEL ubezpieczonego i członków rodziny ubezpieczonego Nazwa firmy płatnika Imię i nazwisko płatnika, ubezpieczonego i członków rodziny ubezpieczonego Data urodzenia płatnika, ubezpieczonego i członków rodziny ubezpieczonego Telefon płatnika, ubezpieczonego i członków rodziny ubezpieczonego Numer rachunku bankowego płatnika, Informacje n.t. niepełnosprawności ubezpieczonego i członków rodziny ubezpieczonego Zawód i miejsce pracy ubezpieczonego
35.	Program Finansowo-Księgowy	Imię i nazwisko Adres zamieszkania Numer konta bankowego

36.	Obsługa Rady Gminy	Imię i nazwisko Adres zamieszkania
37.	Awanse zawodowe nauczycieli, cząstkowa ocena pracy dyrektorów szkół, organizacja konkursów na stanowisko dyrektora szkoły	Imię i nazwisko Adres zamieszkania Data i miejsce urodzenia Wykształcenie Kwalifikacje zawodowe Przebieg stażu Wyniki postępowania egzaminacyjnego
38.	Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	Imię i nazwisko Adres zamieszkania Stan posiadania
39.	Zezwolenie na usuwanie drzew i krzewów z zadrzewień	Imię i nazwisko Adres zamieszkania Stan posiadania
40.	Zezwolenia na sprzedaż napojów alkoholowych	Imię i nazwisko Adres zamieszkania Stan posiadania Numer ewidencyjny PESEL Numer Identyfikacji Podatkowej Seria i numer dowodu osobistego
41.	Usuwanie wyrobów azbestowych	Imię i nazwisko Adres zamieszkania Stan posiadania
42.	Zwrot kosztów kształcenia młodocianych pracowników	Imię i nazwisko Adres zamieszkania Numer ewidencyjny PESEL Imiona rodziców Data i miejsce urodzenia Adres prowadzenia działalności Numer Identyfikacji Podatkowej REGON Kwalifikacje zawodowe Przebieg zatrudnienia młodocianego Otrzymana pomoc de minimis Informacje dotyczące prowadzonej działalności

		gospodarczej, na którą udzielono pomocy de minimis
43.	Dodatki energetyczne	Imię i nazwisko Adres zamieszkania Stan posiadania
44.	Szacowanie strat w uprawach rolnych	Imię i nazwisko Adres zamieszkania Stan posiadania
45.	Decyzje o środowiskowych uwarunkowaniach	Imię i nazwisko Adres zamieszkania
46.	Kontrola spełniania obowiązku nauki	Imię i nazwisko dziecka Imiona rodziców PESEL Adres zamieszkania Adres zameldowania Szkoła lub miejsce, w której dziecko spełnia obowiązek nauki
47.	Zwrot kosztów wychowania przedszkolnego dzieci zamieszkałych poza gminą Fajsławice	Imię i nazwisko dziecka PESEL Adres zamieszkania Imiona rodziców Miejsce nauki
48.	Świadczenia osobiste i rzeczowe na rzecz obrony	Nazwisko i imiona Adres zamieszkania Imię ojca Numer ewidencyjny PESEL Data i miejsce urodzenia Stosunek do powszechnego obowiązku obrony (książeczka wojskowa)
49.	Listy płac ekwiwalentu za udział w akcjach ratowniczych	Nazwisko i imię Adres zamieszkania Imię ojca
50.	BHP	Imię i nazwisko PESEL

		Adres zamieszkania Stan zdrowia Imiona rodziców
51.	Archiwizacja	Dane osobowe wyszczególnione w rejestrze czynności przetwarzania danych
52.	Listy wyborcze	Imię i nazwisko Adres zamieszkania Data urodzenia Numer ewidencyjny PESEL
53.	Oświadczenie o wyrażeniu zgody na dysponowanie działką na cele budowlane	Imię i nazwisko Adres zamieszkania Numer ewidencyjny działki
54.	Nieodpłatna kontrolowana praca fizyczna na cele społeczne	Imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, okres wykonywania kary, orzeczenie o skazaniu
55.	Zamówienia publiczne	Imię i nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu tożsamości, numer telefonu, adres e-mail, REGON, adres prowadzenia działalności gospodarczej, w tym dane wynikające z ustawy Prawo zamówień publicznych oraz z rozporządzenia Ministra Rozwoju w sprawie rodzajów dokumentacji, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia

IV. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych).

