ZARZĄDZENIE NR 66/2018
WÓJTA GMINY SŁAWNO

z dnia 25 maja 2018 r.

w sprawie Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Sławno

Na podstawie art. 24 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) (Dz. Urz. UE. L. Nr 119, str. 1) w związku z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, z 2018 r. poz. 138, 723 i 1000), § 3-5 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 (Dz. U. Nr 100, poz. 1024) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r. poz. 994, 1000) zarządzam, co następuje:

§ 1. W Urzędzie Gminy Sławno wprowadza się:

1) Politykę Bezpieczeństwa, stanowiącą załącznik nr 1 do niniejszego zarządzenia;

2) Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2. Dokumenty, o których mowa w § 1 mają zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Urzędu Gminy Sławno.

§ 3. Zobowiązuje się wszystkich pracowników Urzędu Gminy Sławno do zapoznania się z niniejszym zarządzeniem oraz do przestrzegania zasad zawartych w dokumentach, o których mowa w § 1.

§ 4. Wykonanie zarządzenia powierza się kierownikom referatów Urzędu Gminy Sławno.

§ 5. Traci moc Zarządzenie Nr 79/2016 Wójta Gminy Sławno z dnia 8 lipca 2016 roku w sprawie wprowadzenie Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Sławno.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Sławno

Ryszard Stachowiak

Załącznik Nr 1
do Zarządzenia Nr 66/2018
Wójta Gminy Sławno
z dnia 25 maja 2018 r.

POLITYKA BEZPIECZEŃSTWA w URZĘDZIE GMINY SŁAWNO

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia 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) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur.

Powyższy wstęp określa założenia ustawodawcy przewidziane w art. 47 oraz art. 51 Konstytucji RP jak również treść art. 32 rozporządzenia ogólnego o ochronie danych osobowych, który nakazuje każdemu administratorowi danych wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanemu ryzyku.

I. INFORMACJE OGÓLNE

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Urzędzie Gminy Sławno.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych metodami tradycyjnymi oraz w systemach informatycznych wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

CEL POLITYKI BEZPIECZEŃSTWA

§ 1. Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką wraz z Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych stanowi Politykę ochrony danych osobowych w świetle art. 22 ust. 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 (ogólne rozporządzenie o ochronie danych).

§ 2. 1. Polityka jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora – Gminę Sławno - Urząd Gminy Sławno, w imieniu którego działa Wójt Gminy Sławno i stanowi jeden ze środków organizacyjnych, mających na celu zgodne z prawem przetwarzanie danych osobowych, a także usprawnienie i usystematyzowanie organizacji pracy.

2. Polityka została opracowana i wdrożona w strukturze Administratora w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016. 119. 1);
2) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. Nr 1000 z późn. zm.) oraz
3) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.).

§ 3. Polityka ma zastosowanie do wszystkich pracowników Administratora, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z procedurami bezpieczeństwa danych, opisanymi w niniejszej Polityce i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, te złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

§ 4. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki winny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz pełnej realizacji praw osób, których dane dotyczą.

STOSOWANA TERMINOLOGIA

§ 5. Stosowane w niniejszej Polityce bezpieczeństwa terminy to:

1) **Administrator lub Administrator Danych Osobowych (ADO)** – Urząd Gminy Sławno, reprezentowany przez Wójta Gminy Sławno,
2) **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez ADO, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych, wykorzystywanych przez ADO,
3) **bezpieczeństwo informacji –** zachowanie poufności, integralności i dostępności informacji,

4) **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Dane osobowe są gromadzone, przechowywane, edytowane, archiwizowane w rejestrach, kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Urzędu Gminy Sławno, w dokumentach papierowych, jak również w systemach informatycznych i na elektronicznych nośnikach informacji,
5) **dostępność –** zapewnienie upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami,
6) **DPIA** *(Data Protection Impact Assessment)* – ocena skutków dla ochrony danych osobowych,
7) **Inspektor Ochrony Danych (IOD) –** osoba wyznaczona przez ADO, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora,
8) **integralność –** właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
9) **kierownik komórki organizacyjnej** – kierownik referatu Urzędu Gminy Sławno,
10) **organ nadzorczy** – niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania obowiązujących przepisów w zakresie ochrony danych osobowych; w Polsce jest to Urząd Ochrony Danych Osobowych, z siedzibą w Warszawie, ul. Stawki 2, 00-193 Warszawa, zwany dalej UODO,
11) **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego,
12) **podmiot przetwarzający lub procesor** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,
13) **Polityka** – niniejsza Polityka bezpieczeństwa,
14) **poufność** – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
15) **pracownik** – osoba współpracująca z ADO na podstawie umowy o pracę lub umowy cywilnoprawnej (zlecenie, dzieło), w tym również wolontariusz, praktykant, stażysta, serwisant, itp.,
16) **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

17) **RODO lub rozporządzenie** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. poz. 119) (Dz. U. UE. L. 2016. 119. 1),
18) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania i narzędzi programowych stosowanych w celu przetwarzania danych osobowych elektronicznie,
19) **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, takich jak np. wyposażenie, sprzęt, urządzenia umożliwiający przetwarzanie danych osobowych na papierze,
20) **Unia lub UE** – Unia Europejska,
21) **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.) oraz w obowiązującym zakresie ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. Nr 922 z późn. zm.),
22) **uwierzytelnianie –** weryfikacja tożsamości użytkownika,
23) **użytkownik systemu lub użytkownik systemu informatycznego** – upoważniony przez ADO, wyznaczony do przetwarzania danych osobowych pracownik, który odbył niezbędne przeszkolenie w zakresie ochrony danych osobowych oraz zobowiązał się do przestrzegania wymaganych procedur oraz zachowania w tajemnicy danych, do których ma dostęp obecnie i w przyszłości,
24) **zabezpieczenie danych w systemie informatycznym** – wdrożone i eksploatowane, stosowne środki techniczne i organizacyjne, zapewniające ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem,
25) **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie, w szczególności zgromadzony w bazach danych programów albo dziennikach, kartotekach, wykazach, zestawieniach, rejestrach i ewidencjach,
26) **zgoda osoby, której te dane dotyczą** to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

INFORMACJE OBJĘTE POLITYKĄ ORAZ ZAKRES ZASTOSOWANIA

§ 6. 1. Polityka opisuje zasady i procedury przetwarzania danych osobowych w Urzędzie Gminy Sławno w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych. Jest zestawem praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych. Odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie (na papierze), jak i danych przetwarzanych w systemach informatycznych (w formie elektronicznej).

