Zarządzenie Nr 58/2020

Starosty Stalowowolski z dnia 14 grudnia 2020 r.

w sprawie przyjęcia Polityki ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli

Na podstawie art. 34 ust. 1 Ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2020 r., poz. 920) oraz art. 24 ust. 2 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 (Dz. Urz. UE L 119 z 04.05.2016) zarządzam, co następuje:

§ 1

1. W celu zapewnienia zgodności przetwarzania danych osobowych z wymogami 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, zwanego dalej RODO oraz przepisami prawa krajowego z zakresu ochrony danych osobowych, przyjmuje się Politykę ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli, stanowiącą załącznik do niniejszego Zarządzenia.
2. Zobowiązuje się kierowników komórek organizacyjnych do zapoznania podległych im pracowników oraz innych osób przetwarzających dane osobowe w nadzorowanej komórce z dokumentacją, o której mowa w ust. 1.

§ 2

Traci moc Zarządzenie Nr 18/2018 Starosty Stalowowolskiego z dnia 21 czerwca 2018 r. w sprawie przyjęcia Polityki ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli wraz ze zmianami.

§ 3

Nadzór nad wykonywaniem przepisów niniejszego Zarządzenia powierza się Inspektorowi Ochrony Danych oraz kierownikom komórek organizacyjnych w zakresie działania nadzorowanych przez nich komórek działania.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Starosta Stalowowolski

Janusz Zarzeczny
(podpisano kwalifikowanym podpisem elektronicznym)

Załącznik do Zarządzenia nr 58/2020 Starosty Stalowowolskiego z dnia 14 grudnia 2020 r.
w sprawie przyjęcia Polityki ochrony danych osobowych
przetwarzanych w Starostwie Powiatowym w Stalowej Woli

POLITYKA OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W STAROSTWIE POWIATOWYM W STALOWEJ WOLI

OGÓLNE POSTANOWIENIA, W TYM CELE DZIAŁANIA PODMIOTU

§ 1

1. Celami przyjęcia i realizacji Polityki ochrony danych osobowych, zwanej dalej Polityką, jest ochrona prywatności osób, których dane przetwarzane są w Starostwie Powiatowym w Stalowej Woli i ustalenie wewnętrznych procedur przetwarzania danych osobowych tak, aby zapewnić zgodność przetwarzania danych osobowych z wymogami *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*, zwanego dalej RODO oraz przepisami prawa krajowego z zakresu ochrony danych osobowych.
2. Wszystkie osoby, które mają dostęp i przetwarzają dane osobowe w Starostwie Powiatowym w Stalowej Woli zobowiązane są do stosowania niniejszej Polityki.
3. Polityka została opracowana z uwzględnieniem Normy PN-ISO/IEC 27001:2014.
4. Materialny zakres stosowania Polityki zgodny jest z zakresem ujętym w art. 2 RODO.
5. Administratorami Danych Osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli w zależności od czynności przetwarzania danych mogą być:
   a) Starosta Stalowowolski,
   b) Powiat Stalowowolski,
   c) Zarząd Powiatu Stalowowolskiego lub Rada Powiatu Stalowowolskiego,
   d) Powiatowy Rzecznik Konsumentów w Stalowej Woli,
   e) Pracownicza Kasa Zapomogowa-Pożyczkowa,
   f) Starostwo Powiatowe w Stalowej Woli;
6. Obszarem przetwarzania danych osobowych jest budynek Starostwa Powiatowego w Stalowej Woli oraz budynek Archiwum Zakładowego Starostwa Powiatowego, mieszczące się przy ul. Podleśnej 15 w Stalowej Woli.
7. Budynek Starostwa Powiatowego obejmuje:
   a) IV piętro – czynności przetwarzania zawierają dane art. 9 ust. 1 RODO oraz art. 10 RODO, w tym dane art. 9 ust. 1 RODO osób nieletnich,
   b) III piętro – czynności przetwarzania zawierają dane art. 9 ust. 1 RODO oraz art. 10 RODO,
   c) II piętro – czynności przetwarzania zawierają dane art. 9 ust. 1 RODO oraz art. 10 RODO, w tym dane art. 9 ust. 1 RODO nieletnich oraz informacje niejawne i dokumenty publiczne,
   d) I piętro - czynności przetwarzania zawierają dane art. 9 ust. 1 RODO oraz art. 10 RODO, w tym dane pracowników, kierowników jednostek, stażystów i praktykantów, a także dane finansowo-księgowe,
   e) parter - czynności przetwarzania zawierają dane zwykłe oraz tymczasowo dane art. 9 ust. 1 RODO oraz art. 10 RODO oraz informacje niejawne w związku z ich rejestracją;
8. Na podstawie art. 37 ust. 1 RODO oraz art. 9 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781) w strukturze Starostwa Powiatowego w Stalowej Woli powinien być wyznaczony Inspektor Ochrony Danych.
9. Funkcji Inspektora Ochrony Danych nie może pełnić osoba zatrudniona na stanowisku kierowniczym urzędniczym, ds. informatyzacji, ds. osobowych oraz osoby upoważnione do wydawania decyzji administracyjnych, a także Sekretarz Powiatu, Skarbnik Powiatu, Geolog Powiatowy, inspektor ds. BHP.
10. Wymogi dotyczące ochrony danych osobowych i prywatności powinny być uwzględniane już na wstępnych etapach projektowania usług, produktów, czynności bądź systemów mających służyć do przetwarzania danych osobowych.

§ 2

1. Definicje:

1) dane osobowe – zgodnie z art. 4 pkt. 1) RODO,
2) dane zwykłe – dane osobowe poza zakresem danych ujętym w art. 9 ust. 1 oraz art. 10 RODO,
3) przetwarzanie danych osobowych – zgodnie z art. 4 pkt 2) RODO,
4) zbiór danych osobowych – zgodnie z art. 4 pkt 6) RODO,
5) podmiot przetwarzający – zgodnie z art. 4 pkt 8) RODO,
6) naruszenie ochrony danych osobowych – zgodnie z art. 4 pkt 12) RODO,
7) poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym lub nieupoważnionym osobom, podmiotom lub procesom,
8) integralność - zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
9) dostępność - zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot lub zapewnienie, że informacja jest możliwa do wykorzystania na żądanie,
10) ADO – Administrator danych osobowych,
11) ASI – Administrator systemów informatycznych,
12) IOD – Inspektor ochrony danych,
13) KKO – Kierownicy komórek organizacyjnych,
14) osoba nieuprawniona – osoba z zewnątrz podmiotu lub pracownik, który nie jest upoważniony do dostępu do wskazanego w upoważnieniu zakresu danych osobowych,
15) nośnik zewnętrzny – telefon (również smartfon), laptop, pen-drive, tablety, dysk zewnętrzy, inne elektroniczne urządzenia przenośne,
16) system - systemy informatyczne, aplikacje, programy komputerowe, poczta elektroniczna, chmury obliczeniowe, inne narzędzia informatyczne.

2. Powiat wykonuje określone ustawami zadania publiczne o charakterze ponadgminnym w zakresie wskazanym w art. 4 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2018 r. poz. 995 z późn. zm.). Zgodnie z art. 33 cytowanej ustawy Zarząd Powiatu wykonuje zadania powiatu określone przepisami prawa przy pomocy starostwa powiatowego.
3. Celami działania Powiatu Stalowowolskiego oraz Starostwa Powiatowego w Stalowej Woli są:
   1) realizacja zadań, praw i obowiązków wynikających z przepisów prawa,
   2) realizacja umów,
   3) realizacja zadań wynikających ze sprawowania władzy publicznej,
   4) realizacja zadań wynikających z prowadzenia gospodarki finansowej;
4. Czynniki zewnętrzne i wewnętrzne istotne dla celu działania podmiotu:

Czynniki zewnętrzne	Czynniki wewnętrzne
Zmiany przepisów prawa	Zmiany regulaminów organizacyjnych, zarządzeń starosty i innych aktów wewnętrznych
Zmiany składów organów wykonawczego i stanowiącego	Zmiany stanowisk pracy – rotacja pracowników, sposób zarządzania zasobami ludzkimi
Celowe działania petentów/kontrahentów	Celowe/przypadkowe działania pracowników

negatywnie wpływające na pracę podmiotu m.in. *wandalizm, szpiegostwo, wprowadzanie w błąd, podsłuch, kradzież dokumentów*	m.in. *zaniedbania użytkowników, zgubienie lub zniekształcenie informacji, błędy przy wprowadzaniu danych, uszkodzenia nośników danych, niestosowanie przepisów prawa i aktów wewnętrznych, zniszczenie dokumentów*
Działanie złośliwego oprogramowania - atak hackerski, wirusy	Struktura budynku i pomieszczeń
Zakłócenia źródła zasilania	Defekty sprzętu, nośników informatycznych
Pożar, zalanie/powódź, skutki działania wilgotności	Struktura systemów informatycznych, oprogramowania, luki w oprogramowaniu
	Utrata informacji, nieuprawnione modyfikowanie informacji, ujawnienie

5. Zadania osób odpowiedzialnych za przetwarzanie danych osobowych:

Nazwa stanowiska	Zakres odpowiedzialności i zadań
Administrator danych osobowych	Pełna odpowiedzialność wobec organu nadzorczego i osób, których dane dotyczą; Dba o to, aby IOD był włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Dba o odpowiednie szkolenia pracowników. Podejmuje działania, aby zapewnić odpowiednią ilość środków finansowych przeznaczonych na ochronę danych osobowych. Pełni rolę decyzyjną.
Zarząd Powiatu	Dokonuje zgodnie ze swoimi kompetencjami podziału środków przeznaczonych na ochronę danych osobowych, zarządza mieniem Powiatu. Reguluje zgodnie z kompetencjami sprawy organizacyjne.
Wicestarosta	Pełni zastępstwo w razie nieobecności ADO
Inspektor ochrony danych	1) Realizacja zadań wynikających z art. 39 RODO. 2) Realizacja innych zadań wynikających z przepisów krajowych. 3) Prowadzenie rejestru czynności przetwarzania danych osobowych. 4) Aktualizacja Polityki ochrony danych osobowych we współpracy z ASI. 5) Przeprowadzanie analizy ryzyka we współpracy z ASI. 6) Przygotowywanie zgłoszeń naruszeń ochrony danych osobowych – art. 33 RODO.

	7) Wsparcie kierowników komórek organizacyjnych w przygotowaniu dokumentacji związanej z ochroną danych osobowych m.in. *klauzul informacyjnych, klauzul wyrażeń zgody, umów powierzenia danych osobowych.* 8) Prowadzenie we współpracy z ASI rejestru zdarzeń mogących mieć wpływ na ochronę danych osobowych. 9) Prowadzenie rejestru umów powierzenia. 10) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych. 11) Inne zadania zlecone przez ADO.
Administrator Systemów Informatycznych	1) Wsparcie ADO w doborze środków zabezpieczających dane osobowe w systemach informatycznych, zgodnych z wymaganiami zawartymi w przepisach prawa. 2) Wsparcie ADO i IOD w ocenie skutków dla ochrony danych osobowych w systemach informatycznych. 3) Dokonywanie sprawdzeń systemów informatycznych raz do roku lub w razie konieczności częściej. 4) Dokonywanie przeglądów i konserwacji sprzętu informatycznego raz do roku lub w razie konieczności częściej. 5) Wsparcie IOD w przygotowaniu dokumentacji z zakresu ochrony danych osobowych m.in. *Polityki ochrony danych osobowych dotyczącej infrastruktury informatycznej.* 6) Wsparcie IOD w przeprowadzaniu analiz ryzyka naruszeń praw i wolności osób fizycznych. 7) Wsparcie w realizacji innych zadań wykonywanych przez IOD m.in. dotyczących realizacji obowiązków

	wynikających z praw osób, których dane dotyczą, dokonywania zgłoszeń do organu nadzorczego, w zakresie systemów informatycznych, oceny skutków dla ochrony danych osobowych. 8) Inne zadania zlecone przez ADO lub IOD.
Kierownicy komórek organizacyjnych	1) Nadzór nad prawidłowym przetwarzaniem danych osobowych w nadzorowanej komórce i stosowaniem Polityki ochrony danych osobowych. 2) Znajomość i przestrzeganie przepisów z zakresu ochrony danych osobowych, w tym Polityki ochrony danych osobowych. 3) Odpowiedzialność dyscyplinarna i karna, zgodnie z przepisami prawa, za dokonanie naruszeń ochrony danych, 4) KKO zobowiązani są do włączania IOD we wszystkie sprawy dotyczące ochrony danych osobowych;
Poszczególne stanowiska pracy	1) Znajomość i przestrzeganie przepisów z zakresu ochrony danych osobowych, w tym Polityki ochrony danych osobowych. 2) Odpowiedzialność dyscyplinarna i karna, zgodnie z przepisami prawa, za dokonanie naruszeń ochrony danych.