1. Zabezpieczenie sprzętu

1. Serwerownia jest zlokalizowana w budynku Urzędu Gminy na pierwszym piętrze.

Zabezpieczona jest poprzez:

- systemy sygnalizacji włamania i napadu (SSWiN) oraz kontrola dostępu (KD),

System sygnalizacji włamania i napadu oraz kontroli dostępu wykonany jest aby zabezpieczyć serwerownię przed takimi zagrożeniami jak: włamanie, kradzież, nieuprawniony dostęp do pomieszczenia oraz pożar. System kontroli dostępu przystosowany jest do obsługi jednego przejścia. Zbudowany jest on z kontrolera przejścia oraz czytnika kart zamontowanego przed wejściem do serwerowni. Zapewnia pełną kontrolę i pamięć zdarzeń (rejestracja wejść wraz z identyfikacją karty). Karty zbliżeniowe są w standardzie UNIQUE.

- klimatyzator,
  Ze względu na potrzebę utrzymania optymalnych warunków dla pracy urządzeń w pomieszczeniu serwerowni zastosowano system klimatyzacji.

- drzwi antywłamaniowych
  - drzwi stalowe antywłamaniowe
  - zamki atestowane,
- rolety antywłamaniowe

2. Logiczne serwery bazodanowe rozmieszczone są w pokojach zabezpieczonych w sposób uniemożliwiający dostęp osobom nieupoważnionym (drzwi zamykane na klucz). W ich przypadku stosuje się mechanizmy kryptograficznego zabezpieczenia informacji.

3. Administrator Systemu Informatycznego (Informatyk) wskazuje użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:

- ochronę nośników przenośnych – w tym także nośników danych, na których przechowywane są kopie zabezpieczające,
- prawidłową lokalizację komputerów.

4. Wszystkie urządzenia systemu informatycznego Administratora Danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).

5. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.

6. Bezprzewodowy punkt dostępowy do sieci lokalnej Administratora Danych przeznaczony dla komputerów przenośnych Administratora Danych chroniony jest za pomocą silnych metod kryptograficznych, uwierzytelniania i szyfrowania komunikacji. Dodatkowo funkcjonalność tego segmentu sieci jest okrojona za pomocą urządzenia UTM.

7. Bezprzewodowa sieć Internetowa dla mieszkańców Gminy jest rozdzielona z siecią lokalną Urzędu za pomocą urządzenia UTM.

8. Bieżąca konserwacja sprzętu wykorzystywanego przez Administratora Danych do przetwarzania danych prowadzona jest tylko przez Administratora Systemu

Informatycznego (Informatyka). Natomiast poważne naprawy wykonywane przez personel zewnętrzny realizowane są w siedzibie Administratora Danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.

9. Administrator Systemu Informatycznego (Informatyk) dopuszcza konserwowanie i naprawę sprzętu poza siedzibą Administratora Danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych.

2. Zabezpieczenia we własnym zakresie

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1) ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
2) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych oraz w samochodach;
3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
4) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
5) pilnego strzeżenia akt, pamięci przenośnych i komputerów przenośnych;
6) kasowania po wykorzystaniu danych na dyskach przenośnych;
7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;
8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Inspektora Ochrony Danych;

11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

12) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;

13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

16) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie zabezpieczone obszary, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;

17) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

18) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

19) zachowania tajemnicy danych, w tym także wobec najbliższych;

20) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

21) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego, odpowiednio zabezpieczonym miejscu po zakończeniu dnia pracy;

22) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

23) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

3. Postępowanie z nośnikami przenośnymi i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny zwłaszcza pamiętać, że:

1) dane z nośników przenośnych niebędących kopiami zabezpieczającymi po wprowadzeniu do systemu informatycznego Administratora Danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę Administratora Danych.

4. Wymiana danych i ich bezpieczeństwo

1. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach jednostek. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego Administratora Danych.

2. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.

3. Przed atakami z sieci zewnętrznej wszystkie komputery Administratora Danych (w tym także przenośne) chronione są środkami dobranymi przez Administratora Systemu Informatycznego (Informatyka) w porozumieniu z Inspektorem Ochrony Danych. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń.

4. Administrator Systemu Informatycznego (Informatyk) w porozumieniu z Inspektorem Ochrony Danych dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego Administratora Danych i powiększania bazy danych. Jednocześnie

należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

5. Należy stosować następujące sposoby kryptograficznej ochrony danych:
   - przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się tunelowanie oraz szyfrowanie połączenia,
   - przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron szyfrowanych protokołem SSL oznaczonych jako https://.

5. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator Systemu Informatycznego (Informatyk) po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.

Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Inspektora Ochrony Danych i Administratora Systemu Informatycznego (Informatyka).

6. Kontrola dostępu do sieci

1. System informatyczny posiada połączenie z publiczną siecią telekomunikacyjną (Internetem). Dostęp do niego jest jednak ograniczony na przy pomocy urządzenia UTM z włączoną ochroną FW (zapora ogniowa), IPS (system ochrony przed włamaniami), IDS (system detekcji włamań).

2. Administrator Danych blokuje dostęp inicjowany od strony sieci Internet do sieci Administratora Danych na urządzeniu UTM (FW, ograniczenia dostępu wyłącznie z określonych adresacji poprzez kanały szyfrowane). Uniemożliwia to dostęp do systemu przetwarzającego dane osobowe przez użytkowników sieci Internet.

3. Na jednostkach przetwarzających dane osobowe uruchomiona jest lokalna zapora sieciowa ang. firewall.

4. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

5. Operacje za pośrednictwem rachunku bankowego Administratora Danych może

wykonywać wyłącznie pracownik działu księgowości, upoważniony przez Wójta, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

7. Komputery przenośne i praca na odległość

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby Administratora Danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach, stosowanie własnych charakterystycznych toreb na laptopy nie jest dopuszczalne.

2. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych, ani też w samochodach.

3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.

4. Wykorzystywanie komputerów przenośnych Administratora Danych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.

5. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do Administratora Danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym Administratora Danych.

6. Administrator Systemu Informatycznego w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zabezpieczających danych przetwarzanych na komputerze przenośnym oraz określa zasady:

- postępowania w razie nieobecności w pracy dłuższej niż 5 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym Inspektora Ochrony Danych i uzgodnić z nim zwrot komputera przenośnego Administratorowi Danych;

- zwrotu sprzętu w razie zakończenia pracy u Administratora Danych.

7. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

8. Monitorowanie dostępu do systemu i jego użycia

System informatyczny Administratora Danych odnotowuje następujące zdarzenia:

1) daty pierwszego wprowadzenia danych do systemu,

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

Odnotowanie informacji, o których mowa w pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Administrator Systemu Informatycznego (Informatyk) przeprowadza synchronizację zegarów stacji roboczych z serwerem ntp, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez pracowników działu informatyki z konta o uprawnieniach administracyjnych.

System informatyczny Administratora Danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:

1) identyfikator użytkownika,

2) datę i czas zalogowania i wylogowania się z systemu,

3) zapisy udanych i nieudanych prób dostępu do systemu,

4) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych..

9. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Wszyscy pracownicy oraz osoby, które otrzymały pozytywną opinię Administratora Danych w Urzędzie Gminy Fajsławice (zabezpieczoną umową zapewniającą przestrzeganie przepisów dotyczących ochrony danych osobowych), pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych w Urzędzie Gminy Fajsławice danych osobowych oraz stosownych sposobach zabezpieczeń tych danych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

V. Przeglądy polityki ochrony danych osobowych i audyty systemu

Polityka ochrony danych osobowych powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych Inspektor Ochrony Danych może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

Inspektor Ochrony Danych analizuje, czy polityka ochrony danych osobowych i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) zmian w budowie systemu informatycznego,

2) zmian organizacyjnych Administratora Danych, w tym również zmian statusu osób

upoważnionych do przetwarzania danych osobowych,

3) zmian w obowiązującym prawie.

Inspektor Ochrony Danych po uzgodnieniu z Wójtem może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z Administratorem Systemu Informatycznego (Informatykiem). Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez Inspektora Ochrony Danych, jak i Administratora Systemu Informatycznego (Informatyka).

Wójt, biorąc pod uwagę wnioski Inspektor Ochrony Danych, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

VI. Postępowanie w wypadku klęski żywiołowej

Klęska żywiołowa jest katastrofą, spowodowaną działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczegółowych.

1. O zagrożeniu, jego skali i podjętych krokach zaradczych osoba kierująca ewakuacją zobowiązana jest powiadomić Inspektora Ochrony Danych. W razie niemożności skontaktowania się z nim zawiadamia Wójta Gminy.

2. Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełnienia obowiązku, o którym mowa w rozdziale polityki bezpieczeństwa informacji.

3. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których są dane osobowe, obowiązani są do przerwania pracy – w miarę możliwości przed opuszczeniem tych pomieszczeń do:

   - zamknięcia systemu informatycznego,

   - zabezpieczenia danych osobowych gromadzonych w kartotekach.

4. W czasie trwania akcji ratunkowej i po jej zakończeniu Inspektor Ochrony Danych oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczyć dane osobowe przed nieuprawnionym do nich dostępem.

5. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

VII. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik Administratora Danych, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, jest obowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Inspektora Ochrony Danych.

2. Inspektor Ochrony Danych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest obowiązany niezwłocznie:

- Poinformować Administratora Danych i stosować się do jego zaleceń;
- Zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji oraz jej treść o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu;

3. Administrator Systemu Informatycznego (Informatyk), który stwierdził fakt lub uzyskał informację o naruszeniu bezpieczeństwa danych osobowych w systemie informatycznym jest obowiązany niezwłocznie:

- Wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i godziną oraz podpisać;
- Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby nieuprawnionej do danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych;
- Podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony, w szczególności poprzez:
    a. Fizyczne odłączenie urządzeń i segmentów sieci, które mogły uniemożliwić dostęp do danych osobowych osobie nieuprawnionej,
    b. Wylogowanie użytkownika podejrzanego o naruszenie bezpieczeństwa danych osobowych,
    c. Zmianę hasła użytkownika, poprzez konto z którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby

uzyskania takiego dostępu;

- Dokonać szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia bezpieczeństwa danych osobowych;
- Przywrócić prawidłowe działanie systemu informatycznego służącego przetwarzaniu danych osobowych.

4. Po przywróceniu prawidłowego stanu, należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz podjąć kroki, mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

5. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym szkodliwym oprogramowaniem, należy ustalić źródło jego pochodzenia i utworzyć zabezpieczenia antywirusowe oraz organizacyjne, wykluczające podobne zdarzenia w przyszłości.

6. Inspektor Ochrony Danych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia naruszenia bezpieczeństwa danych osobowych i przekazuje go Administratorowi Danych. Jeżeli zdarzenie dotyczyło naruszenia zabezpieczeń systemu informatycznego, służącego przetwarzaniu danych osobowych to Inspektor Ochrony Danych w przygotowaniu raportu współpracuje z Administratorem Systemu Informatycznego (Informatykiem).

VIII. Postanowienia końcowe

Polityka ochrony danych osobowych jest dokumentem wewnętrznym Urzędu Gminy Sieciechów.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści. Wzór oświadczenia stanowi załącznik nr 9.

Polityka ochrony danych osobowych wchodzi w życie z dniem podpisania.

Regulamin Ochrony Danych Osobowych w Urzędzie Gminy Sieciechów

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. Użytkownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (komputerów, urządzeń biurowych, tabletów i smartfonów)
2. Demontaż, instalowanie lub podłączanie dodatkowych urządzeń jest zabronione
3. Użytkownik jest zobowiązany do usuwania tymczasowych plików z nośników/dysków z miejsc, gdzie dostęp do nich miałyby osoby nieupoważnione
4. Użytkownik jest zobowiązany do przekazania informatykowi nośników przeznaczonych do zniszczenia

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik komputerów, programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie. Zabronione jest udostępnianie konta innemu użytkownikowi
2. Użytkownik nie może zmieniać swoich uprawnień, np. zostać Administratorem na swoim komputerze
3. Użytkownik komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu
5. Użytkownik przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
6. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
7. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe
8. Administrator prowadzi monitoring użytkowania komputerów służbowych, w tym kontrola Internetu, monitorowanie wydruków, monitoring stron internetowych, monitoring działań użytkowników.

3 POLITYKA HASEŁ

1. Hasła powinny składać się z min. 8 znaków
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić

6. Hasła muszą być zmieniane co 30 dni
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu na klucz) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób postronnych
2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach
3. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik

5 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA FIRMĘ/ORGANIZACJĘ

1. Użytkownicy nie mogą wynosić na zewnątrz niezaszyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD, pamięci typu Flash)
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski przenośne, zahasłowane pliki, zabezpieczone smartfony)
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach w celu zabezpieczenia ich przed zagubieniem i kradzieżą