2. Politykę stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w niniejszej Polityce.

3. Rygorowi Polityki podlegają także dane powierzone ADO do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi udostępnione.

II. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

§ 7. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych w Urzędzie Gminy Sławno odpowiadają:

1) Administrator, zwany Administratorem Danych Osobowych (ADO);
2) Inspektor Ochrony Danych (IOD) w zakresie nadzoru i monitorowania przestrzegania niniejszej Polityki;
3) Administrator Systemów Informatycznych (ASI) w zakresie nadzoru i monitorowania przestrzegania niniejszej Polityki;
4) wszyscy pracownicy Urzędu Gminy Sławno, tj. kierownicy komórek organizacyjnych i osoby upoważnione do przetwarzania danych osobowych oraz posiadające zgodę na przebywanie w obszarze przetwarzania danych osobowych w zakresie powierzonych im obowiązków, uprawnień, odpowiedzialności, upoważnień i pełnomocnictw.

ADMINISTRATOR DANYCH OSOBOWYCH

§ 8. ADO wyznacza IOD i ASI oraz upoważnia poszczególnych pracowników do przetwarzania danych osobowych oraz wyraża zgodę na przebywanie osób w obszarze przetwarzania danych osobowych.

§ 9. ADO jest odpowiedzialny za:

1) zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
2) wdrożenie odpowiednich procedur ochrony danych osobowych,
3) jeśli uzna to za konieczne, stosowanie kodeksów postępowania lub mechanizmów certyfikacji, jako elementu dla stwierdzenia przestrzegania ciążących na nim obowiązków,
4) zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą,
5) prowadzenie rejestru czynności przetwarzania danych osobowych,
6) prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
7) współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
8) wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
9) zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
10) dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
11) zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultacje z organem nadzorczym,

12) nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
13) zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,
14) w stosunku do IOD:
    a) zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
    b) wspieranie w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,
    c) zagwarantowanie, by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
    d) publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

§ 10. Administrator nadzoruje działania IOD oraz ASI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.

§ 11. ADO każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania IOD oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona ustnie lub w formie wiadomości e-mail.

INSPEKTOR OCHRONY DANYCH

§ 12. Funkcję IDO pełni osoba wyznaczona przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.

§ 13. Do zadań IOD należy:
1) informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
2) monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
3) monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
4) doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem a podmiotem przetwarzającym lub pomiędzy pracownikami ADO),
5) działania zwiększające świadomość pracowników ADO w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
6) szkolenia dla pracowników uczestniczących w operacjach przetwarzania danych,
7) przeprowadzanie sprawdzeń i kontroli w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
8) udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
9) współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,
10) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

§ 14. Funkcję ASI pełni osoba zatrudniona na stanowisku informatyka, wyznaczona przez Administratora.

§ 15. Do zadań ASI należy w szczególności:

1) prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
2) opracowywanie oraz aktualizacja ogólnego opisu technicznych środków bezpieczeństwa wdrożonych w strukturze ADO,
3) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
4) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
5) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
6) sprawowanie nadzoru nad kopiami zapasowymi danych,
7) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
8) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
9) dokonywanie cyklicznych przeglądów, prowadzenie uaktualnień i stosowanie procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów,
10) ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 16. 1. ADO realizując niniejszą Politykę w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym i/lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.

2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu wstępnego szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze ADO.

3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie w formie pisemnej, potwierdzonej przez osobę otrzymującą.

4. Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik Nr 1 do Polityki.

5. ADO prowadzi ewidencję wydanych upoważnień do przetwarzania danych osobowych, której wzór stanowi Załącznik Nr 2 do Polityki.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 17. 1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, ustawy oraz postanowieniami Polityki i Instrukcji Zarządzania Systemem Informatycznym.

2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o zapoznaniu się z obowiązującymi przepisami prawa w tym zakresie i instrukcjami oraz o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera składane oświadczenie, którego wzór stanowi Załącznik Nr 3 do niniejszej Polityki.

3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r. Nr 917 z późn. zm.) bądź rozwiązania stosunku cywilnoprawnego.

§ 18. Kierownicy referatów Urzędu Gminy Sławno oraz Sekretarz, Skarbnik, Zastępca Wójta:

1) zobowiązani są do stałego nadzoru i przestrzegania zapisów Polityki, w tym przez podległych pracowników,
2) przetwarzają dane osobowe w sposób określony w „Rejestrze czynności przetwarzania danych osobowych" i „Rejestrze kategorii czynności przetwarzania danych osobowych",
3) zobowiązani są do zgłoszenia IOD planowanego tworzenia nowych zbiorów danych oraz informowania IOD o zmianach, dotyczących przetwarzania zbiorów danych już zdefiniowanych,
4) zobowiązani są do zgłaszania IOD pracowników, którzy będą przetwarzać dane osobowe w celu wstępnego przeszkolenia oraz wydania upoważnienia do przetwarzania danych osobowych i nadania uprawnień do określonych systemów / zbiorów danych jak również zgłaszania pracowników, którzy posiadali upoważnienie do przetwarzania danych osobowych, a zakończyli swoją pracę w Urzędzie albo pracowników, którzy posiadali uprawnienie dostępu, a zmiana ich zakresu obowiązków spowodowała konieczność cofnięcia uprawnień do przetwarzania danych osobowych lub określonych zbiorów danych, wg wzoru określonego w Załączniku Nr 4 do Polityki,
5) zobowiązani są do zgłaszania IOD wszystkich przypadków naruszeń bezpieczeństwa informacji lub też nienależytego zabezpieczenia zbiorów danych,
6) zobowiązani są do informowania IOD o wszystkich zmianach przepisów prawa, mających wpływ na sposób przetwarzania danych osobowych będących w dyspozycji pracowników i o zmianach w organizacji pracy referatu, mających wpływ na bezpieczeństwo przetwarzanych danych.