6. Oczekiwania osób, których dane dotyczą w stosunku do podmiotu przetwarzającego dane:

Osoby, których dane dotyczą	Oczekiwania
Osoby, które udostępniają dane osobowe w celu realizacji swoich praw, interesów i obowiązków	Szybkie i rzetelne załatwienie sprawy zgodnie z przepisami prawa
Pracownicy, z którymi nawiązano stosunek pracy	Rzetelna realizacja umowy, dbałość o prawa pracowników
Stażyści, praktykanci	Zdobycie wiedzy praktycznej i poszerzenie wiedzy teoretycznej
Strony umów cywilnoprawnych	Wywiązanie się z zapisów umowy
Radni Rady Powiatu, członkowie Zarządu Powiatu	Możliwość wykonywania obowiązków w ramach powierzonej władzy

§ 3

Zabezpieczenia organizacyjne

1. Osoby zatrudnione muszą posiadać kwalifikacje odpowiednie do danego stanowiska określone w przepisach prawa m.in. ustawie z dnia 21 listopada 2008 r. o pracownikach samorządowych.
2. Przetwarzać dane osobowe mogą tylko osoby, którym ADO udzielił upoważnienia i polecenia przetwarzania. Wzór upoważnienia i polecenia przetwarzania zawiera **załącznik nr 1.**
3. Sprawy z zakresu nadania upoważnienia prowadzi IOD przy konsultacji z danym KKO.
4. KKO wskazuje IOD zakres upoważnienia, składając wniosek o nadanie upoważnienia dla osoby przetwarzającej dane osobowe **stanowiący załącznik nr 23,** w przypadku:
   1) pracownika zgodny z kartą zadań,
   2) praktykanta zgodny z programem praktyk,
   3) stażysty zgodny z programem stażu;
5. W razie nieobecności ADO podpisu upoważnień, o których mowa w ust. 2, dokonuje Wicestarosta.
6. Osoba, której ma być nadane pierwsze upoważnienie, przechodzi stosowne przeszkolenie z zakresu ochrony danych osobowych, które przeprowadza IOD oraz przeszkolenie z zakresu bezpieczeństwa informatycznego, które przeprowadza ASI.
7. W przypadku konieczności wydania kolejnego upoważnienia pracownik jest pouczony o zasadach lub przepisach prawa, na które musi zwrócić uwagę przy wykonywaniu nowych czynności służbowych. Nie jest już wtedy przeprowadzane pełne szkolenie, o którym mowa w ust. 6.
8. Osoba zatrudniona na stanowisku ds. osobowych przekazuje następujące informacje o zatrudnionych osobach, stażystach, praktykantach do IOD i ASI:
   a) Imię, nazwisko,
   b) Stanowisko,
   c) Okres i podstawa zatrudnienia lub okres i podstawa organizacji stażu i praktyki,
   d) Komórka organizacyjna;
9. Stanowisko ds. osobowych zobligowane jest również do przekazania IOD i ASI informacji o zmianie zakresu obowiązków czy stanowiska pracy, a także o zwolnieniach pracowników.
10. Osoba, która otrzymała upoważnienie podpisuje również stosowne oświadczenie o zachowaniu w tajemnicy pozyskanych danych osobowych oraz stosowanych zabezpieczeniach w trakcie i po ustaniu stosunku pracy, stażu lub praktyk, a także oświadczenie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych **stanowiące załącznik nr 19.**
11. Oświadczenie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych, podpisywane jest jednorazowo, przy pierwszym nadaniu upoważnienia.
12. Ewidencję upoważnień prowadzi IOD zgodnie z wzorem w **załączniku nr 2.**
13. Po wydaniu upoważnienia pracownik otrzymuje od IOD identyfikator oraz kartę wstępu do Kancelarii Ogólnej.
14. Dostęp w systemie umożliwiającym wejście do Kancelarii Ogólnej nadaje pełnomocnik ds. informacji niejawnych, a w razie jego nieobecności starszy informatyk urzędu.
15. Osoby sprzątające wykonują swoje obowiązki:
   a) po godzinach pracy Starostwa Powiatowego,
   b) w Wydziale Komunikacji i Transportu, Archiwum Zakładowym oraz Powiatowym Centrum Zarządzania Kryzysowego w godzinach pracy Starostwa Powiatowego w obecności upoważnionych pracowników,

c) KKO może również zawnioskować ze względu na specyfikę przetwarzania danych osobowych (np. przetwarzanie danych szczególnych) o sprzątanie pomieszczeń w godzinach pracy Starostwa Powiatowego w obecności upoważnionych pracowników;

16. Stosowne przeszkolenie z zakresu zasad ochrony danych osobowych przechodzą również na początku kadencji radni Rady Powiatu Stalowowolskiego oraz członkowie Zarządu Powiatu Stalowowolskiego.
17. Osoby, które nie mają nadanego upoważnienia, o którym mowa w ust. 2, w obszarze przetwarzania danych osobowych, bez obecności upoważnionego pracownika, mogą wykonywać swoje czynności służbowe po wyrażeniu zgody przez administratora danych zgodnie ze wzorem ujętym w **załączniku nr 20.**
18. IOD prowadzi rejestr osób, którym wyrażono zgodę na przebywanie w obszarze przetwarzania danych osobowych.
19. Korespondencja wychodząca zawierająca dane osobowe musi być wysyłana listem poleconym tak, aby mogła być zwrócona do urzędu w przypadku braku odbioru przez adresata lub niewłaściwego jej zaadresowania.

§ 4

Postępowanie w trakcie i po okresie zatrudnienia

1. Pracownicy naruszający zasady ochrony danych osobowych i Politykę ochrony danych osobowych podlegają postępowaniu dyscyplinarnemu oraz odpowiadają za uchybienia zgodnie z przepisami prawa.
2. Pracownicy przechodzą stosowne szkolenia dotyczące zmian w Polityce ochrony danych osobowych oraz przepisach prawa z zakresu ochrony danych osobowych.
3. IOD oraz ASI pełnią rolę doradczą i informacyjną dla pracowników.
4. Pracownicy, z którymi rozwiązywany będzie stosunek pracy lub którym wygasa stosunek pracy:
   1) zobowiązani są do zwrotu kart do czytników i innych nośników informatycznych, których używali,
   2) przekazania bezpośredniemu przełożonemu niezałatwionych spraw i teczek,
   3) gdy ma to zastosowanie przekazania bezpośredniemu przełożonemu szablonów pism, służbowych plików i innych dokumentów, zapisanych w profilu użytkownika, niezbędnych do wykonywania dalszych zadań w komórce organizacyjnej.
5. Pracownicy, o których mowa w ust. 4, uzupełniają kartę zwrotu stanowiska. Wzór karty zwrotu stanowiska zawiera **załącznik nr 3.**
6. Za właściwe uzupełnienie karty zwrotu stanowiska odpowiada KKO.
7. Karta powinna być zwrócona w ostatnim dniu świadczenia pracy.
8. Administratorzy systemów odbierają pracownikom prawa dostępu do systemów lub blokują dostęp do systemu w dniu następującym po ostatnim dniu rozwiązania lub wygaśnięcia stosunku pracy.
9. Użytkownik po uzyskaniu odpowiedniego upoważnienia do przetwarzania danych osobowych ma tworzony profil w systemie środowiskowym.
10. Profil w systemie środowiskom tworzony jest przez osoby zatrudnione na stanowisku ds. informatyzacji po uzyskaniu informacji od IOD o wydaniu upoważnienia poprzez wewnętrzny moduł zgłoszeń informatycznych.
11. Dostęp do profilu może mieć administrator systemu lub procesy pracujące z uprawnieniami administracyjnymi w sytuacjach związanych z czynnościami administracyjnymi oraz kierownik komórki organizacyjnej w sytuacjach wymienionych w Polityce ochrony danych osobowych.
12. Profil użytkownika jest profilem służbowym i wszystkie przechowywane w nim pliki nie powinny zawierać danych ze sfery prywatnej.

13. Pracodawca nie ponosi odpowiedzialności za dane ze sfery prywatnej przechowywane w służbowym profilu użytkownika.
14. Dostęp do profilu użytkownika chroniony jest loginem, nadawanym przez osoby zatrudnione na stanowisku ds. informatyzacji oraz hasłem.
15. Pierwsze hasło nadawane jest przez osoby zatrudnione na stanowisku ds. informatyzacji, użytkownik jest zobligowany do jego niezwłocznej zmiany przy pierwszym uruchomieniu.
16. Pliki zapisane na dyskach wspólnych, systemowym koszu, w folderze pobrane oraz w folderze skanowane należy po realizacji celu przetwarzania danych osobowych niezwłocznie trwale usuwać.
17. W przypadku, gdy komputer używany przez pracownika wymieniany jest na inny, pracownik zobligowany jest do usunięcia danych, a jeżeli tego nie dokona dane są usuwane przez osoby zatrudnione na stanowisku ds. informatyzacji.
18. W sytuacji, gdy komputer jest wycofany z użytku pracownik zobligowany jest do usunięcia danych, a jeżeli tego nie dokona dane są usuwane przez osoby zatrudnione na stanowisku ds. informatyzacji.
19. Osoby, których stosunek pracy wygasa lub zmieniają stanowisko pracy zobligowane są do usunięcia danych na swoim profilu lub przekazania tych danych kierownikowi komórki organizacyjnej.
20. W przypadku, gdy pracownik, któremu wygasa stosunek pracy lub zmienia stanowisko pracy nie usunie danych na profilu, dane te są usuwane przez osoby zatrudnione na stanowisku ds. informatyzacji po wcześniejszym poinformowaniu kierownika komórki organizacyjnej.
21. W przypadku nagłej tymczasowej nieobecności pracowników dostęp do profilu użytkownika następuje przez osoby zatrudnione na stanowisku ds. informatyzacji na wniosek kierownika komórki organizacyjnej w jego obecności.
22. Na stanowiskach ds. informatyzacji monitorowany jest poprzez sprzęt firewall i UTM oraz w przypadku zagrożeń informatycznych przez program antywirusowy ruch użytkowników w sieci, w tym ruch pracowników obejmujący m.in. rodzaj pobranych załączników, wejścia na strony internetowe, korzystanie z aplikacji.
23. Analizowane są incydenty pod danym nr IP zgłoszone przez system IDS.
24. Na stacjach roboczych zainstalowane jest oprogramowanie, które zbiera dane o wykonanych wydrukach.
25. W razie konieczności w przypadku nagłej tymczasowej nieobecności pracowników dostęp do skrzynki służbowej poczty elektronicznej obsługiwanej na danym stanowisku pracy następuje przez osoby zatrudnione na stanowisku ds. informatyzacji na wniosek kierownika komórki organizacyjnej.
26. Osoby, których stosunek pracy wygasa lub zmieniają stanowisko pracy zobligowane są do oczyszczenia służbowej skrzynki poczty elektronicznej, a informatycy do przekierowania otrzymywanych wiadomości na służbową skrzynkę kierownika komórki organizacyjnej.
27. Zasady prowadzenia monitoringu przez pracodawcę na podstawie Kodeksu Pracy zostały uregulowane w Regulaminie Pracy.

§ 5

Powierzanie przetwarzania danych osobowych i ich udostępnianie

1. Powierzenie danych osobowych może nastąpić tylko na podstawie umowy powierzenia danych osobowych. Wzór umowy, który może być dostosowany potrzeb danej komórki organizacyjnej, zawiera załącznik nr 4.
2. W wyjątkowych sytuacjach dopuszcza się, aby powierzenie zostało uregulowane w formie odpowiednich zapisów w umowie głównej.

3. Umowa powierzenia lub zapis w umowie głównej musi spełniać zadość wymaganiom ujętym w art. 28 RODO.
4. Umowy dotyczące usług sieciowych dodatkowo powinny zawierać mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania i bezpieczeństwa.
5. Projekt umowy, o której mowa w ust. 1 należy skonsultować z IOD oraz jeżeli powierzenie następuje w systemie informatycznym projekt należy skonsultować również z ASI.
6. Podmiot przetwarzający musi dawać odpowiednie gwarancje wdrożenia środków technicznych i organizacyjnych, by spełnić wymogi RODO np. poprzez stosowanie certyfikatów, kodeksów postępowania, odpowiednich procedur wewnętrznych, stosowanie norm ISO i podejmowanie innych działań.
7. Lista kontrolnych pytań pomagających w wyborze podmiotu przetwarzającego określona została **w załączniku nr 32.**
8. Odpowiedzialność za powierzenie danych osobowych spoczywa na ADO.
9. IOD prowadzi rejestr umów powierzenia. Wzór zawiera **załącznik nr 5.**
10. Po podpisaniu umowy powierzenia KKO zgłasza ten fakt IOD, który rejestruję umowę.
11. Dane mogą być udostępnione stronom trzecim na podstawie przepisów prawa i złożonego pisemnego wniosku. Jeżeli przepisy szczególne nie zawierają wzoru wniosku o udostępnienie danych osobowych stosuje się wzór, który zawiera **załącznik nr 14.**
12. Sprawę z zakresu udostępnienia danych osobowych rozpatruje IOD lub KKO, a jeżeli udostępnienie dotyczy danych przetwarzanych w systemie, w realizacji sprawy bierze udział ASI.
13. Przy udostępnianiu danych osobowych należy brać pod uwagę w szczególności art. 4 pkt 9), art. 6, art. 9, i art. 10 RODO oraz motyw 31 RODO, a także przepisy szczególne.