6 ZASADY KORZYSTANIA Z INTERNETU

1. Zabrania się instalowania programów z Internetu bez konsultacji z informatykiem
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez takie oprogramowanie
3. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem do pobrania oraz na hackerskie
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Pliki z danymi osobowymi w Wordzie, Excelu, w Pdf lub spakowane (7zip), przed wysłaniem ich do osób trzecich powinny być zahasłowane lub podpisane elektronicznym podpisem kwalifikowanym lub profilem zaufanym.
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
4. Należy zgłaszać informatykowi przypadki podejrzanych emaili
5. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"
6. Użytkownicy powinni okresowo kasować niepotrzebne maile

8 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora/IOD/Informatyka w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Do sytuacji wymagających powiadomienia, należą:
   - niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
   - niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
   - nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:
   - zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
   - zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
   - umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:
   - ślady na drzwiach, oknach i szafach wskazują na próbę włamania
   - dokumentacja jest niszczona bez użycia niszczarki
   - fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
   - otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
   - ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
   - wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz Urzędu Gminy Fajsławice bez upoważnienia
   - udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
   - telefoniczne próby wyłudzenia danych osobowych
   - kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi
   - maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   - pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów

- hasła do systemów przyklejone są w pobliżu komputera

9 Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:
   - przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań
   - zachowania w tajemnicy danych osobowych do których ma dostęp
   - niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań
   - zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem

10 Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów karnych zawartych w RODO z dnia 27 kwietnia 2016 r.

Instrukcja zarządzania RODO

Urząd Gminy SIECIECHÓW

1. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych

2. Zabezpieczenia fizyczne

1. drzwi do pomieszczeń biurowych, archiwów zamykane są na klucz
2. drzwi do serwerowni zamykane są na klucz
3. dokumentację papierową i nośniki elektroniczne przechowywaną w pomieszczeniach zabezpieczono w szafach zamykanych na klucz
4. stosowany jest monitoring
5. zapewniono ochronę obiektu
6. wdrożono system kontroli dostępu

3. Zabezpieczenia techniczne

1. zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu
2. serwerownia wyposażona w gaśnice
3. powiadamianie Informatyka o alertach temperatury serwerowni
4. ochrona przed skutkami pożaru
5. klimatyzacja w serwerowni
6. zasilanie serwerowni przez UPS
7. zabezpieczenie infrastruktury technicznej z siecią teleinformatyczną i jej zasilaniem

4. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemów informatycznych nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu)
2. Nadawanie, zmiana, odbieranie uprawnień użytkownika do systemów informatycznych odbywa się na polecenie przełożonych (lub innych osób upoważnionych)
3. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada Administrator
4. Obowiązuje zasada minimalizacji uprawnień. Zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub utrata upoważnienia są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu oraz unieważnienia hasła i odnotowanie tego faktu w ewidencji upoważnień.
5. Informatyk jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów pracowników oraz kont w systemach, za które są odpowiedzialni pracownicy.
6. Pracownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi

sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.

7. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.

5. Metody i środki uwierzytelnienia (polityka haseł)

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione. Identyfikatory i hasła są sposobem zagwarantowania rozliczności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.

1. Standard hasła: hasło 8 –znakowe, zmieniane co 30 dni. Użytkownicy są zobowiązani do samodzielnej zmiany hasła. Hasła stanowią tajemnicę służbową, znaną wyłącznie temu pracownikowi.

2. Należy pamiętać że to pracownik ponosi pełna odpowiedzialność za utworzone hasło dostępu i jego przechowywanie. Zakazane jest przechowywanie haseł w widocznym miejscu, automatycznych procesach logowania.

3. Wszystkie konta dostępowe do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Informatyka sposobem uwierzytelniania.

4. Hasła nie mogą być takie same jak identyfikator użytkownika. Nie używa się haseł wykorzystanych.

5. Hasła dla użytkowników o wysokich uprawnieniach mogą być wykorzystane tylko w uzasadnionych przypadkach i fakt ten powinien zostać udokumentowany.

6. Hasła administracyjne zdeponowane są w bezpiecznym miejscu

7. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp

8. Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stację roboczą. Kończąc pracę użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy.

6. Wymagania dotyczące sprzętu i oprogramowania

1. Wygaszacz stacji roboczej powinien być skonfigurowany w taki sposób, aby aktywował się automatycznie po upływie 10 minut od ostatniego użycia stacji roboczej, uruchamiając blokadę stacji roboczej, wymuszającą ponowne zalogowanie.
2. Ekrany monitorów należy ustawić w taki sposób by uniemożliwić osobom postronnym wgląd lub spisanie, sfotografowanie aktualnie wyświetlanej informacji na ekranie monitora.
3. Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
4. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.