§ 19. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w celu wykonywania nałożonych na nią obowiązków służbowych, zgodnych z posiadanym zakresem obowiązków, a rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,
2) musi zachować w tajemnicy dane osobowe oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia w Urzędzie, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki i Instrukcji Zarządzania Systemem Informatycznym,
4) stosuje określone przez IOD procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych,

5) korzysta z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników,
6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym,
7) zabezpiecza indywidualne hasła dostępu do zbiorów danych osobowych przed dostępem osób trzecich.

OSOBY POSIADAJĄCE ZGODĘ NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

§ 20. 1. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne wyłącznie:
1) za pisemną zgodą ADO lub
2) na podstawie odrębnych umów dotyczących powierzenia przetwarzania danych osobowych w myśl art. 28 RODO albo
3) w obecności osoby upoważnionej do przetwarzania danych osobowych.

2. Obszar przetwarzania danych osobowych, o którym mowa w ust. 1 to pomieszczenia, w tym pomieszczenia biurowe Urzędu Gminy Sławno, w których przetwarzane są dane osobowe, których wykaz stanowi Załącznik Nr 5 do Polityki.

3. Przez osoby nieuprawnione, o których mowa w ust. 1 rozumie się zarówno pracowników ADO jak i osoby oraz podmioty świadczące usługi na rzecz ADO, w tym serwisantów, monterów, osoby sprzątające, ochronę, itp. oraz klientów Urzędu Gminy Sławno.

4. Osoba posiadająca zgodę na przebywanie w obszarze przetwarzania danych osobowych, wydaną przez ADO zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, a naruszenie obowiązku ochrony danych osobowych skutkuje poniesieniem odpowiedzialności karnej lub cywilnoprawnej, zgodnie z odrębnymi przepisami.

5. Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych stanowi Załącznik Nr 6 do niniejszej Polityki.

6. ADO prowadzi ewidencję wydanych zgód dla osób upoważnionych do przebywania w obszarze przetwarzania danych osobowych, której wzór stanowi Załącznik Nr 7 do Polityki.

III. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

§ 21. 1. Przetwarzanie danych osobowych w strukturze ADO odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:
1) zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO *(zasada legalności),*
2) w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą *(zasada rzetelności)*,
3) w sposób przejrzysty dla osób, których dane dotyczą *(zasada przejrzystości)*,
4) w konkretnych, wyraźnych i prawnie uzasadnionych celach *(zasada ograniczenia celu),*
5) w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane *(zasada minimalizacji danych),*
6) przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania *(zasada prawidłowości),*

7) przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane *(zasada ograniczenia przechowywania),*
8) w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych *(zasada integralności i poufności),*
9) w udokumentowany sposób *(zasada rozliczalności)*.

2. ADO gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia ich zgodności z ogólnymi zasadami przetwarzania danych.

3. Dane są przetwarzane wyłącznie w celach, dla których zostały zebrane, w sytuacji, gdy:
1) ich przetwarzanie jest wymagane przepisami prawa,
2) dane zostały uzyskane od osoby, której dotyczą i wyraziła ona zgodę na ich przetwarzanie,
3) w sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

4. Ocena niezbędności przetwarzania danych do wypełnienia celów ADO powinna być dokonywana indywidualnie w każdej sytuacji.

OBOWIĄZEK INFORMACYJNY

§ 22. W przypadku zbierania danych osobowych od osoby, której one dotyczą w celu zapewnienia rzetelności i przejrzystości przetwarzania danych ADO informuje tę osobę o:
1) adresie swojej siedziby, pełnej nazwie, danych kontaktowych oraz danych kontaktowych do IOD,
2) celu i podstawie prawnej przetwarzania danych, a w szczególności o kategoriach odbiorców danych, ewentualnej możliwości przekazania danych do państwa trzeciego lub organizacji międzynarodowej, okresie przechowywania lub kryteriach ustalenia okresu przechowywania danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania, sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
4) możliwości cofnięcia wyrażonej zgody na przetwarzanie danych osobowych oraz konsekwencjach niepodania danych, bez względu na to czy jest to warunek ustawowy czy na zasadzie dobrowolności,
5) jeśli ma to zastosowanie o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu,
6) prawie wniesienia skargi do organu nadzorczego.

§ 23. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą ADO podaje osobie, której dane dotyczą informacje o:
1) adresie swojej siedziby, pełnej nazwie, danych kontaktowych oraz danych kontaktowych do IOD,
2) celu, kategoriach danych osobowych i podstawie prawnej przetwarzania danych, a w szczególności o kategoriach odbiorców danych, ewentualnej możliwości przekazania danych do państwa trzeciego lub organizacji międzynarodowej, okresie przechowywania lub kryteriach ustalenia okresu przechowywania danych,
3) źródle pochodzenia danych,
4) prawie dostępu do treści swoich danych oraz ich poprawiania, sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,

5) jeśli ma to zastosowanie o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu,
6) prawie wniesienia skargi do organu nadzorczego.