§ 6

Strefy dostępu

1. Starostwo Powiatowe w Stalowej Woli mieści się w budynku użyteczności publicznej, z tego względu dostęp w godzinach pracy urzędu do pomieszczeń pod nadzorem upoważnionych pracowników, poza wyjątkami zawartymi w ust. 2, mają wszyscy interesanci.
2. Tylko upoważnieni pracownicy w związku z realizacją zadań służbowych lub osoby pełniące kontrolę albo nadzór mają wstęp w godzinach pracy urzędu do:
   a) Archiwum Zakładowego (oddzielny budynek),
   b) pomieszczeń do przechowywania dokumentacji geodezyjnej – nr 8, nr 7 (dwa wejścia), nr 4 (dwa wejścia), nr 5 (parter),
   c) Archiwum Geologicznego – pokój nr 305 (III piętro),
   d) serwerowni – pokój nr 320 (III piętro),
   e) wyznaczonych obszarów w poszczególnych pomieszczeniach na stanowiskach pracy,
   f) Powiatowego Centrum Zarządzania Kryzysowego,
   g) pomieszczeń wyznaczonych w Wydziale Komunikacji i Transportu w odrębnym zarządzeniu.
3. Nadzór nad pomieszczeniami Powiatowego Inspektoratu Nadzoru Budowlanego w Stalowej Woli znajdującymi się na IV piętrze pełni Powiatowy Inspektor Nadzoru Budowlanego.

§ 7

Środki bezpieczeństwa fizycznego

1. Szafki do przechowywania dokumentów z danymi osobowymi muszą być wyposażone w zamek.

2. Dokumenty można przechowywać również w szafach metalowych lub pancernych.
3. Należy stosować politykę czystego biurka tzn.:
   a) dokumenty zawierające dane osobowe należy przechowywać w zamkniętej szafce, a klucz do szafki należy zabezpieczyć przed dostępem osób nieuprawnionych np. poprzez stosowanie depozytorów kluczy,
   b) w trakcie pracy należy tak układać dokumenty, aby nieuprawnione osoby przebywające przy biurku nie miały dostępu do danych m.in. poprzez odpowiednie odkładanie dokumentów, przykrywanie dokumentów kartką, przyjmowanie interesantów przy innym biurku, odkładanie dokumentów pod ladę,
   c) dokumenty w trakcie pracy nie mogą zostać zabrudzone, zniszczone, zagubione,
   d) dokumenty należy niszczyć tylko w niszczarce, wyrzucanie dokumentów do kosza – nawet podartych, jest zakazane,
   e) dokumenty wydrukowane na drukarce na korytarzu należy niezwłocznie odebrać lub korzystać z tzw. wydruku bezpiecznego;
4. Przy przenoszeniu dokumentów do innego pomieszczenia należy zachować środki ostrożności, aby ich nie zagubić i zabezpieczyć tak, aby osoby nieuprawnione nie miały do nich wglądu.
5. Pomieszczenie, w którym przetwarzane są dane osobowe nie może być pozostawione niezamknięte bez nadzoru osoby upoważnionej.
6. Klucze przechowywane są w zamkniętej szafce w Kancelarii Ogólnej, z wyjątkiem Wydziału Komunikacji i Transportu.
7. Pracownik po zakończeniu pracy zobowiązany jest do odwieszenia klucza w zamykanej szafce w Kancelarii Ogólnej.
8. Wejście do Kancelarii Ogólnej drzwiami głównymi po godzinie 15:30 jest możliwe po przyłożeniu karty przez uprawnionego pracownika do czytnika.
9. Po godzinie 15:30 przy wejściu i wyjściu drzwi Kancelarii Ogólnej otwierają się po przyłożeniu karty do czytnika. Kartą należy się odbić podczas wejścia i wyjścia oraz sprawdzić czy drzwi Kancelarii Ogólnej zostały zamknięte.
10. Klucze wejściowe do Kancelarii Ogólnej w razie awarii czytnika znajdują się u kancelisty (2 egzemplarze), na stanowisku ds. administracyjno-gospodarczych oraz u Sekretarza Powiatu.
11. Prowadzenie nadzoru nad kluczami zapasowymi powierza się pracownikowi zatrudnionemu na stanowisku ds. administracyjno-gospodarczych, który jest uprawniony do wykonania zapasowego egzemplarza klucza.
12. Odpowiedzialność za przestrzeganie zasad bezpieczeństwa fizycznego w danej komórce organizacyjnej ponosi Naczelnik/Kierownik.
13. Osoby, które zajmują się postępowaniem zamówień publicznych przed zakupem mebli i wyposażenia infrastruktury budynku oraz pomieszczeń powinny zasięgnąć opinii IOD czy pomieszczenie dostosowane będzie do zasad ochrony danych osobowych m.in.

a) biurka muszą być dopasowane do tego, aby możliwe było ustawienie ekranu monitora w sposób niewidoczny dla osób nieupoważnionych,
b) w pomieszczeniach, w których przyjmuje się kilku interesantów jednocześnie należy tworzyć boksy, biurka z przegrodami, strefy przyjęć interesantów;

14. Dokumenty zawierające dane osobowe mogą być wynoszone poza teren Starostwa Powiatowego w wersji papierowej lub elektronicznie na zabezpieczonym nośniku informatycznym:
    1) gdy wyrazi na to zgodę bezpośredni przełożony oraz jest to niezbędne do wykonania czynności służbowych,
    2) w celu wykonywania pracy zdalnej zgodnie z Zarządzeniem pracodawcy;

15. Za dokumenty wyniesione poza teren Starostwa Powiatowego w celach służbowych poza miejsce zatrudnienia odpowiada pracownik, który zobowiązany jest do zachowania środków bezpieczeństwa tak, aby ich nie zniszczyć, nie zagubić i zapewnić odpowiednią poufność.
16. Wynoszenie dokumentów zawierających dane szczególnej kategorii, o których mowa w art.9 ust. 1 RODO i danych zawartych w art. 10 RODO do domu jest zabronione, chyba że wymaga tego zlecona praca zdalna.
17. Pracownik musi mieć wyrażoną zgodę na wyniesienie dokumentów poza zakład pracy, zgodnie z wzorem określonym w załączniku nr 22 lub w przypadku pracy zdalnej zgodnie z zarządzeniem Starosty.
18. Budynek po zakończeniu pracy zabezpieczony jest alarmem i nadzorem firmy ochroniarskiej.
19. Dostęp do archiwum zakładowego zabezpieczony jest alarmem, a nadzór nad zabezpieczeniami pełni archiwista zakładowy.
20. Klucz do danego pokoju może odebrać pracownik, który pracuje na stanowisku pracy przyporządkowanym do tego pokoju.
21. Odpowiedzialność za klucz w godzinach pracy ponosi pracownik, który pobrał klucz z Kancelarii Ogólnej lub znalazł się w jego posiadaniu w trakcie wykonywania pracy.
22. Stażyści lub praktykanci mogą odebrać klucz do pokoju po wpisaniu się do ewidencji odbioru kluczy. Ewidencja znajduje się w Kancelarii Ogólnej. Wzór ewidencji stanowi **załącznik nr 15.**
23. Nadzór nad odbieraniem kluczy przy rozpoczęciu pracy urzędu i w trakcie pracy urzędu powierza się pracownikom Kancelarii Ogólnej.
24. Pracownicy Kancelarii Ogólnej otrzymują informacje o osobach, którym wygasł stosunek pracy lub zakończyli staż lub praktyki od IOD.
25. Zabrania się wynoszenia kluczy poza teren Starostwa Powiatowego, z wyjątkiem kluczy do drzwi wejściowych urzędu i Kancelarii Ogólnej.
26. Pracownicy, którzy posiadają klucze do drzwi wejściowych urzędu i Kancelarii Ogólnej podpisują oświadczenie zawarte w **załączniku nr 16.**
27. Kod alarmu znają wyznaczeni przez Administratora Danych Osobowych pracownicy, którzy podpisują oświadczenie zawarte w **załączniku nr 16.**
28. W przypadku zgubienia kluczy należy ten fakt zgłosić niezwłocznie do pracownika zatrudnionego na stanowisku ds. administracyjno-gospodarczych. Pracownik zatrudniony na stanowisku administracyjno-gospodarczych niezwłocznie zgłasza ten incydent do IOD.
29. Dokumenty publiczne, o których mowa w Ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych (t.j. Dz. U. z 2020 r. poz. 725), należy zabezpieczać zgodnie z zasadami w niej ujętymi.

§ 8

Zabezpieczenia infrastruktury informatycznej

1. Nadzór nad zabezpieczeniami infrastruktury informatycznej pełni ASI.
2. Przed zakupem sprzętu komputerowego, systemów, aplikacji, programów, narzędzi informatycznych osoby dokonujące zamówienia publicznego bądź inne osoby dokonujące zakupu muszą zasięgnąć opinii ASI lub IOD czy system dostosowany jest do zasad ochrony danych osobowych i czy nie ma konieczności przeprowadzenia oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO. b
3. Zabezpieczenia systemów informatycznych należy dobierać do zakresu przetwarzanych danych osobowych i częstotliwości ich przetwarzania.
4. System musi spełniać wymagania określone w *Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla*

rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247).

5. W miarę możliwości należy przed zakupem lub rozpoczęciem pracy z danym systemem przeprowadzić test akceptacyjny.
6. Decyzję o konieczności czy należy przeprowadzić ocenę dla skutków ochrony danych osobowych podejmuje ADO po powzięciu informacji od KKO, ASI i IOD.
7. Oceny skutków dla ochrony danych osobowych dokonuje IOD oraz ASI na zlecenie ADO.
8. Odpowiedzialność za dokonanie oceny skutków dla ochrony danych osobowych i akceptację ryzyka spoczywa na ADO.
9. Ocenę skutków dla ochrony danych osobowych można zlecić podmiotowi zewnętrznemu.
10. Na każdej stacji komputerowej bądź innym nośniku zainstalowane jest oprogramowanie antywirusowe, które zarządzane jest centralnie przez głównego informatyka i starszego informatyka urzędu.
11. Oprogramowania, zwłaszcza antywirusowe, systemy, aplikacje muszą być systematycznie aktualizowane. Za nadzór nad aktualizacjami odpowiada administrator danego systemu.
12. Jeżeli aktualizacja znaczącą wpływa na zmiany w działaniu oprogramowania, systemu, aplikacji, w którym przetwarzane są dane osobowe, należy przeprowadzić ocenę skutków dla ochrony danych osobowych.
13. W związku ze stosowanymi IOD oraz ASI mają prawo monitorować ruch pracowników w sieci oraz sposób pracy na urządzeniu komputerowym.
14. Gdy zachodzi konieczność informatycy mogą łączyć się zdalnie i pracować w systemie po wcześniejszej manualnej akceptacji połączenia przez użytkownika.
15. Zabronione jest samodzielne instalowanie programów i narzędzi przez użytkowników. Konieczność instalowania oprogramowania musi być zgłoszona ASI i mogą jej dokonać administratorzy.
16. Dostęp do komputerów, innych urządzeń informatycznych, systemów, oprogramowań, aplikacji mają tylko upoważnieni pracownicy.
17. Najbezpieczniejszą formą przekazywania danych osobowych w sieci jest Elektroniczna Platforma Usług Administracji Publicznej (e-PUAP).
18. ASI prowadzi szkolenia z zakresu bezpieczeństwa infrastruktury komputerowej, uwzględniające:
    1) zagrożenia bezpieczeństwa informacji przetwarzanej w wersji elektronicznej,
    2) skutki naruszenia zasad bezpieczeństwa informacji przetwarzanej w wersji elektronicznej, w tym odpowiedzialność prawna,
    3) stosowanie środków zapewniających bezpieczeństwo informacji przetwarzanej w wersji elektronicznej, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
19. ASI zobligowany jest do poszerzania swojej wiedzy z zakresu pojawiających się zagrożeń. ADO zapewnia w tym celu odpowiednie środki finansowe i organizacyjne.
20. Wygaszacze powinny włączać się na każdym stanowisku komputerowym po 15 minutach bezczynności komputera. Ze względu na charakter pracy czas ten może być wydłużony lub skrócony.
21. Systemy i inne narzędzia informatyczne, w których przetwarzane są dane szczególnej kategorii wymienione w art. 9 RODO lub dane dotyczące naruszeń prawa wymienione w art. 10 RODO lub przetwarzanie danych nie jest sporadyczne, muszą być zabezpieczone hasłem, zmienianym raz na 30 dni, składającym się z co najmniej 8 znaków złożonych z:

a) Małych i dużych liter,
b) Znaku specjalnego,

c) Liczb/y

22. Systemy i inne narzędzia informatyczne, w których nie są przetwarzane dane szczególnej kategorii wymienione w art. 9 RODO lub dane dotyczące naruszeń prawa wymienione w art. 10 RODO lub dane są przetwarzane sporadycznie mogą być zabezpieczone hasłem zmienianym raz na kwartał.
23. Hasło powinno być skomplikowane, nie powinno wiązać się z danymi osobowymi pracownika, jego stanowiskiem pracy czy działalnością urzędu, może być układem stworzonym przez kombinację liter i znaków na klawiaturze.
24. Sprzęt komputerowy musi raz do roku przechodzić konserwację i przegląd, obejmujące ich rodzaj i konfigurację w celu zapewnienia integralności i dostępności danych, których dokonują - główny informatyk urzędu oraz starszy informatyk.
25. ASI dokonuje sprawdzenia przed usunięciem, zbyciem lub przekazaniem sprzętu do ponownego użycia czy wszystkie jego składniki i dane wraz z licencjonowanymi programami zostały usunięte lub odpowiednio zabezpieczone. W tym celu spisuje protokół.
26. Sprzęt komputerowy powinien być podłączony do listw przeciwprzepięciowych.
27. Wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą UTM oraz zapory firewall.
28. W uzasadnionych przypadkach pracownik może pracować zdalnie poza miejscem zatrudnienia zgodnie z zasadami przyjętymi w zakładzie pracy z wykorzystaniem odpowiednio zabezpieczonego sprzętu informatycznego.
29. Dostępu do systemów informatycznych i innych narzędzi informatycznych udzielają osoby na stanowisku ds. informatyzacji po dokonaniu stosownego zgłoszenia poprzez wewnętrzny moduł zgłoszeń informatycznych przez IOD lub KKO zgodnie z zakresem wskazanym we wniosku o nadanie upoważnienia do przetwarzania danych osobowych.
30. Dostęp do systemów wykorzystywanych w Starostwie Powiatowym w Stalowej Woli mogą mieć tylko upoważnieni pracownicy w związku z wykonywaniem czynności służbowych lub pracownicy firm zewnętrznych w związku z ich serwisem lub aktualizacją na podstawie zawartej umowy powierzenia.
31. W razie konieczności dostęp do systemów i programów może być zmieniany.
32. Administrator danego systemu prowadzi ewidencję jego użytkowników.
33. IOD wraz z ASI prowadzą ogólny przegląd praw dostępu użytkowników, natomiast administratorzy danego systemu odpowiadają za bieżący nadzór nad dostępem użytkowników.
34. Nadzór, o którym mowa w ust. 33 obejmuje m.in.:
    1) okresowe sprawdzanie czy użytkownicy mają dostęp zgodny z zakresem upoważnienia,
    2) blokowanie użytkowników, którym wygasł stosunek pracy, zmienili stanowisko lub dostęp nie jest potrzebny,
    3) dostosowanie uprawnień użytkowników do zaistniałych zmian,
    4) blokowanie użytkowników, którzy naruszyli zasady ochrony danych osobowych;
35. Prawa administracyjne w danym systemie nadaje ASI, który odpowiada za nadzór nad prawami administracyjnymi.
36. Prawa administracyjne w systemie mogą mieć:
    a) kierownicy komórek organizacyjnych lub samodzielne stanowiska pracy,
    b) stanowiska ds. informatyzacji,
    c) wyznaczeni przez KKO pracownicy, którym prawa administracyjne są niezbędne do wykonywania czynności służbowych,
    d) Starosta, Wicestarosta, Sekretarz Powiatu i Skarbnik Powiatu;
37. Nadzór, o którym mowa w ust. 35 obejmuje m.in.:
    1) okresowe sprawdzanie czy administratorzy nie wykorzystują nadanych uprawnień administracyjnych niezgodnie z celami służbowymi,
    2) sprawdzanie czy prawa administracyjne zostały nadane odpowiednim osobom,

3) zabieranie praw administracyjnych nieuprawnionym osobom;

38. ASI prowadzi wykaz administratorów danych systemów.
39. Drukarki umieszczone na korytarzu powinny mieć zabezpieczenie przed nieuprawnionym dostępem m.in. kopiowanie przy użyciu karty, drukowanie po odpowiedniej identyfikacji użytkownika. Instrukcje bezpiecznego wydruku znajdują się przy drukarkach oraz na stanowiskach ds. informatyzacji**.**
40. Zabronione jest dokonywanie samodzielnych napraw sprzętu informatycznego.
41. Należy stosować politykę czystego ekranu:
    a) dokonywać systematycznie sprawdzeń folderów i plików z danymi osobowymi, w tym na dyskach wspólnych, czy nie wymagają usunięcia,
    b) systematycznie opróżniać kosz i folder „skanowane”,
    c) rejestry elektroniczne zawierające dane osobowe należy zabezpieczać hasłem lub przechowywać w folderach przyporządkowanych do konta użytkownika,
    d) należy zwracać uwagę na to, jakie pliki umieszcza się na dysku wspólnym i kto ma wgląd do dysków wspólnych,
    e) w szablonach pism anonimizować dane osobowe;
42. Korzystanie ze prywatnego sprzętu informatycznego bez zgłoszenia takiej konieczności oraz wyrażenia zgody ASI jest zabronione. Wzór zgłoszenia zawiera **załącznik nr 21.**
43. Wszelkie kwestie awarii, błędów, napraw, aktualizacji, pomocy technicznej związanej z korzystaniem z zasobów informatycznych należy zgłaszać przy pomocy wewnętrznego modułu informatycznego „help desk”, dostępnego w Biuletynie Wewnętrznym.
44. Opis systemów służących do przetwarzania danych osobowych został ujęty w **załączniku nr 13.**
45. Najwłaściwszą formą elektronicznego wewnętrznego przekazywania danych osobowych i dokumentów ich zawierających jest system służący do elektronicznego zarządzania dokumentacją.
46. Osoby umieszczające artykuły do publikacji w BIP zobligowane są do zanonimizowania danych osobowych w publikowanym artykule lub zawartych w publikowanym dokumencie, chyba że istnieje przepis prawa nakazujący ich publikację.
47. Osoby zatwierdzające artykuł do publikacji w BIP zobligowane są do weryfikacji czy dane osobowe zostały odpowiednio zanonimizowane przez osobę tworzącą artykuł lub powinny być opublikowane na podstawie przepisów prawa.
48. W przypadku publikacji danych osobowych niezgodnie z przepisami prawa, należy zgłosić się do IOD.
49. Administrator BIP w przypadku zauważenia naruszenia prawa w związku z publikacją w BIP może cofnąć publikację i zobligowany jest do zgłoszenia incydentu do IOD.

§ 9

Internet

1. Każdy pracownik ma lub może mieć dostęp do Internetu jeżeli charakter wykonywanych czynności na to zezwala.
2. Dostęp ze względu na charakter przetwarzanych danych może zostać zablokowany przez ASI po zgłoszeniu przez KKO.
3. ASI zobligowany jest do stosowania odpowiednich urządzeń np. UTM, aplikacji, oprogramowania np. zapór firewall zapewniających bezpieczeństwo w sieci oraz wydzielanie odpowiednich struktur w sieci.
4. Za dobór środków zabezpieczających odpowiada ADO uwzględniając zakres przetwarzanych danych, rodzaj zagrożeń i posiadane środki finansowe.
5. KKO nadzoruje ruch pracowników w sieci.

6. ASI blokuje dostęp do stron pornograficznych, erotycznych, społecznościowych i innych uznanych za szkodliwe bądź zbędne w pracy.
7. W związku z odpowiednimi zabezpieczeniami sieci internetowej aktywność pracowników w Internecie jest monitorowana i obejmuje m.in. odwiedzane strony internetowe, pobierane z Internetu pliki, programy, aplikacje i inne narzędzia informatyczne, w tym załączniki pobierane z prywatnej poczty elektronicznej, dane o logowaniu.
8. Informatycy mogą weryfikować ruch w Internecie w raportach wygenerowanych przez urządzenia i systemy służące do zabezpieczania sieci internetowej.
9. Zapisy dotyczące prowadzenia monitoringu aktywności pracowników w Internecie reguluje Regulamin Pracy.
10. W trakcie przetwarzania danych osobowych na platformach przy pomocy przeglądarki internetowej należy po zakończonej pracy wylogować się i zamknąć przeglądarkę.
11. Zabronione jest domyślne zapisywanie haseł w przeglądarkach internetowych.
12. Przed zalogowaniem należy sprawdzić czy platforma została uruchomiona właściwym połączeniem szyfrowanym zgodnie z przykładem w **załączniku nr 17.**

§ 10

Postępowanie z pocztą elektroniczną

1. Pracownicy mogą sprawdzać prywatne skrzynki pocztowe z użyciem przeglądarki internetowej. Zabronione jest natomiast pobieranie załączników.
2. Jeżeli korzystanie z prywatnych skrzynek pocztowych będzie naruszało ochronę danych i zagrażało bezpieczeństwu informatycznemu korzystanie z prywatnych skrzynek pocztowych może być zablokowane danemu użytkownikowi, grupie użytkowników lub w całym urzędzie.
3. Treści wiadomości zawarte w prywatnych skrzynkach pocztowe nie są monitorowane przez ASI i IOD. Monitorowany jest natomiast ruch sieci, a więc w Raportach systemu zabezpieczeń widoczne są nazwy i rodzaje pobranych załączników z prywatnej skrzynki.
4. Kwestie korzystania z prywatnej skrzynki pocztowej zostały uregulowane również w Regulaminie Pracy.
5. Pracownicy korzystają ze służbowych kont e-mail lub kont wydziałowych, nad którymi nadzór pełni KKO.
6. Pierwsze hasła do służbowych skrzynek elektronicznych nadają informatycy.
7. Zabronione jest korzystanie ze służbowej poczty elektronicznej w celach prywatnych.
8. Ustawia się najwyższy domyślny poziom ochrony skrzynki pocztowej służbowej z połączeniem szyfrowanym.
9. ASI i IOD pomagają pracownikom odpowiednio zabezpieczać przesyłane dane.
10. Zabronione jest pobieranie niesprawdzonych i podejrzanych załączników.
11. Pocztą elektroniczną można przesyłać tylko zaszyfrowane pliki z danymi zabezpieczone odpowiednio hasłem lub odpowiednio zanonimizowane.
12. Nie wolno przekazywać pocztą elektroniczną danych szczególnej kategorii, o których mowa w art. 9 ust. 1 RODO lub zawierających dane, o których mowa w art. 10 RODO.
13. Zakazane jest korzystanie z przechowywania i przesyłania danych w chmurach innych niż te, które dopuszczone zostały przez ADO .
14. Zaleca się, aby przesyłanie danych osobowych następowało za pomocą Elektronicznej Platformy Usług Administracji Publicznej.
15. W przypadku wysyłki wiadomości zawierających dane osobowe na niewłaściwy adres poczty elektronicznej należy ten fakt zgłosić niezwłocznie do IOD w celu podjęcia czynności wyjaśniających.

16. W przypadku otrzymania wiadomości zawierających dane osobowe, których nie jest się adresatem należy wysłać nadawcy wiadomość: *„Wiadomość została wysłana na niewłaściwy adres e-mail. Informuję, że pani/a e-mail zostanie usunięty ze skrzynki poczty elektronicznej”* oraz usunąć wiadomość ze skrzynki.
17. Użytkownik służbowej skrzynki pocztowej odpowiada za jej właściwe użytkowanie, w szczególności za:
    1) usuwanie wiadomości zbędnych – nietworzących akt sprawy, spamów, reklam,
    2) usuwanie wiadomości zawierających dane osobowe, których zakończył się cel przetwarzania,
    3) niezwłoczne zgłaszanie do IOD lub informatyków wiadomości podejrzanych,
    4) dbanie o poprawność wysyłki i nazwy adresatów,
    5) stosowanie ukrytej kopii w przypadku wysyłki do wielu adresatów,
    6) korzystanie z klienta poczty elektronicznej a nie przeglądarki,
    7) korzystanie ze służbowej poczty elektronicznej poza pracą w sytuacjach opisanych w § 7 ust. 14.