7. Procedura tworzenia kopii zapasowych

W celu zapewnienia bezpieczeństwa przetwarzania danych osobowych istnieje obowiązek tworzenia kopii zapasowych. Proces tworzenia kopii zapasowych nadzoruje Administrator.

1. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest Informatyk.
2. Kopie zapasowe systemów przetwarzających dane osobowe są codziennie zapisywane na osobnych dyskach odpowiednich serwerów. Zapis odbywa się w godzinach 21 - 3, a w dniu następnym są sprawdzane i kopiowane na dodatkowe urządzenia – serwery służące do przechowywania danych.
3. Nośniki kopii zapasowych oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.
4. Nośniki z kopiami zapasowymi przechowywane są w sejfie w osobnej lokalizacji.
5. Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.
6. Informatyk określa czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych.
7. Informatyk odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego. Po odtworzeniu systemu informatycznego Informatyk odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.

8. Informatyk przeprowadza weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych. Weryfikacja taka powinna być przeprowadzana nie rzadziej niż raz na pół roku.

8. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki są niszczone w sposób fizyczny
2. Nośniki informacji muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji
3. Dokumentacja papierowa niszczona jest w niszczarkach

9. Procedura zabezpieczenia systemu informatycznego

9.1. Bezpieczeństwo przetwarzania danych poza Urzędem Gminy

1. Stosuje się szyfrowanie dysków komputerów przenośnych zawierających dane osobowe, jeśli wynoszone są poza obszar Urzędu Gminy
2. Dane osobowe na komputerach przenośnych wynoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach
3. Dyski przenośne / pendrive wynoszone poza Urząd Gminy muszą być zaszyfrowane
4. Sprzęt mobilny (smartfony/tablety) zabezpieczono mechanizmem uwierzytelniania
5. Sprzęt mobilny wyposażony jest w oprogramowanie umożliwiające jego nadzór, blokowanie dostępu, czyszczenie zawartości
6. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem VPN przez Informatyka
7. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet uwierzytelnienia dokonuje się z użyciem loginu i podania hasła

9.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów

1. Dokonuje się konfiguracji urządzeń sieciowych oraz sprzętu IT w celu zabezpieczenia przed nieuprawnionym dostępem do nich
2. Dokonuje się aktualizacji oprogramowania systemów i aplikacji.
3. Stosowany jest monitoring usług sieciowych w celu deaktywacji nieużywanych
4. Zastosowano system antywirusowy i filtr antyspamowy
5. Stosowany jest Firewall
6. Zastosowano mechanizmy kontroli dostępu do sieci.

9.3. Zabezpieczenia infrastruktury IT

1. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

2. uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Urzędzie Gminy Sieciechów;
3. samowolnego korzystania z nośników przenośnych;
4. otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z Informatykiem;
5. korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
6. podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.
7. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić Informatyka. Do objawów powyższych można zaliczyć:
   - istotne spowolnienie działania systemu informatycznego;
   - nietypowe działanie aplikacji;
   - nietypowe komunikaty;
   - utratę danych lub modyfikację danych.
8. system informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
   - oprogramowanie antywirusowe;
   - zaporę sieciową;
   - aktualizację oprogramowania systemowego;
   - konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.
9. Informatyk jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:
   - weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych;
   - weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych;
   - przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych;
   - weryfikację poprawności aktualizacji oprogramowania systemowego.

10. Procedura wykonywania przeglądów i konserwacji

1. Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników oraz przez podmioty zewnętrzne.
2. Prace serwisowe wykonywane na terenie Urzędu Gminy Sieciechów przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi Informatyka.
3. Przekazanie sprzętu teleinformatycznego do naprawy poza teren Urzędu Gminy Sieciechów jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:
   - sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem;
   - przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.
4. Protokoły, o których mowa w punkcie 3, lub ich kopie przechowywane są przez Administratora.
5. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:
   - wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem;
   - wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu Gminy Sieciechów ;
   - przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu);
   - zakres prac serwisowych i ich wynik;
   - czas przeprowadzania prac serwisowych.