§ 24. Usunięcie danych osobowych nie wymaga zgody osoby, której dane dotyczą.

§ 25. Jeżeli ADO planuje przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje osobę, której dane dotyczą, o tym celu oraz udziela jej wszelkich informacji, o których mowa w § 22.

§ 26. 1. Informacje, o których mowa w § 22-23, z zastrzeżeniem ust. 2 ADO podaje:
1) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych,
2) przy pierwszej komunikacji z osobą, której dane dotyczą lub przy pierwszym ujawnieniu danych osobowych innemu odbiorcy,
3) w sposób jasny i łatwy do zrozumienia, w zależności od rzeczywistych potrzeb: ustnie, telefonicznie, pisemnie, e-mailem, na stronach internetowych i BIP lub na tablicach informacyjnych, itp. z zastosowaniem m.in. opracowanych klauzul informacyjnych.

2. § 22-23 nie mają zastosowania, gdy:
1) osoba, której dane dotyczą, dysponuje już tymi informacjami,
2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku lub uniemożliwiłoby realizację celów przetwarzania, przy zapewnieniu ochrony praw osoby, której dane dotyczą,
3) pozyskiwanie lub ujawnianie danych jest uregulowane prawem,
4) dane osobowe muszą pozostać poufne, zgodnie z odrębnymi przepisami.

§ 27. 1. Obowiązek informowania osób, których dane są przetwarzana w sposób i na zasadach określonych w § 22-26, ADO nakłada na wszystkie osoby zatrudnione w Urzędzie Gminy Sławno, biorące udział w przetwarzaniu danych osobowych.

2. Bezpośredni nadzór nad przetwarzaniem danych osobowych i realizacją obowiązku informacyjnego sprawują kierownicy komórek organizacyjnych Urzędu Gminy Sławno, zgodnie z zakresami obowiązków.

ZAKRES PRZETWARZANIA DANYCH OSOBOWYCH

§ 28. 1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Urzędu Gminy Sławno w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (systemy, bazy danych, programy).

2. Wykaz zbiorów ewidencyjnych dla danych osobowych, zawierający ich strukturę oraz narzędzia stosowane w procesie przetwarzania zawiera Załącznik Nr 8 do Polityki.

§ 29. 1. Ze względu na rodzaj i charakter przetwarzanych danych osobowych w Urzędzie Gminy Sławno przetwarza się dwie kategorie danych:
1) dane osobowe tzw. „zwykłe” – wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych, takie jak: imię i nazwisko, adres zamieszkania, PESEL, numer i seria dowodu osobistego, numer i seria paszportu (jako innego dokumentu tożsamości), NIP, numer konta bankowego, numer działki ewidencyjnej gruntu (oraz jej bonitacja i powierzchnia), numer księgi wieczystej dla nieruchomości, dane o stanie posiadania nieruchomości (wielkość, powierzchnia, rodzaj zabudowy), numer telefonu, adres poczty elektronicznej, identyfikator internetowy w postaci numeru IP, adres strony internetowej, konto epuap, konta pozostałych serwisów, w tym kont społecznościowych, dane o stanie ekonomicznym, wizerunek osoby fizycznej,

2) dane osobowe szczególnych kategorii – tzw. „dane wrażliwe” przetwarzane w oparciu o zapisy art. 9 RODO, tj. dane ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne (ewidencja ludności), dane dotyczące zdrowia, seksualności lub orientacji seksualnej, dane dotyczące stanu majątkowego, stanu zdrowia, historii leczenia gromadzone w przypadkach np. postępowań w sprawach ulg i umorzeń czy związanych ze zwalczaniem uzależnień albo ujawniające treść orzeczeń o skazaniu, ukaraniu, mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

2. Dane, o których mowa w ust. 1 przetwarzane są zarówno w przypadku osób fizycznych – petentów Urzędu Gminy Sławno jak i pracowników.

§ 30. 1. ADO prowadzi:

1) rejestr czynności przetwarzania danych osobowych;
2) rejestr kategorii czynności przetwarzania danych osobowych, dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych;

o których mowa w odrębnych przepisach.

2. ADO prowadzi rejestry, o których mowa w ust. 1 w formie papierowej lub elektronicznej.

3. ADO udostępnia rejestry, o których mowa w ust. 1 na żądanie organu nadzoru.

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

§ 31. ADO realizując niniejszą Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi wyłącznie na drodze powierzenia przetwarzania danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych.

§ 32. 1. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu ADO jest konieczność realizacji zadań przez podmiot zewnętrzny zapewniający wystarczające gwarancje ochrony danych.

2. Zawierana przez ADO umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO.

3. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.

§ 33. W przypadku, gdy elementy niezbędne do powierzenia przetwarzania danych osobowych znajdują się w treści umowy podstawowej zawartej z podmiotem przetwarzającym dane, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.

§ 34. 1. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiadają wszyscy pracownicy Urzędu Gminy Sławno, zgodnie z kompetencjami.

2. Przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym dane osobowe każdy z pracowników merytorycznych Urzędu Gminy Sławno jest zobowiązany poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych.

3. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji ADO lub udzielonymi pełnomocnictwami.

§ 35. 1 Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.