§ 11

Środki ochrony w ramach narzędzi programowych i baz danych

1. W celu zapewnienia integralności i dostępności danych osobowych wykonuje się kopie baz danych osobowych lub zbiorów danych osobowych.
2. Kopie podlegają regularnym sprawdzeniom i testom poprawności.
3. Kopie zapasowe wykonywane są przez głównego informatyka urzędu oraz starszego informatyka lub wyznaczonego pracownika w wydziale.
4. Nadzór nad wykonywaniem kopii zapasowych pełni ASI lub KKO - jeżeli został do tego zobligowany.
5. Kopie zapasowe przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
6. Każdy z użytkowników narzędzi komputerowych ma ustalony swój profil użytkownika wraz z prawami do korzystania z narzędzi programowych zgodnymi ze stanowiskiem pracy.
7. Główny informatyk urzędu oraz starszy informatyk zobowiązani są do ustawienia opcji domyślnych oprogramowań, systemów, aplikacji na najwyższym poziomie zabezpieczeń z zakresu ochrony danych osobowych.
8. Instalacja oprogramowania oraz jego użytkowanie powinno odbywać się zgodnie z zaleceniami producenta.
9. Jeżeli system umożliwia odnotowywanie logów, powinny być prowadzone dzienniki logów. Dzienniki logów prowadzą główny informatyk urzędu oraz starszy informatyk. Nadzór spoczywa na ASI.
10. Odtworzenie danych z kopii zapasowej przez administratorów powinno mieć miejsce:
    1) gdy zachodzi konieczność sprawdzenia jakości kopii zapasowej np. przy próbie odtworzeniowej lub z innych przyczyn technicznych np. awarii dysku komputera,
    2) na wniosek użytkownika,
    3) w przypadku konieczności odtworzenia danych z profilu użytkownika na wniosek kierownika komórki organizacyjnej;
11. Odpowiednie zabezpieczanie danych w plikach elektronicznych może polegać:
    a) szyfrowaniu przy pomocy odpowiedniego narzędzia szyfrującego,
    b) zabezpieczaniu pliku lub folderu hasłem wykorzystując możliwość daną już przez producenta,
    c) anonimizowaniu danych osobowych poprzez zakrycie danych kartką lub zamalowanie ich na kopii czarnym flamastrem, a następnie ich zeskanowanie,

d) użyciu funkcji „chroń” w .pdf; zakazane jest w rozszerzeniu .pdf nakładanie pasków lub innych kształtów zakrywających poprzez użycie narzędzi w funkcji „skomentuj”;

§ 12

Nośniki zewnętrzne

1. Dane można przetwarzać na służbowych nośnikach zewnętrznych.
2. Nośniki zewnętrzne znajdują się na wyposażeniu Wydziałów i są przechowywane przez Naczelników lub wskazanych pracowników.
3. Nośniki zewnętrzne mogą znajdować się na wyposażeniu radnych Rady oraz członków Zarządu Powiatu Stalowowolskiego.
4. Nośniki zewnętrzne, na których przetwarzane są dane osobowe muszą być zabezpieczone hasłem oraz zaszyfrowane.
5. Prowadzi się wykaz nośników zewnętrznych wraz z imieniem i nazwiskiem pracownika korzystającego z nośnika z podaniem nr identyfikacyjnego nośnika. Wykaz prowadzi ASI.
6. Odpowiedzialność za nośnik i dane w nim zawarte ponosi pracownik korzystający z nośnika.
7. Nośniki oraz dyski komputera wycofane z użycia należy niszczyć specjalistycznym sprzętem pozwalającym na trwałe usunięcie danych z nośnika i samego nośnika.
8. Odpowiedzialność za prawidłowe usunięcie danych i nośników spoczywa na ASI, który sporządza z tych czynności protokół.
9. Na karcie lub w pamięci telefonu należy przechowywać dane kontaktowe (imię, nazwisko, nr telefonu) tylko wykorzystywane do rozmów służbowych.
10. W telefonie nie wolno przechowywać danych osobowych m.in. wizerunku, adresów zamieszkania, zdjęć dokumentów dłużej niż jest to niezbędne do realizacji celu ich przetwarzania.
11. Jeżeli jest to technicznie możliwe, na telefonie instaluje się program antywirusowy i dokonuje jego aktualizacji. Odpowiedzialność za instalację i aktualizację ponosi pracownik posiadający w użytkowaniu telefon.
12. W telefonie ustawia się automatyczną blokadę pulpitu oraz zabezpiecza dostęp poprzez hasło (może być cyfrowe lub znak graficzny).
13. Z Internetu w telefonie i innym nośniku zewnętrznym korzysta się zgodnie z zasadami ujętymi w § 8-10 niniejszej Polityki.
14. W razie zniszczenia lub zaginięcia nośnika danych osobowych należy niezwłocznie powiadomić ASI lub IOD.
15. Do użytkowania nośników zewnętrznych stosuje się określone w Polityce zabezpieczenia infrastruktury informatycznej.
16. Nośniki zewnętrzne należy po zakończeniu pracy przechowywać w miejscu niedostępnym dla osób postronnych np. szafka zamykana na klucz.
17. Nośniki zewnętrzne można wynosić poza siedzibę urzędu w uzasadnionych przypadkach. W takiej sytuacji za nośnik odpowiada pracownik.
18. Wpinanie nośników zewnętrznych innych niż służbowe, bez zgody ASI i wcześniejszego sprawdzenia nośnika pod kątem bezpieczeństwa na przeznaczonym do takich celów komputerze, jest zabronione.

§ 13

Serwerownia

1. Nadzór na bezpieczeństwem serwerowni w urzędzie sprawuje ASI.
2. Dostęp do serwerowni, w tym klucze, mają przede wszystkim główny informatyk urzędu, starszy informatyk, IOD, stanowisko ds. administracyjno-gospodarczych oraz osoby upoważnione przez ADO.

3. Dostęp osób poza wymienionymi w ust. 1 w celach serwisowych następuje tylko w obecności upoważnionych pracowników.
4. Z czynności serwisowych wykonanych przez osoby wymienione w ust. 3 sporządza się protokół podpisany przez serwisanta i ASI bądź upoważnionego pracownika.
5. Serwerownia powinna być odpowiednio chłodzona oraz spełniać wymogi ochrony przeciwpożarowej.
6. W serwerowni powinny być również prowadzone przez głównego informatyka urzędu lub starszego informatyka pomiary temperatury i wilgotności.
7. Główny informatyk urzędu oraz starszy informatyk powinni dokonywać przeglądów i konserwacji sprzętu oraz dbać o ich czystość.
8. Wydział Komunikacji i Transportu posiada własną serwerownię, nadzór nad bezpieczeństwem której sprawuje Naczelnik Wydziału.

§ 14

Sprawdzenia wewnętrzne

1. IOD we współpracy z ASI raz do roku zobowiązany jest do przygotowania i wdrożenia programu sprawdzeń, w jakim stopniu Polityka ochrony danych osobowych, przepisy prawa i zasady z zakresu ochrony danych osobowych są realizowane i utrzymywane.
2. Sprawdzenia, o których mowa w ust. 1 niniejszego paragrafu dokonywane są w celu realizacji monitorowania przestrzegania RODO.
3. Program obejmuje dwa sprawdzenia i ustalany jest w grudniu roku poprzedzającego przeprowadzenie sprawdzenia. Program zatwierdza ADO.
4. Program zawiera:
   1) Kryteria i zakres sprawdzenia
   2) Komórki organizacyjne podlegające sprawdzeniu
5. Sprawdzenia dokumentuje się, a ich wyniki przedstawia ADO.
6. Wyniki sprawdzenia zawierają propozycje działań mających na celu skorygowanie ewentualnych niezgodności.
7. Jeżeli w trakcie sprawdzenia wykryte zostanie naruszenie ochrony danych osobowych IOD i ASI ma obowiązek zgłosić ten fakt ADO oraz wpisać naruszenie do wewnętrznego rejestru naruszeń ochrony danych prowadzonego przez IOD, a jeżeli zachodzi taka konieczność zgłosić naruszenie organowi nadzorczemu i powiadomić osoby, których dane dotyczą lub zawiadomić policję.
8. IOD i ASI raz do roku dokonuje również monitoringu przeprowadzonej analizy ryzyka i w razie konieczności dokonuje aktualizacji.
9. ADO może zlecić przeprowadzenie audytu podmiotowi zewnętrznemu.

§ 15

Zgłaszanie naruszeń ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych należy ten fakt niezwłocznie zgłosić IOD, ASI lub ADO w celu podjęcia działań wyjaśniających.
2. Przykłady naruszeń oraz działań zaradczych zostały zawarte **w załączniku nr 6**.
3. Działania wyjaśniające przeprowadza IOD lub ASI przy udziale KKO. W działaniach wyjaśniających bierze udział pracownik, którego naruszenie dotyczy.
4. ADO decyduje czy naruszenie należy zgłosić do organu nadzorczego lub powiadomić osoby, których dane dotyczą zgodnie z wymogami art. 33 i 34 RODO.
5. Po przeprowadzeniu działania wyjaśniającego sporządza się raport podpisany przez przeprowadzającego działanie wyjaśniające. Wzór raportu zawiera **załącznik nr 7.**

6. Do raportu dołącza się pozyskane dowody naruszenia zasad ochrony danych osobowych, opis reakcji na incydent, opis podjętych rozwiązań oraz w przypadku, gdy za naruszenie odpowiada pracownik - pouczenia osób odpowiedzialnych za powstanie incydentu.
7. Naruszenie ewidencjonuje się w rejestrze naruszeń ochrony danych osobowych prowadzonym przez IOD. Wzór rejestru zawiera **załącznik nr 8.**
8. Osoba stwierdzająca naruszenie zobowiązana jest do zgłoszenia takiego naruszenia do bezpośredniego przełożonego, który zgłasza ten fakt IOD lub bezpośrednio do IOD. Formularz zgłoszenia zawiera **załącznik nr 26.**
9. Naruszenie musi być oszacowane przez IOD zgodnie z metodą opisaną **w załączniku nr 27,** wykorzystująca metodę ENISA.

§ 16

Rejestr czynności i kategorii przetwarzania danych osobowych

1. IOD prowadzi rejestr czynności przetwarzania danych osobowych, zgodnie z wymogami art. 30 RODO. Wzór zawarty jest w **załączniku nr 9.**
2. IOD prowadzi rejestr kategorii czynności przetwarzania danych osobowych, zgodnie z wymogami art. 30 RODO, zawarty w **załączniku nr 9.**
3. KKO zobowiązani są do zgłoszenia IOD nowej czynności przetwarzania danych osobowych.
4. IOD weryfikuje czy zgłoszoną przez KKO czynność przetwarzania danych osobowych należy wpisać do rejestru czynności przetwarzania danych osobowych.
5. KKO zobowiązani są do zgłoszenia IOD informacji, że Powiat Stalowowolski lub Starostwo Powiatowe w Stalowej Woli stało się dla danej kategorii czynności przetwarzania podmiotem przetwarzającym.
6. Rejestry, o których mowa w ust. 1 i ust. 2 prowadzone są w wersji elektronicznej z wykorzystaniem MS Office, w ciągu roku kalendarzowego.
7. Następnie wydruk rejestru z danego roku kalendarzowego przechowywany jest w teczce spraw

§ 17

Analiza ryzyka

1. IOD i ASI, w porozumieniu z KKO, przeprowadza analizę ryzyka naruszeń praw osób, których dane dotyczą.
2. Analiza jest oddzielnym dokumentem zatwierdzonym przez ADO.
3. Analiza przeprowadzana jest zgodnie z metodyką opisaną w **załączniku nr 10.**
4. Analiza jest aktualizowana w razie konieczności raz na rok lub częściej.
5. Aktualizacji dokonuje IOD i ASI.
6. Analiza zawiera wykaz aktywów i ich właścicieli wraz z ich klasyfikacją wartości dla podmiotu.
7. Postępowanie z aktywami wyszczególnionymi w analizie regulują przepisy prawa, przepisy wewnętrzne, karty zadań pracowników.
8. Odpowiedzialność za nadzór pracowników w zakresie postępowania z aktywami spoczywa na KKO.
9. IOD na pisemne zlecenie wspiera ADO w ocenie skutków dla ochrony danych w kwestiach:
    1) czy należy przeprowadzić ocenę skutków dla ochrony danych,
    2) metodologii przeprowadzenia oceny skutków dla ochrony danych,
    3) czy należy przeprowadzić wewnętrzną ocenę czy też zlecić ją podmiotowi zewnętrznemu,
    4) zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą,

5) prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować).

10. Do oceny skutków można użyć narzędzi udostępnionych przez Urząd Ochrony Danych Osobowych.
11. Jeśli administrator nie zgadza się z zaleceniami IOD w wyżej wymienionych przypadkach, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia zaleceń IOD.

§ 18

Obowiązek informacyjny

1. Wzór klauzuli informacyjnej w celu wypełnienia obowiązku informacyjnego, o którym mowa w art. 13 RODO – w przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą i art. 14 RODO - w przypadku pozyskiwania danych z innych źródeł, zawiera **załącznik nr 11.** Wzór należy dopasować do konkretnej czynności przetwarzania danych osobowych.
2. Wzór klauzul informacyjnych w związku z postępowaniem administracyjnym prowadzonym na podstawie Kodeksu postępowania administracyjnego zawiera **załącznik nr 24.**
3. Obowiązek informacyjny na podstawie art. 13 RODO spełnia się przy zbieraniu danych osobowych.
4. Obowiązek informacyjny na podstawie art. 14 RODO spełnia się w rozsądnym terminie, maksymalnie w ciągu miesiąca od pozyskania danych osobowych.
5. Źródłem pochodzenia danych może być:
   a) rejestr publicznie dostępny np. CEIDG, KRS,
   b) jednostka samorządu terytorialnego, urząd, organ, podmiot publiczny,
   c) podmiot prywatny np. w przypadku danych kontaktowych pracowników;
6. Obowiązek informacyjny można spełnić:
   a) poprzez dopięcie informacji w wersji papierowej do przesyłanego pisma – gdy mamy kontakt tylko na odległość,
   b) klauzula może mieć formę pisemnej informacji podpisanej przez osobę, której dane dotyczą dopiętej do akt sprawy,
   c) elektronicznie – jeżeli kontaktujemy się elektronicznie np. poprzez e-mail.
   d) dla ogółu społeczeństwa – na BIP, stronie internetowej, wywieszenie na tablicy ogłoszeń, wyłożenie w miejscu ogólnie dostępnym,
   e) na formularzu wniosku,
   f) ze względów dowodowych nie jest preferowana forma ustna.
7. Obowiązek informacyjny należy spełnić także względem osób prawnych, z wyłączeniem sytuacji, w której przetwarzane są dane firmy (NIP, adres siedziby, telefon ogólny do firmy, e-mail ogólny do firmy) m.in. poprzez:
   a) umieszczenie stopki, o której mowa w ust. 10, w e-mail lub
   b) umieszczenie stopki z informacjami, o których mowa w ust. 10, w stopce pisma w edytorze tekstowym;
8. Przy zawieraniu umów z osobami prawnymi należy w treści umowy umieścić zapis zawarty w załączniku nr 31.
9. Informacji udziela się zgodnie z wymogami art. 13 i art. 14 RODO, z zastrzeżeniem art. 3-4 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).
10. Pracownicy w poczcie elektronicznej w wiadomościach wysyłanych muszą mieć ustawioną stopkę o treści: *„Administratorem danych osobowych jest Starosta Stalowowolski, ul. Podleśna*

15 37-450 Stalowa Wola, tel. 15 643 37 09; dane kontaktowe do Inspektora Ochrony Danych: abi@stalowowolski.pl, tel. 15 643 36 35; więcej informacji znajduje się w Biuletynie Informacji Publicznej Starostwa Powiatowego w Stalowej Woli w zakładce „Ochrona danych osobowych".