WYKAZ BUDYNKÓW, POMIESZCZEŃ lub części pomieszczeń TWORZĄCYCH OBSZAR < W KTÓRYCH SĄ PRZETWARZANE, PRZECHOWYWANE, NISZCZONE DANE OSOBOWE W UZRZĘDZIE GMINY W SIECIECHOWIE

a/ pomieszczenia znajdujące się w budynku Jednostki przy ul. Rynek 16

- (biura) pokoje nr : 1,2, 3, 4,5, 6,7, 8, 9,10,11,12

b/ budynek przy ul. 11 Listopada 2 Gminna Biblioteka Publiczna 1, 2

- (biura) pokoje nr : GOPS 3,4 GK 6 , Księgowość Oświatowa 10

Załącznik nr 7 do Polityki Ochrony Danych Osobowych

Rejestr naruszeń ochrony danych osobowych

Lp.	Naruszenie	Data i godzina zgłoszenia podejrzenia naruszenia	Data i godzina stwierdzenia naruszenia	Data naruszenia (okres, którego dotyczy)	Kategoria i liczba osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Osoba/źródło informacji o zdarzeniu	Miejsce naruszenia	Okoliczności naruszenia-opis charakteru naruszenia, analiza zdarzenia, przyczyna wystąpienia	Opis skutków naruszenia	Osoba/jednostka odpowiedzialna za naruszenie	Podjęte działania naprawcze	Rezultat działań naprawczych	Ryzyko naruszenia praw lub wolności osób fizycznych	Obowiązek poinformowania Prezesa Urzędu Ochrony Danych Osobowych

Załącznik nr 8 do Polityki Ochrony Danych Osobowych

.....
(Miejscowość, data)

.....
(Sygnatura)

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych

1. Data: ..... Godzina:.....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

.....

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika, jeśli występuje)

3. Lokalizacja zdarzenia:

.....

.....

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

5. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

6. Podjęte działania:

.....

.....

Załącznik nr 9 do Polityki Ochrony Danych Osobowych

Sieciechów, dn. .....

.....
(imię i nazwisko)

.....
(stanowisko służbowe)

OŚWIADCZENIE

Oświadczam, iż zostałam/zostałem* zaznajomiona/zaznajomiony* z przepisami dotyczącymi ochrony danych osobowych, w szczególności 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, wprowadzonymi i wdrożonymi na jego podstawie do stosowania przez Administratora Danych „Polityką ochrony danych osobowych" oraz „Instrukcją zarządzania RODO" w Urzędzie Gminy Sieciechów.

Jednocześnie zobowiązuję się do ich przestrzegania.

.....
(podpis osoby składającej oświadczenie)

* niepotrzebne skreślić

.....

.....

7. Skutki zdarzenia:

.....

.....

.....

.....

8. Postępowanie wyjaśniające:

.....

.....

.....

.....

.....
(podpis Administratora Danych Osobowych)

Załącznik Nr 4
do Zarządzenia Nr 45/2018
z dnia 9 sierpnia 2018

Sieciechów dnia 2018r
(miejscowość, data

.....
(pieczęć jednostki organizacyjnej)

Nr rej. /2018

Upoważnienie do przetwarzania danych osobowych

Działając jako Administrator Urzędu Gminy Sieciechów na podstawie art.29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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(Dz.U.UE.L.2016.119.1)-dalej- **„RODO", niniejszym:**

1.upoważniam do przetwarzania danych osobowych ,których administratorem w rozumieniu art.4 pkt 7 RODO jest Wójt Gminy Sieciechów lub które zostały powierzone administratorowi do przetwarzania.:

(imię i nazwisko)

Zatrudnionego/nej w na stanowisku inspektora w **Urzędzie Gminy w Sieciechowie** ,
(oznaczenie jednostki i komórki organizacyjnej)

do przetwarzania, w ramach wykonywanych obowiązków służbowych, niżej wymienionych zbiorów danych osobowych w okresie: od .2018r do; bezterminowo:

l.p.	Nazwa zbioru	Postać zbioru	Nazwa programu	Identyfikator
1.				
2.				
3.				
4.				

Wymieniona osoba zostaje wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Gminy w Sieciechowie

Rozwiązanie stosunku pracy jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych w Urzędzie Gminy w Sieciechowie

(pieczęć i podpis administratora danych)

Wykonano w 3 egzemplarzach:
Egz. Nr 1 – pracownik
Egz. Nr 2 – akta personalne pracownika
Egz. Nr 3 – Inspektor Ochrony Danych Osobowych

Otrzymałam/em dnia .....
Podpis pracownika .....