2. ADO ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.

§ 36. ADO w zakresie prowadzonej przez siebie działalności może przetwarzać dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi, a przyjęcie danych w powierzenie przez ADO musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

UDOSTĘPNIANIE DANYCH OSOBOWYCH

§ 37. 1. ADO dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

§ 38. 1. Przekazywanie danych osobowych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.
2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych jak i udostępnienia danych osobowych w przypadkach, gdzie zastosowanie mają § 31-37 Polityki.
§ 39. 1. Przekazanie danych osobowych do państwa trzeciego może nastąpić w sytuacji, gdy Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony – bez specjalnego zezwolenia.
2. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w ust. 1, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy ADO samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.
3. Odpowiednie zabezpieczenia, o których mowa w ust. 2 ADO zapewnia za pomocą:
1) prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,
2) wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,
3) standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,
4) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,
5) zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub
6) zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

4. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w ust. 3 ADO może zapewnić w szczególności za pomocą:
1) klauzul umownych między ADO lub podmiotem przetwarzającym a ADO, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub
2) uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

§ 40. 1. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez ADO do państwa trzeciego pomimo braku decyzji Komisji Europejskiej oraz zapewnienia odpowiednich zabezpieczeń pod warunkiem, że:
1) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,
2) przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
3) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,
4) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego lub posiadane roszczenia,
5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub
6) przekazanie nastąpi z publicznego rejestru.

2. Pracownik Urzędu Gminy Sławno przed planowanym przekazaniem danych do państwa trzeciego jest zobowiązany poinformować o tym IOD oraz skonsultować z nim warunki przekazania tych danych.

WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

§ 41. ADO dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.

§ 42. 1. Współadministrowanie danymi może zachodzić wówczas, gdy ADO oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych, a w procesie przetwarzania danych osobowych są spełnione równocześnie następujące warunki:
1) ADO i inny podmiot są administratorami w rozumieniu art. 4 pkt 7 RODO,
2) ADO i inny podmiot wspólnie ustalą cele przetwarzania danych,
3) ADO i inny podmiot wspólnie ustalą sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.

2. W przypadku spełnienia warunków, o których mowa w ust. 1 ADO oraz inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.

§ 43. 1. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

2 W sytuacji, kiedy w zakresie zachodzących w strukturze ADO procesów przetwarzania danych osobowych pojawią się procesy, wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, pracownicy Urzędu Gminy Sławno informują o tym fakcie IOD.

3. IOD dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.

4. W przypadku, kiedy wynik oceny, o której mowa w ust. 2 wskazuje na współadministrowanie danymi osobowymi, IOD, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w ust. 1.

AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

§ 44. 1. Audyty zgodności przetwarzania danych osobowych zgodnie z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze ADO przeprowadzane są przez IOD lub audytora zewnętrznego.
2. IOD / audytor zewnętrzny przeprowadza audyt według opracowanego planu audytów, sporządzonego na okres nie krótszy niż kwartał i nie dłuższy niż rok, obejmującego co najmniej jeden audyt.
3. Audyt prowadzony może być również w trybie doraźnym - w sytuacji powzięcia przez IOD informacji o wystąpieniu incydentu z zakresu przestrzegania procedur ochrony danych osobowych.
4. Plan audytów IOD / audytor zewnętrzny przygotowuje w formie pisemnej i przedstawia ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
5. W planie audytów IOD / audytor zewnętrzny uwzględnia, w szczególności:
1) przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
2) procesy przetwarzania danych osobowych objęte audytem,
3) konieczność weryfikacji zgodności przetwarzania danych osobowych z:
a) zasadami przetwarzania danych osobowych,
b) zasadami dotyczącymi zabezpieczenia danych osobowych,
c) zasadami przekazywania danych osobowych.
5. W toku audytu IOD / audytor zewnętrzny dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
6. W terminie do 30 dni od zakończenia audytu, IOD / audytor zewnętrzny przygotowuje sprawozdanie dla ADO.

REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

§ 45. 1. ADO uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności prawo do:
1) wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
2) dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
3) sprostowania danych (art. 16 RODO),
4) usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),
5) ograniczenia przetwarzania (art. 18 RODO),
6) przenoszenia danych (art. 20 RODO),
7) wyrażenia sprzeciwu (art. 21 RODO),
8) niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi Załącznik Nr 9 do Polityki.

OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

§ 46. 1. ADO wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.

2. Wdrażając środki techniczne i organizacyjne ADO uwzględnia stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania danych, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

3. ADO wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.

4. Stosowane środki techniczne i organizacje muszą zapewnić w szczególności, by dane osobowe nie były domyślnie udostępniane.

5. W pierwszej kolejności ADO rozważa, czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.

§ 47. ASI zapewnia, aby spełnienie warunków wskazanych w § 46 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu, itp.

§ 48. 1. ADO przy współpracy z IOD i ASI ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania stosujący przy tym środki i podejście takie jak: pseudonimizacja, szyfrowanie danych osobowych, inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania oraz środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

2. Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa wdrożonych w strukturze ADO stanowi Załącznik Nr 10 do Polityki.

OCENA SKUTKÓW DLA OCHRONY DANYCH

§ 49. 1. ADO dokonuje oceny skutków dla ochrony danych osobowych – DPIA (Data Protection Impact Assessment), wyłącznie gdy jest to niezbędne w celu opisania przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.

2. Nie wprowadza się obowiązku stałego monitorowania przetwarzanych danych osobowych pod kątem wysokiego naruszenia praw lub wolności osób fizycznych w związku z przetwarzaniem tych danych, gdyż przetwarzanie to jest wykonywane na mocy przepisów prawa. Przepisy te regulują sposób przetwarzania poszczególnych kategorii danych osobowych w Urzędzie.

3. DPIA może stanowić narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.

4. W celu przeprowadzenia oceny skutków dla ochrony danych osobowych mogą być stosowane sformalizowane arkusze, wg. potrzeb.

INCYDENTY OCHRONY DANYCH OSOBOWYCH

§ 50. 1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych odpowiadają wszyscy pracownicy Urzędu Gminy Sławno, zgodnie z kompetencjami oraz IOD i ASI.

2. ADO stosuje zapisy art. 33 i 34 RODO w identyfikacji, ocenie i zgłoszeniu zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia oraz powiadomienia osób, których dotyczyło naruszenie ochrony danych.