11. Informację o przekazaniu danych osobowych do państwa trzeciego w celu poinformowania o ewentualnym ryzyku takiego przekazania zawiera **załącznik nr 25**.
12. Przykładowi odbiorcy danych osobowych, uwzględniani w klauzulach informacyjnych:
    a) w przypadku prowadzonych postępowań administracyjnych – strony postępowania,
    b) podmioty, z którymi zawarto umowy powierzenia,
    c) podmiot prywatny, z którym zawarto umowę w celu serwisu systemu informatycznego do elektronicznego obiegu dokumentacji w Starostwie Powiatowym w Stalowej Woli,
    d) podmioty, jednostki, osoby fizyczne, osoby prawne, organy publiczne, którym ujawnia się dane osobowe w uzasadnionych przypadkach na podstawie przepisów prawa lub w związku z interesem publicznym,
    e) strony trzecie wykazujące prawny interes np. w celu dochodzenia roszczeń.
13. Organów publicznych, które otrzymały dane w związku z prowadzonych przez nie postępowaniem nie traktuje się jako odbiorców danych osobowych i nie wykazuje w klauzulach informacyjnych.
14. Organami, o których mowa w ust. 13 mogą być:
    a) policja i inne organy ścigania,
    b) sądy,
    c) prokuratura,
    d) organy publiczne prowadzące postępowania kontrolne lub administracyjne;

§ 19

Klauzula wyrażenia zgody

1. Wzór klauzuli wyrażenia zgody zawiera **załącznik nr 12.** Wzór należy dopasować do konkretnej czynności przetwarzania danych osobowych.
2. Przed zebraniem zgody na przetwarzanie danych osobowych należy sprawdzić czy nie występują inne przesłanki legalizujące, o których mowa w art. 6, 9 lub 10 RODO oraz przepisach szczególnych.
3. Zbieranie zgód od pracowników regulują również przepisy Kodeksu pracy.
4. Zgoda może być podstawą przetwarzania danych tylko wtedy, gdy nie występują inne przesłanki legalizujące.
5. Przed zawarciem zgody na przetwarzanie danych osobowych należy skonsultować czynność tą z Inspektorem Ochrony Danych lub radcą prawnym.
6. Po zawarciu zgody należy ten fakt zgłosić do Inspektora Ochrony Danych, który nada klauzuli wyrażenia zgody nr. Wzór rejestru klauzul wyrażeń zgody zawiera **załącznik nr 28.**

§ 20

Prawa osób, których dane dotyczą

1. Na żądania osób, których dane dotyczą w związku z realizacją ich praw zawartych w art. 12-23 RODO, odpowiada pisemnie ADO.
2. Sprawy z zakresu realizacji praw, o których mowa w § 13 ust. 1, realizuje IOD przy współudziale ASI i KKO.
3. Prawa, osób których dane dotyczą realizowane są na pisemny wniosek tej osoby, z zastrzeżeniem ust. 4.

4. Wycofanie zgody musi by równie łatwe, co jej wyrażenie tj. jeżeli zgoda była wyrażona elektronicznie, również elektronicznie powinna być możliwość jej wycofania.
5. Wzór wniosku o udostępnienie informacji i kopii danych osobowych zawiera **załącznik nr 18.**
6. W przypadku realizacji prawa do sprzeciwu, należy wykazać istnienie prawnie uzasadnionych podstaw do przetwarzania nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
7. Do realizacji ust. 6 można posłużyć się analizą interesu nadrzędnego administratora stanowiącą **załącznik nr 29.**
8. Sprostowanie danych następuje na pisemny wniosek osoby, której dane dotyczą.
9. Jeżeli sprostowanie dotyczy zbiorów, czynności przetwarzania lub systemów obejmujących wiele komórek organizacyjnych IOD przekazuje informacje o konieczności uaktualnienia danych osobowych zgodnie z żądaniem.
10. Usuwanie danych osobowych i ich przeglądanie pod kątem ograniczenia przechowywania:
    a) spoczywa na użytkowniku profilu środowiskowego w przypadku danych w tym profilu,
    b) administratorze danego systemu po zgłoszeniu przez użytkownika, w przypadku danych w systemie,
    c) kierownika komórki organizacyjnej w przypadku prowadzonych spraw,
    d) archiwiście zakładowym w przypadku dokumentów zarchiwizowanych;
11. Okresy przechowywania danych osobowych i zalecane przeglądy zostały wskazane w **załączniku nr 30.**

§ 21

Regulamin monitoringu wizyjnego

1. W Starostwie Powiatowym w Stalowej Woli monitoring wizyjny prowadzony jest w celu zapewnienia bezpieczeństwa publicznego oraz ochrony mienia na podstawie Ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2020 r. poz. 920).
2. Nagranie z monitoringu wizyjnego zapisywane jest automatycznie na rejestratorze i jest przechowywane maksymalnie przez 14 dni, potem ulega automatycznemu nadpisaniu i zostaje trwale usunięte.
3. Nagranie obrazu z rejestratora z wykorzystaniem systemu informatycznego na trwałe nośniki informatyczne (np. płyty CD, pendrive) następuje:
    1) w związku z realizacją wniosku o jego udostępnienie przez osobę, której dane dotyczą,
    2) gdy przepis prawa lub postanowienie sądowe nakazuje zgranie obrazu i jego przechowywanie,
    3) zaistniała konieczność dochodzenia roszczeń, a nagranie jest materiałem dowodowym.
4. Nagranie na nośniku informatycznym może być przechowywane przez okres nieprzekraczający 3 miesięcy od dnia zapisu na rejestratorze, chyba że:
    1) przepis prawa lub postanowienie sądowe nakazuje dłuższe jego przechowywanie,
    2) zaistniała konieczność dochodzenia roszczeń, a nagranie jest materiałem dowodowym.
5. Dostęp do nagrań mają uprawnione przez administratora osoby.
6. Udostępnienie nagrań następuje na pisemny wniosek, stanowiący załącznik nr 14, podmiotów uprawnionych do ich otrzymania zgodnie z przepisami prawa.
7. Wniosek o udostępnienie nagrania, jeżeli przepis prawa bądź postanowienie sądu nie nakazuje jego udostępnienia, może zostać rozpatrzony przez Administratora negatywnie z uwagi na naruszenie praw i wolności osób znajdujących się na nagraniu.

8. Nagranie może być udostępnione w zakresie obejmującym tylko zaistniałe zdarzenie bądź fragment, na którym widoczna jest osoba, która wnosi o udostępnienie, chyba przepis prawa bądź postanowienie sądu wskazuje inaczej.
9. Teren objęty monitoringiem wizyjnym oznaczony został tabliczkami „Teren monitorowany" lub „Obiekt monitorowany".
10. Na nagraniach pochodzących z monitoringu wizyjnego przetwarzany jest wizerunek, ewentualnie numery tablic rejestracyjnych i nazwy marek pojazdów, które znalazły się w obrębie rejestracji obrazu.
11. Klauzule informacyjne, zgodnie z art. 13 RODO, zostały umieszczone przy tabliczkach „Obiekt monitorowany".

§ 22

Przetwarzanie danych osobowych przez Radnych

1. Dokumentację w wersji papierowej pozyskaną w związku ze sprawowaną funkcją radnego zawierającą dane osobowe, których zakończył się cel przetwarzania, Radny zobligowany jest do przekazania na stanowisko ds. obsługi Rady Powiatu w celu jej trwałego zniszczenia.
2. Dokumentację w wersji elektronicznej pozyskaną w związku ze sprawowaną funkcją radnego zawierającą dane osobowe, których zakończył się cel przetwarzania Radny zobligowany jest do trwałego usunięcia.
3. Dokumentację w wersji papierowej Radny może w trakcie wykonywania mandatu przechowywać w Starostwie Powiatowym w Stalowej Woli stanowisku ds. obsługi Rady Powiatu.
4. Radny zobligowany jest do zabezpieczania dokumentacji tak, aby jej w sposób przypadkowy lub niezgodny z prawem nie zniszczyć, nie utracić, nie zmodyfikować, nie ujawnić lub dopuścić osoby nieuprawnione do jej wglądu.
5. Korzystając z prywatnych środków komunikacji jak e-mail lub telefon Radny zobowiązany jest do usunięcia danych osobowych, których cel przetwarzania się zakończył.
6. Przy przetwarzaniu danych osobowych w związku ze sprawowaniem mandatu Radni zobligowani są do stosowania niniejszej Polityki.
7. Radni są administratorami danych osobowych przetwarzanych w związku z realizacją art. 21 ust. 2a Ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2020 r. poz. 920).

§ 23

Przekazywanie danych osobowych telefonicznie

1. Przekazywanie danych osobowych poprzez rozmowę telefoniczną jest możliwe po weryfikacji tożsamości rozmówcy oraz sprawdzenia upoważnienia do otrzymania żądanych informacji.
2. Można w trakcie rozpatrywania sprawy ustalić z petentem, że może otrzymać informacje telefonicznie po przekazaniu np. znaku sprawy lub innego kodu/ numeru identyfikacyjnego ustalonego w komórce organizacyjnej.
3. Przykładowe pytania sprawdzające rozmówcę, poza podaniem imienia i nazwiska:
   1) proszę podać numer PESEL,
   2) proszę wskazać miejsce i datę urodzenia,
   3) proszę podać znak sprawy i adres zamieszkania,
   4) proszę opisać sprawę – podać szczegóły sprawy,
   5) proszę podać serię i nr dowodu osobistego;

§ 24

1. Dane osobowe muszą być przetwarzane zgodnie z przepisami prawa europejskiego i krajowego dotyczącymi ochrony danych osobowych oraz zgodnie z niniejszą Polityką.
2. Dane osobowe należy również przetwarzać zgodnie z Wytycznymi Grupy Roboczej 29 i innymi zaleceniami organów europejskich oraz zaleceniami organu nadzorczego.
3. W sprawach nieuregulowanych w niniejszej Polityce stosuje się przepisy prawa europejskiego i krajowego.
4. Materiały dotyczące ochrony danych osobowych znajdują się w biuletynie wewnętrznym dla pracowników Starostwa Powiatowego w Stalowej Woli pod adresem sieciowym http://10.161.203.30, w zakładce „Ochrona danych osobowych" lub na stronie Urzędu Ochrony Danych Osobowych – uodo.gov.pl
5. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
6. Osoba naruszająca Politykę może być decyzją Administratora danych osobowych poddana postępowaniu dyscyplinarnemu zgodnie z zasadami panującymi w podmiocie.
7. IOD oraz ASI raz na dwa lata lub w razie konieczności częściej przeprowadzają sprawdzenie aktualności przyjętej Polityki.

Starosta Stalowowolski

Janusz Zarzeczny
(podpisano kwalifikowanym podpisem elektronicznym)

Wykaz załączników do Polityki Ochrony Danych Osobowych:

1. Wzór upoważnienia i polecenia do przetwarzania danych osobowych.
2. Wzór rejestru upoważnień.
3. Karta zwrotu stanowiska.
4. Wzór umowy powierzenia danych osobowych.
5. Wzór rejestru umów powierzenia.
6. Przykłady naruszeń oraz działań zaradczych.
7. Raport z naruszeń ochrony danych osobowych.
8. Wzór rejestru naruszeń ochrony danych osobowych.
9. Wzór rejestru czynności i rejestru kategorii czynności.
10. Metodologia analizy ryzyka.
11. Wzór klauzuli informacyjnej.
12. Wzór klauzuli wyrażenia zgody.
13. Opis systemów informatycznych.
14. Wzór wniosku o udostępnienie danych osobowych
15. Wzór ewidencji odbioru kluczy stażystów i praktykantów.
16. Oświadczenie o posiadaniu kluczy do drzwi wejściowych i Kancelarii Ogólnej.
17. Rysunek połączenia szyfrowanego.
18. Wzór wniosku o udostępnienie informacji i kopii danych osobowych.
19. Oświadczenie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli.
20. Wyrażenie zgody na przebywanie w obszarze przetwarzania danych osobowych.
21. Zgłoszenie korzystania z prywatnego sprzętu IT.
22. Zgoda na wynoszenie dokumentów poza budynki administratora.
23. Wniosek o nadanie upoważnienia dla osoby przetwarzającej dane osobowe.
24. Wzór klauzul informacyjnych w związku z postępowaniem administracyjnym.