§ 51. 1. Każdy z pracowników, w przypadku podejrzenia lub stwierdzenia naruszenia zasad bezpieczeństwa, ma obowiązek bezzwłocznie poinformować o zdarzeniu IOD przedkładając wypełnioną Kartę zgłoszenia incydentu z zakresu przestrzegania procedur ochrony danych osobowych, wg wzoru stanowiącego Załącznik Nr 11 do Polityki.

2. IOD celem wyjaśnienia okoliczności mających wpływ na zaistnienie incydentu, przeprowadza bezzwłocznie audyt doraźny, który ma na celu w szczególności uprawdopodobnienie, czy wystąpiło ryzyko naruszenia praw lub wolności osób fizycznych. Dokumentuje podejmowane przez siebie czynności wraz z podaniem daty i godziny ich przeprowadzenia w Rejestrze incydentów / naruszeń ochrony danych osobowych, którego wzór stanowi Załącznik Nr 12 do Polityki.

§ 52. 1. Po przeprowadzeniu audytu doraźnego, w przypadku uprawdopodobnienia wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych, ADO informuje organ nadzorczy nie najpóźniej niż w terminie 72 godzin od stwierdzenia wystąpienia incydentu przez osobę zgłaszającą.

2. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

3. Zawiadomienie nie jest wymagane, jeżeli:

1) wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,
2) zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
3) wymagałoby ono niewspółmiernie dużego wysiłku.

PRZEPISY KOŃCOWE

§ 53. 1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.

2. Przeglądu Polityki dokonuje IOD i ASI.

3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki co do procesów funkcjonujących w strukturach ADO i obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator.

4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury ADO przegląd Polityki wykonywany jest niezwłocznie.

5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, IOD i ASI działając wspólnie dokonują jej aktualizacji w wymaganym zakresie.

§ 54. Naruszenie obowiązków wynikających z niniejszej Polityki oraz przepisów ustawy o ochronie danych osobowych i RODO może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

§ 55. Niniejsza Polityka jest dokumentem jawnym, udostępnianym wszystkim zainteresowanych, publikowanym na stronie BIP za wyjątkiem:

1) Załącznika Nr 5 – Obszar przetwarzania danych osobowych w Urzędzie Gminy Sławno,
2) Załącznika Nr 8 – Wykaz zbiorów ewidencyjnych dla danych osobowych
3) Załącznika Nr 10 – Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa w Urzędzie Gminy Sławno,

które są traktowane jako dokumenty wewnętrzne, o kluczowym znaczeniu dla bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Sławno, zastrzeżone wyłącznie do użytku własnego.

§ 56. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy obowiązujące w tym zakresie.

Załącznik Nr 1
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Data nadania upoważnienia:
……

UPOWAŻNIENIE NR …./…..
DO PRZETWARZANIA DANYCH OSOBOWYCH

Wójt Gminy Sławno, działając w imieniu Administratora Danych Osobowych upoważnia Panią/ Pana:

.....
imię i nazwisko upoważnionego

do przetwarzania danych, w celach związanych z wykonywaniem obowiązków na zajmowanym stanowisku oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.

Niniejsze upoważnienie obejmuje przetwarzanie danych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.) i elektronicznej.

Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w zbiorach:

1) e-kancelaria – elektroniczny system obiegu dokumentów;
2) związanych z realizacją bieżących zadań i poleceń, zgodnych z zakresem obowiązków lub w czasie pełnienia zastępstwa.

w zakresie: wglądu, wprowadzania, modyfikacji, usuwania, archiwizacji albo udostępniania innym podmiotom, **koniecznym do wykonywania obowiązków służbowych/pracowniczych**.

Zobowiązuję Panią/Pana do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami:

- 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),
- ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
- ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

oraz wydanymi na ich podstawie aktami wykonawczymi, a także Polityką Bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Sławno.

Upoważnienie jest ważne do odwołania lub ustania stosunku pracy lub innej umowy.

W przypadku posiadania wcześniej wydanych upoważnień niniejsze upoważnienie odwołuje wszystkie uprzednio wydane upoważnienia.

Osoba upoważniona do przetwarzania danych objętych ww. zakresem jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia/zakończeniu okresu trwania umowy oraz zachowaniu w tajemnicy informacji o ich zabezpieczeniu.

……
podpis osoby nadającej upoważnienie

Ja, niżej podpisany/-a **przyjąłem/-ełam do wiadomości** zakres uprawnień wynikających z upoważnienia oraz **zobowiązuję się** do przestrzegania obowiązujących zasad związanych z ochroną danych osobowych.

Jednocześnie **oświadczam,** że jestem świadomy/-a odpowiedzialności karnej za nieprzestrzeganie zasad związanych z ochroną danych osobowych.

Przyjmuję do wiadomości i stosowania.

…….....

data i czytelny podpis osoby upoważnionej

Załącznik Nr 2
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Ewidencja upoważnień do przetwarzania danych osobowych

L.p.	Nr upoważnienia	Data nadania upoważnienia	Imię i nazwisko osoby upoważnionej	Stanowisko osoby upoważnionej	Data ustania upoważnienia	Uwagi

Załącznik Nr 3
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

OŚWIADCZENIE

Oświadczam, że w związku z wykonywaniem obowiązków służbowych przetwarzam dane osobowe oraz mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem (-am) się z:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
- ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych,
- 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 (ogólne rozporządzenie o ochronie danych),
- rozporządzeniem 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,
- Polityką Bezpieczeństwa w Urzędzie Gminy Sławno,
- Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

Jednocześnie zobowiązuję się w okresie trwania stosunku pracy /stażu /praktyki /umowy zlecenia /umowy o dzieło* jak również po ich ustaniu, do zachowania w tajemnicy wszystkich danych osobowych, do których będę miał(a) dostęp w związku z wykonywaniem obowiązków.

Oświadczam, że jestem świadomy(a) odpowiedzialności karnej za udostępnienie lub umożliwienie dostępu do danych osobowych osobom nieupoważnionym.

…….....
data i podpis osoby składającej oświadczenie

* niepotrzebne skreślić

Załącznik Nr 4
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Wniosek
o wydanie upoważnienia do przetwarzania danych osobowych

Wnoszę o wydanie upoważnienia do przetwarzania danych osobowych dla Pani/Pana

…….....,

zatrudnionej/-go na stanowisku …….....

w Referacie ……..……

Urzędu Gminy Sławno od dnia …… do dnia ……..
w celach związanych z wykonywaniem obowiązków na zajmowanym stanowisku oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład zarówno w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.) jak i elektronicznej w zakresie: wglądu, wprowadzania, modyfikacji, usuwania, archiwizacji albo udostępniania innym podmiotom, koniecznym do wykonywania obowiązków służbowych/pracowniczych.

1. Nazwa zbiorów danych osobowych:
   1) ……
   2) ……
   3) ……
   4) ……
   5) ……
   6) ……

2. System informatyczny / oprogramowanie:
   1) ……
   2) ……
   3) ……
   4) ……
   5) ……
   6) ……

.....
…… data i podpis kierownika Referatu

NIE UDOSTĘPNIAĆ!

Załącznik Nr 5
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Obszar przetwarzania danych osobowych w Urzędzie Gminy Sławno

Załącznik Nr 6
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Data wydania zgody:
……

ZGODA NR …./…..
NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie zapisów Polityki bezpieczeństwa w Urzędzie Gminy Sławno i w myśl zapisów pkt A.I.2 załącznika do 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 (Dz. U. z 2004 r. Nr 100, poz. 1024), upoważniam

Panią/Pana: …….

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania:

☐ obowiązków służbowych,

☐ prac zleconych na podstawie umowy nr …….. z dnia ……,

☐ szczegółowych zadań, jak:

……
……
……

Niniejsza zgoda jest ważna do dnia …… / do odwołania.

…….....
podpis osoby wydającej zgodę

Załącznik Nr 7
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Ewidencja zgód
dla osób upoważnionych do przebywania w obszarze przetwarzania danych osobowych

L.p.	Nr zgody	Data wydania zgody	Imię i nazwisko osoby upoważnionej	Zgoda wydana ze względu na	Okres obowiązywania		Uwagi
					od	do	

NIE UDOSTĘPNIAĆ!

Załącznik Nr 8
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Wykaz zbiorów ewidencyjnych
dla danych osobowych

Załącznik Nr 9
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Procedura realizacji praw osób, których dane dotyczą

1. Wszyscy pracownicy Urzędu Gminy Sławno dbają o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza ADO.
2. ADO ułatwia osobom korzystanie z praw poprzez różne działania, w tym: zamieszczanie na stronie internetowej urzędu informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Urzędzie, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Urzędem w tym celu, itp.
3. Wszyscy pracownicy Urzędu Gminy Sławno dbają o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
4. ADO wprowadza adekwatne metody identyfikacji i uwierzytelnienia osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych. Podstawowym narzędziem identyfikacji i uwierzytelnienia jest wgląd do dokumentu tożsamości osoby, której dane dotyczą, a na rzecz której to osoby ma nastąpić realizacja jej praw i obowiązków informacyjnych.
5. W celu realizacji praw osób, których dane dotyczą zapewnione są procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez ADO. Można również zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany. Mechanizmy te w szczególności określa dokumentacja techniczna czy podręcznik użytkownika każdego z systemów elektronicznego przetwarzania danych.
6. Wszyscy pracownicy Urzędu Gminy Sławno informują osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby. Udostępniają treść klauzuli informacyjnej m.in. bezpośrednio w Urzędzie w miejscu uzyskania danych od osoby (stanowisko obsługi interesanta w każdym z pomieszczeń biurowych), drogą komunikacji na odległość (e-mail, telefon) i na stronie internetowej oraz BIP Urzędu.
7. Nie informuje się osoby o przetwarzaniu jej danych, przy pozyskaniu danych o tej osobie niebezpośrednio od niej, jeśli pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy tej osoby lub dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie, w tym ustawowym obowiązkiem zachowania tajemnicy.
8. Informuje się osoby o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe, np. poprzez zamieszczenie znaków informujących o objęciu obszaru monitoringiem wizyjnym.
9. ADO bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko praw lub wolności tej osoby.
10. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO Administrator danych rozpatruje indywidualnie.
11. ADO niezwłocznie, w terminie do 30 dni od wniesienia żądania realizuje następujące prawa osób, których dane dotyczą:
    a) prawo dostępu do danych,
    b) prawo do sprostowania danych,
    c) prawo do usunięcia danych,
    d) prawo do przenoszenia danych,

e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do niepodlegania decyzjom opartym wyłącznie na profilowaniu.

11. Żądania osób:

1) Prawa osób trzecich

Realizując prawa osób, której dane dotyczą, Urząd wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnica handlową, dobra osobiste), Urząd może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

2) Nieprzetwarzanie

ADO informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

3) Odmowa

ADO informuje osobę, niezwłocznie, a najdłużej w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia i o prawach osoby z tym związanych.

4) Dostęp do danych

Na żądanie osoby dotyczące dostępu do jej danych ADO informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

Osoba zainteresowana może skorzystać z prawa dostępu do swoich danych osobowych nie częściej niż raz na 6 miesięcy.

5) Kopie danych

Na żądanie ADO wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej, bezpłatnej kopii danych. Za każdą kolejną kopię danych ADO może naliczyć opłatę w wysokości wynikającej z kosztów administracyjnych.

6) Sprostowanie danych

ADO dokonuje sprostowania danych na żądanie osoby. Ma prawo odmówić sprostowania, chyba że osoba, której dane dotyczą wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych ADO informuje osobę o odbiorcach danych, na żądanie osoby biorąc pod uwagę, że organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem, nie są uznawane za odbiorców.