25. Informacja o przekazaniu danych osobowych do państwa trzeciego.
26. Formularz zgłoszenia naruszenia ochrony danych osobowych.
27. Opis metody ENISA.
28. Rejestr klauzul wyrażeń zgody.
29. Analiza interesu nadrzędnego administratora.
30. Przykładowe okresy przechowywania danych osobowych.
31. Zapisy o ochronie danych osobowych do umów.
32. Pytania kontrolne pomagające w wyborze procesora.

Data wydania:

STAROSTA STALOWOWOLSKI

UPOWAŻNIENIE I POLECENIE PRZETWARZANIA NR

Na podstawie art. 29 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 (Dz. Urz. UE L 119 z 04.05.2016) wraz ze sprostowaniem **upoważniam Pana/ią:**

……
Imię i nazwisko

zatrudnioną/nego lub odbywającego/cą staż/praktyki w Starostwie Powiatowym w Stalowej Woli na stanowisku … w Wydziale/Referacie… na podstawie … **do dostępu oraz przetwarzania danych osobowych wyłącznie do celów służbowych i w zakresie czynności ujętych w karcie zadań, a przede wszystkim do …** *(wpisać czynność przetwarzania danych osobowych oraz jeżeli dotyczy - system informatyczny, do którego upoważniony będzie miał dostęp).*

Polecam Panu przetwarzanie danych osobowych w powyższym zakresie i celu. Upoważnienie i polecenie wydaje się na czas trwania stosunku pracy (*w przypadku umów na czas określony, staży, praktyk – wpisać okres upoważnienia).* Upoważnienie i polecenie traci ważność z chwilą *ustania lub rozwiązania stosunku pracy/ zakończenia stażu lub praktyk.*

Inspektor Ochrony Danych

Administrator Danych Osobowych

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Zobowiązuje się **do zachowania w tajemnicy** dane osobowe, które przetwarzałam/em i do których miałam/em dostęp oraz sposoby ich zabezpieczenia, w trakcie zatrudnienia oraz po ustaniu *stosunku prac/ zakończeniu stażu lub praktyk.*

Data i czytelny podpis osoby upoważnionej

1) Szkolenie z zakresu ochrony danych osobowych:

1. Przepisy europejskie i krajowe dotyczące ochrony danych osobowych.
2. Podstawowe definicje i zasady przetwarzania danych osobowych – art. 4-11 RODO.
3. Realizacja obowiązku informacyjnego.
4. Pozostałe prawa osób, których dane dotyczą.
5. Środki zabezpieczeń fizycznych i organizacyjnych.
6. Zapoznanie z Polityką ochrony danych osobowych.
7. Zgłaszanie naruszeń ochrony danych osobowych.
8. Rola organu nadzorczego, IOD oraz środki ochrony prawnej, sankcje i odpowiedzialność.

……..
data i podpis Inspektora Ochrony Danych Osobowych

2) Szkolenie z zakresu zabezpieczeń informatycznych:

……..
data i podpis Administratora Systemów Informatycznych

Rejestr upoważnień do przetwarzania danych osobowych w Starostwie Powiatowym w Stalowej Woli

za okres od:

Nr Rejestru	Data wydania	Nazwisko i imię / stanowisko	Wydział	Podstawa zatrudnienia	Okres na który wydano upoważnienie	Zakres upoważnienia	ID do komputera ID do EZD ID inne

KARTA ODDANIA STANOWISKA PRACY

PO USTANIU ZATRUDNIENIA LUB W PRZYPADKU ZMIANY STANOWISKA PRACY

Imię i nazwisko pracownika……..

Dotychczasowe stanowisko……..

	Data	**Uwagi**	**Podpis odbierającego**	**Podpis pracownika**
Zwrot karty do rejestratora czasu pracy – na stanowisko ds. osobowych lub IOD				
Zwrot nośnika informatycznego wraz z rodzajem – do głównego informatyka urzędu lub starszy informatyk				
Przekazanie akt spraw i innych dokumentów - do KKO				
Inne zwroty/ przekazania – do KKO				
Profil użytkownika				
Poczta elektroniczna				

KARTĘ ODDANIA STANOWISKA PRACY NALEŻY ODDAĆ INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

UMOWA Nr

POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ……..pomiędzy **Administratorem Danych Osobowych** - *Starostą Stalowowolskim/ Powiatem Stalowowolskim reprezentowanym przez Zarząd Powiatu, w imieniu którego działają Starosta Stalowowolski oraz Wicestarosta Stalowowolski/ Powiatem Stalowowolskim reprezentowanym przez Starostę Stalowowolskiego z siedzibą Starostwa Powiatowego w Stalowej Woli* przy ul. Podleśnej 15, 37 – 450 Stalowa Wola, zwanym w dalszej części umowy **Powierzającym**,

a

……

zwanym dalej **Przetwarzającym**

§ 1

PRZEDMIOT I CZAS TRWANIA PRZETWARZANIA DANYCH OSOBOWYCH

1. W ramach umowy Powierzający jako Administrator Danych, zgodnie z art. 28 ust. 3 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 (Dz. Urz. UE L 2016, Nr 119, s. l) zwanym dalej "RODO", powierza czynności związane z przetwarzaniem danych osobowych w zakresie: *należy wpisać zakres czynności, w ramach których następuje powierzenie np. świadczenia usług tłumaczenia/ serwisu.*
2. Poprzez zawarcie Umowy Administrator poleca przetwarzanie danych osobowych Przetwarzającemu, a także każdej osobie działającej z upoważnienia Podmiotu przetwarzającego mającej dostęp do danych osobowych, co stanowi udokumentowane polecenie w rozumieniu art. 28 ust. 3 lit. a) w związku z art. 29 RODO.
3. Przedmiotem powierzenia są dane osobowe przetwarzane w: *aktach spraw/ systemie informatycznym/ bazie danych.*
4. Przetwarzanie odbywać się będzie przez okres: *wpisać okres przetwarzania np. na czas trwania umowy głównej*
5. Przetwarzający oświadcza, że zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO

i chroniło prawa osób, których dane zostały powierzone zgodnie z art. 28 ust. 1 oraz art. 32 RODO.

6. Przez *naruszenie ochrony danych osobowych* należy rozumieć naruszenie, o którym mowa w art. 4 pkt 12 RODO.

§ 2

CHARAKTER I CEL PRZETWARZANIA, RODZAJ DANYCH OSOBOWYCH ORAZ KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Powierzenie przetwarzania, o którym mowa w § 1 następuje w celu*: wpisać cel powierzenia np. w celu wsparcia technicznego i serwisu programu …/ sporządzenia dokumentacji księgowej/ wykonania usług archiwizacji/ usunięcia danych osobowych/ sporządzenia tłumaczenia.*
2. Przetwarzanie przez Przetwarzającego danych osobowych objętych niniejszą umową w celach innych niż wynikające z niniejszej umowy jest niedozwolone.
3. Powierzający powierza do przetwarzania następujący rodzaj danych osobowych: np. *dane zwykłe zawarte w przedłożonych przez stronę dokumentach/ dane szczególne, o których mowa w art. 9 ust. 1 RODO w zakresie stanu zdrowia/ dane, o których mowa w art. 10 RODO.*
4. Przetwarzanie obejmuje czynności takie jak: *operacja/ zestaw operacji wykonywanych na danych osobowych/ zestawach danych osobowych/ w sposób zautomatyzowany/ niezautomatyzowany m.in.: (wybrać właściwe) 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;*
5. Powierzone dane osobowe *nie będą/ będą* przekazywane przez Przetwarzającego do państw trzecich.
6. Powierzenie będzie obejmować: *wpisać kategorię osób, których powierzenie dotyczy np. pracowników Powierzającego*, *mieszkańców powiatu stalowowolskiego, inwestorów, strony postępowań.*

§ 3

OBOWIĄZKI I PRAWA ADMINISTRATORA ORAZ PODMIOTU PRZETWARZAJĄCEGO

1. Przetwarzający zobowiązuje się do:

1) przetwarzania danych osobowych wyłącznie w celu określonym w niniejszej umowie oraz nieudostępniania danych osobom nieuprawnionym,
2) zastosowania przy przetwarzaniu danych osobowych środków technicznych i organizacyjnych zapewniających ochronę danych w zakresie określonym w art. 32 RODO zgodnie z art. 28 ust. 3 lit. c RODO,

3) dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających nadane upoważnienie do przetwarzania danych osobowych oraz prowadzenie ewidencji tych osób,
4) zapewnienia, że osoby, które zostały przez niego upoważnione do przetwarzania danych osobowych, będą zachowywały w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia w czasie obowiązywania niniejszej umowy oraz po jej rozwiązaniu, a także po ustaniu stosunku pracy,
5) niezwłocznego poinformowania Powierzającego o wszelkich naruszeniach ochrony danych osobowych i informacjach mogących mieć wpływ na bezpieczeństwo przetwarzania powierzonych danych;

2. Przetwarzający pomaga Powierzającemu wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw, określonych w rozdziale III RODO, zgodnie z art. 28 ust. 3 lit. e RODO.
3. Przetwarzający przekazuje informacje na wniosek Powierzającego w związku z wykonywaniem praw, o których mowa w ust. 2, niezwłocznie, maksymalnie w ciągu 21 dni od dnia otrzymania wniosku.
4. Przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Powierzającemu wywiązać się z obowiązków określonych w art. 32-36 RODO.
5. Przetwarzający w celu wywiązania się z obowiązku określonego w ust. 4 odpowiada na wniosek Powierzającego niezwłocznie, maksymalnie w ciągu 21 dni od dnia otrzymania wniosku.
6. Po zakończeniu realizacji umowy Przetwarzający zobowiązuje się niezwłocznie, maksymalnie w ciągu 21 dni, zwrócić wszelkie powierzone mu do przetwarzania dane osobowe lub trwale je usunąć wraz z wszelkimi istniejącymi kopiami, chyba że istnieją przepisy prawa zezwalające na ich dalsze przechowywanie.
7. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Powierzającego o:

1) jakimkolwiek postępowaniu administracyjnym lub sądowym, decyzji administracyjnej, orzeczeniu, zapowiedzianych kontrolach i inspekcjach, jeśli dotyczą one danych osobowych powierzonych przez Powierzającego,
2) każdym nieupoważnionym dostępie do danych osobowych i innych naruszeniach ochrony danych osobowych,
3) każdym żądaniu otrzymanym bezpośrednio od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie;

§ 4

1. Przetwarzający może powierzyć wykonanie części czynności niniejszej umowy innemu podmiotowi tylko na podstawie pisemnej umowy po wcześniejszej akceptacji przez Powierzającego.

2. Powierzający zastrzega sobie możliwość przeprowadzenia kontroli Przetwarzającego w zakresie przestrzegania wymagań wynikających z art. 28 RODO, w tym wypełniania zapisów niniejszej umowy, zgodnie z art. 28 ust. 3 lit. h RODO:
3. W przypadku stwierdzonych naruszeń ochrony danych osobowych Powierzający przeprowadza niezwłocznie kontrolę doraźną, a w pozostałych przypadkach Powierzający przeprowadza kontrolę po zawiadomieniu Przetwarzającego 7 dni przed dniem planowanej kontroli.
4. Po kontroli Powierzający może przekazać Przetwarzającemu pisemne zalecenia pokontrolne wraz z terminem ich realizacji.
5. Przetwarzający zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
6. Przetwarzający zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Powierzającego dotyczące przetwarzania powierzonych mu w związku z realizacją niniejszej umowy danych osobowych.

§ 5

1. Przetwarzający przyjmuje do wiadomości, iż podczas realizacji niniejszej umowy w zakresie przestrzegania przepisów RODO, ponosi odpowiedzialność jak Powierzający.
2. Przetwarzający odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez niego powierzonych danych osobowych i naruszaniem RODO.
3. W przypadku naruszenia przepisów o ochronie danych osobowych w ramach realizacji niniejszej umowy z przyczyn leżących po stronie Przetwarzającego, w następstwie którego Powierzający zostanie zobowiązany do wypłaty odszkodowania lub ukarany grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Przetwarzający zobowiązuje się do zwrócenia równowartości odszkodowania lub grzywny poniesionych przez Powierzającego.
4. W przypadku naruszenia postanowień niniejszej umowy Powierzający może natychmiastowo rozwiązać umowę o powierzeniu przetwarzania danych osobowych oraz Umowę podstawową z winy Przetwarzającego.

§ 6

Powierzający zobowiązuje się do niezwłocznego przekazywania Przetwarzającemu wszelkich informacji, które mogą mieć wpływ na bezpieczeństwo danych osobowych przetwarzanych w ramach niniejszej umowy.

§ 7

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy powszechnie obowiązującego prawa.