7) Uzupełnienie danych

ADO uzupełnia i aktualizuje dane na żądanie osoby. Ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. pracownicy Urzędu Gminy Sławno nie mają prawa przetwarzać danych, które są zbędne).

ADO może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Urząd procedur (np. co do pozyskiwania takich danych), prawa lub istnieją podstawy, aby uznać oświadczenie za niewiarygodne.

8) Usunięcie danych

Na żądanie osoby ADO usuwa dane, gdy:

a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,

b) zgoda na ich przetwarzanie została cofnięta a nie ma innej podstawy prawnej przetwarzania,
c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
d) dane były przetwarzane niezgodnie z prawem,
e) konieczność usunięcia wynika z obowiązku prawnego,
f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. udział w konkursie na stronie internetowej).

Prawo do usunięcia danych jest realizowane w taki sposób, by zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą poniższe wyjątki, tzn. po stwierdzeniu, że przetwarzanie danych nie jest konieczne do:

a) korzystania z prawa do wolności wypowiedzi i informacji,
b) wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa,
c) wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
d) celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub do celów statystycznych,
e) ustalenia, dochodzenia lub obrony roszczeń,
f) uwzględnienia interesu publicznego w dziedzinie zdrowia publicznego.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Urząd Gminy Sławno, ADO podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

9) Ograniczenie przetwarzania

ADO dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich stosowania,
c) Urząd Gminy Sławno nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Urzędu Gminy Sławno zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania ADO przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

10) Przenoszenie danych

Na żądanie osoby ADO wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu

podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Urzędowi Gminy Sławno, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych ADO.

11) Sprzeciw w szczególnej sytuacji

Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane są przetwarzane przez ADO w oparciu o uzasadniony interes Urzędu Gminy Sławno lub o powierzone Urzędowi zadanie w interesie publicznym, ADO uwzględni sprzeciw, o ile nie zachodzą po stronie Urzędu ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

12) Sprzeciw przy celach statystycznych

Jeżeli ADO przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Urząd Gminy Sławno uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

13) Sprzeciw względem marketingu bezpośredniego

Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez ADO na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Urząd Gminy Sławno uwzględni taki sprzeciw i zaprzestanie takiego przetwarzania.

14) Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu

Jeżeli ADO przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, ADO zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie ADO, chyba że taka automatyczna decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Urzędem Gminy Sławno,
b) jest wprost dozwolona przepisami prawa,
c) opiera się na wyraźnej zgodzie osoby odwołującej się.

15) Minimalizacja

ADO dba o minimalizację przetwarzania danych pod kątem:

a) adekwatności danych do celów (ilość danych i zakresu przetwarzana),
b) dostępu do danych,
c) czasu przechowywania danych.

16) Minimalizacja zakresu

ADO weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach RODO i dokonuje ich okresowego przeglądu i weryfikacji.

17) Minimalizacja dostępu

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

ADO stosuje kontrolę dostępu fizycznego, m.in. poprzez ograniczenie dostępu do pomieszczeń serwerowni czy archiwum zakładowego.

ADO dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających w oparciu o wydane upoważnienia do przetwarzanie danych oraz ewidencję osób upoważnionych do przetwarzania danych.

ADO dokonuje też okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż na raz na rok.

18) Minimalizacja czasu

ADO wdraża mechanizmy kontroli „cyklu życia" danych osobowych w Urzędzie Gminy Sławno, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów informatycznych Urzędu, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się w kopiach zapasowych systemów i informacji przetwarzanych przez Urząd. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystywania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

12. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
13. ADO odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Załącznik Nr 10
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa w Urzędzie Gminy Sławno

Załącznik Nr 11
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Karta zgłoszenia incydentu
z zakresu przestrzegania procedur ochrony danych osobowych

Referat	
Stanowisko	
Imię i nazwisko zgłaszającego	
Zakres danych, zbiór danych którego dotyczy zgłoszenie	
Data, godzina stwierdzenia wystąpienia incydentu	
Opis incydentu	
Data, godzina, podpis zgłaszającego	
Data, godzina, podpis IOD	

Załącznik Nr 12
do Polityki Bezpieczeństwa
w Urzędzie Gminy Sławno

Rejestr incydentów / naruszeń ochrony danych osobowych

Lp.		1.	2.	3.	4.
1.	Naruszenie (opis naruszenia)				
2.	Data i godzina zgłoszenia podejrzenia naruszenia				
3.	Data i godzina stwierdzenia naruszenia				
4.	Data naruszenia/okres, którego dotyczy				
5.	Kategoria i liczba osób, których dotyczy naruszenie				
6.	Zakres danych i/lub kategorie danych, których dotyczy naruszenie				
7.	Osoba/źródło informacji o naruszeniu				
8.	Miejsce naruszenia				
9.	Okoliczności naruszenia – opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia				
10.	Opis skutków/ konsekwencji				
11.	Ryzyko naruszenia praw i wolności				
12.	Opis możliwego naruszenia praw lub wolności				
13.	Osoba/ jednostka odpowiedzialna za naruszenie				
14.	Podjęte działania – opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu				
15.	Rezultat działań naprawczych				
16.	Osoba odpowiedzialna za wdrożenie działań naprawczych				
17.	Czy zachodzi obowiązek poinformowania UODO				
18.	Czy poinformowano organa ścigania				
19.	Czy zachodzi obowiązek poinformowania osoby których naruszenie dotyczy				
20.	Monitoring działań naprawczych				

NIE UDOSTĘPNIAĆ!

Załącznik Nr 2
do Zarządzenia Nr 66/2018
Wójta Gminy Sławno
z dnia 25 maja 2018 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w URZĘDZIE GMINY SŁAWNO