2. Wszelkie zmiany lub uzupełnienia niniejszej umowy dla swojej ważności wymagają formy pisemnej.
3. Umowa wchodzi w życie z dniem podpisania.
4. Spory wynikłe z tytułu niniejszej umowy będzie rozstrzygał sąd właściwy dla siedziby Powierzającego.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron umowy.

…… ……

Przetwarzający Powierzający

Wzór rejestru umów powierzenia

Nr umowy	Podmiot przetwarzający	Okres	Miejsce przechowywania/ osoba odpowiedzialna	Zakres umowy

Formy naruszeń ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych i sposoby postępowania

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
INFORMACJA, DOKUMENTY, WIEDZA	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Odpowiednio zabezpieczyć dokumenty, zmienić sposób pracy. Zawiadomić IOD.
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Ujawnienie danych osobowych osobom nieupoważnionym	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
Kradzież dokumentów	Zawiadomić IOD lub ADO, w razie konieczności policję. Zgłosić naruszenie do organu nadzorczego. Powiadomić osoby, których dane dotyczą. Podjąć działania w celu odzyskania danych.
Zagubienie dokumentów	Zawiadomić IOD lub ADO. Zgłosić naruszenie do organu nadzorczego. Powiadomić osoby, których dane dotyczą. Podjąć działania w celu odzyskania danych.
Zniszczenie dokumentów	Zawiadomić IOD lub ADO. Zgłosić naruszenie do organu nadzorczego. Powiadomić osoby, których dane dotyczą. Podjąć działania w celu odzyskania danych.
Zalanie	Zawiadomić IOD. Podjąć działania w celu odzyskania danych np. wysuszenie. W przypadku dużego zalania i utraty danych: zgłosić naruszenie do organu nadzorczego, powiadomić osoby, których dane dotyczą.
Zanieczyszczenie	Zawiadomić IOD. Podjąć działania w celu odzyskania danych. W przypadku dużego zanieczyszczenia i utraty danych: zgłosić naruszenie do organu nadzorczego, powiadomić osoby, których dane dotyczą.
Nieprzestrzeganie zasady ograniczenia celu	Usunąć lub zanonimizować dane, które są zebrane niezgodnie z celem.
Nieprzestrzeganie zasady minimalizacji danych	Usunąć lub zanonimizować dane nadmiarowe.
Nieprzestrzeganie zasady prawidłowości danych	Podjąć działania mające na celu sprostowanie danych.
Nieprzestrzeganie zasady ograniczenia przechowywania	Usunąć lub zarchiwizować dane, które nie są już wykorzystywane do prowadzenia sprawy.

Przetwarzanie danych bez podstaw prawnych	Usunąć lub zanonimizować dane, które są zebrane bez podstaw prawnych.
Błąd użytkownika/ prowadzącego sprawę	Wezwać ASI – w przypadku błędu informatycznego. Powiadomić przełożonego. Ustalić środki zaradcze.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić IOD.
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji.
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Zablokować dostęp do aplikacji.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Zabrać kartkę. Niezwłocznie powiadomić IOD.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działanie programów. Niezwłocznie powiadomić IOD.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać ASI w celu odinstalowania programów.
Modyfikowanie parametrów systemu i aplikacji, w tym sfałszowanie oprogramowania.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Przywróć poprzednie parametry. Ustalić co zostało zmienione i jak wpłynęło to na przetwarzane dane.
Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać ASI w celu wykonania kontroli antywirusowej.
Dane z nieautoryzowanych źródeł	Wezwać ASI w celu sprawdzenia możliwego źródła pochodzenia danych. Ustalić z IOD i KKO dalsze postępowanie np. zablokować działanie aplikacji, usunąć dane.
Niewłaściwe funkcjonowanie urządzeń	Wezwać ASI w celu sprawdzenia przyczyn niewłaściwego funkcjonowania. Przywrócić urządzenie do poprawnego działania bądź je wymienić.
Manipulowanie danymi, w tym atak hackerski, przełamanie zabezpieczeń	Wezwać ASI. Sprawdzić dzienniki logów, historię dokumentów. Zablokować dostęp do aplikacji bądź kontrolować postępowanie hackera. Zmienić dane dostępowe - login i hasło, podnieść poziom zabezpieczeń. Sprawdzić rozmiar zmian i

	wpływ na działanie podmiotu. Wyciągnąć konsekwencje wobec pracowników, jeżeli to pracownik dopuścił się naruszenia. W razie konieczności zawiadomić policję, organ nadzorczy i osoby, których dane dotyczą.
Zniszczenie, awaria urządzeń	Wezwać ASI. Sprawdzić rozmiar zniszczenia i jego wpływ na działanie podmiotu. Dokonać naprawy lub wymiany sprzętu na nowy.
Przeciążenie systemu informatycznego	Wezwać ASI. Sprawdzić przyczyny przeciążenia. Podjąć działania zaradcze np. zakup pamięci, dodatkowego dysku.
Błędy utrzymania systemu	Sprawdzenia dokonuje ASI. Zmienić sposób utrzymania systemu. Naprawić błąd.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport.
Pobranie załącznika ze złośliwym oprogramowaniem	Niezwłocznie wezwać ASI.
Ujawnienie hasła nieuprawnionym osobom	Niezwłocznie zmienić hasło. Poinformować ASI. Monitorować „ruch” w systemie.
Niewłaściwe udostępnienie danych BIP i na stronie internetowej	Powiadomić KKO i ASI. Niezwłocznie poprawić lub usunąć niewłaściwie udostępnione dane.
Wysłanie e-mail z danymi osobowymi do niewłaściwego adresta	Powiadomić KKO i IOD.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie. Powiadomić KKO.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić ASI i IOD.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić ASI i IOD.
Zgubienie kluczy do pomieszczeń i budynku	Niezwłocznie zgłosić na stanowisko ds. administracyjnych i IOD. Wymienić wkładki i kupić nowe klucze. W razie konieczności zmienić kod alarmu.

W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić ASI i IOD.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić IOD i ASI.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie ASI lub IOD.
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Powiadomić niezwłocznie ASI lub IOD.

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w …….

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:
Kroki opisu
1. Kategorie danych osobowych…
2. Liczba osób, których dane naruszono…
3. Rodzaj naruszenia (tradycyjne dane, system informatyczny, umyślne, nieumyślne)…

5. Przyczyny wystąpienia zdarzenia (sprawdzić sposoby dotychczasowych zabezpieczeń, zrobić analizę ryzyka ponownie):
……..
……..
……..

6. Podjęte działania:
……..
……..
……..

7. Postępowanie wyjaśniające z informacją czy należy zgłaszać incydent do organu nadzorczego:
……..
……..
……..

…….
Data i podpis osoby przeprowadzającej działanie wyjaśniające

Rejestr naruszeń ochrony danych osobowych

Data zdarzenia	Rodzaj zdarzenia	Opis	Wymaga zgłoszenia do organu nadzorczego TAK/NIE	Wymaga powiadomienia osób, których dane dotyczą TAK/NIE

Rejestr czynności przetwarzania danych osobowych

Nazwa i dane kontaktowe administratora danych:

Imię i nazwisko inspektora ochrony danych osobowych:

Wydział	Lp.	Nazwa procesu przetwarzania	Nazwa i dane kontaktowe współadministratora danych	Cele przetwarzania	Kategorie odbiorców	Opis kategorii osób, których dane dotyczą	Opis kategorii danych osobowych	Dokumentacja zabezpieczeń - gdy dane przekazywane są do państwa trzeciego lub organizacji międzynarodowej - (*w tym nazwa państwa, do którego dane są przekazywane*)	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

REJESTR KATEGORII PRZETWARZANIA DANYCH OSOBOWYCH

Nazwa podmiotu przetwarzającego:

Dane kontaktowe podmiotu przetwarzającego:

Nazwa i dane kontaktowe administratora danych osobowych	Imię i nazwisko i dane kontaktowe inspektora danych osobowych	Kategorie przetwarzań	Dokumentacja zabezpieczeń - gdy dane przekazywane są do państwa trzeciego lub organizacji międzynarodowej - (*w tym nazwa państwa, do którego dane są przekazywane*)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Metodologia analizy ryzyka

1. **Identyfikacja zasobów.**
   Analizą ryzyka zajmuje się Inspektor ochrony danych osobowych, Administrator systemów informatycznych we współpracy z Kierownikami komórek organizacyjnych. Wyszczególnia się następujące aktywa:
   1) czynności przetwarzania danych osobowych,
   2) zasoby ludzkie,
   3) infrastrukturę informatyczną (m.in. sprzęt informatyczny, oprogramowanie, aplikacje, narzędzia informatyczne, strony internetowe, Biuletyn Informacji Publicznej).

W identyfikacji zasobów bierze się pod uwagę czynności przetwarzania danych wpisane do rejestru czynności przetwarzania danych osobowych.

2. **Szacowanie wartości zasobów.**
   Po identyfikacji zasobów następuje ocena ich wartości dla podmiotu według skali:

a) wartość dla czynności przetwarzania danych osobowych:

Skala wartości informacji	Opis
wysoka	Dane szczególnej kategorii lub dane art. 10 RODO albo następuje przekazywanie danych do państwa trzeciego albo dane dotyczą głównej działalności Starostwa Powiatowego w Stalowej Woli (największa liczba realizowanych usług)
średnia	Przetwarzanie danych w systemie informatycznym i brak danych szczególnej kategorii lub danych art. 10 RODO bądź średnia warto ść informacji pod kątem liczby realizowanych usług
niska	Dane przetwarzane w wersji papierowej i brak danych szczególnej kategorii lub danych art. 10 RODO bądź niska wartość pod kątem liczby realizowanych usług

b) wartość dla infrastruktury informatycznej:

Skala wartości informacji	Opis
wysoka	Ponad 20 użytkowników i dane przetwarzane stale lub zawiera dane szczególnej kategorii albo dane dotyczące wyroków skazujących lub następuje przepływ danych do państw trzecich
średnia	10-20 użytkowników lub dane przetwarzane stale, brak danych art. 9 i art. 10 RODO

niska	Dane przetwarzane sporadycznie, brak danych art. 9 i art. 10, poniżej 10 użytkowników

c) wartość dla zasobów ludzkich:

Skala wartości informacji	Opis
wysoka	Ponad 20 użytkowników i dane przetwarzane stale lub zawiera dane szczególnej kategorii albo dane dotyczące wyroków skazujących lub następuje przepływ danych do państw trzecich
średnia	10-20 użytkowników lub dane przetwarzane stale, brak danych art. 9 i art. 10 RODO
niska	Dane przetwarzane sporadycznie, brak danych art. 9 i art. 10, poniżej 10 użytkowników

3. Szacowanie ryzyka.

Przyjmuje się, że podstawową zasadą ochrony danych jest ochrona danych osobowych pod kątem integralności, poufności i dostępności.

Przy szacowaniu ryzyka bierze się pod uwagę przede wszystkim czynniki takie jak:

1. Lokalizacja jednostki i obszarów przetwarzania danych osobowych.
2. Stosowane dotychczasowe środki zabezpieczeń.
3. Kategorie przetwarzanych danych osobowych.
4. Występowanie powierzenia danych osobowych.
5. Doświadczenie osób przetwarzających dane osobowe.
6. Sposób przetwarzania danych osobowych (wersje papierowe, systemy informatyczne).
7. Kategorie odbiorców.

Zasoby szacuje się pod kątem skutków (S) utraty dla poufności, integralności i dostępności według skal:

Poufność - dopasowanie do kategorii danych	**Dla ADO**
zwykłe	(1-2)
szczególna kategoria danych osobowych	3
dane art. 10 RODO (wyroki skazujące, dane dotyczące naruszeń prawa)	3
nie dotyczy	0
Integralność	
niskie	1
średnie	2
wysokie	3
krytyczne	4
nie dotyczy	0

Dostępność - poza systemami rozumiana jako brak dostępności do dokumentów papierowych		Dostępność dla zasobów ludzkich	
niskie wymagania - nie ma większego wpływu na realizację zadań w dłuższym przedziale czasu	1	Niskie wymagania - nieobecność powyżej 14 dni nie zaburza wykonywania zadań przez komórkę	1
średnie wymagania - ma znaczący wpływ na realizację zadań, dostęp musi nastąpić w ciągu kilku dni	2	Średnie wymagania - nieobecność powyżej 14 dni zaburza wykonywanie zadań w komórce	2
wysokie wymagania - niedostępność powoduje duże szkody, dostęp musi być przywrócony w ciągu kilku godzin	3	Wysokie wymagania - dłuższa nieobecność zaburza funkcjonowanie urzędu	3
ekstremalne wymagania - sparaliżowanie pracy, dostęp następuje w ciągu kilku minut	4	Absolutne wymagania - stanowisko musi być zawsze obsadzone	4
nie dotyczy	0		

Szacuje się również poziom (niski, średni, wysoki) dla następujących zagrożeń z uwzględnieniem czynnika (N- natura, U – umyślny, P – przypadkowy) jego występowania:

Numer zagrożenia	Zagrożenie	Czynnik	Poziom
ZG - 1	Pożar	N, U, P	
ZG - 2	Kradzież dokumentów	U	
ZG - 3	Odtworzenie z wyrzuconych nośników	U	
ZG - 4	Dane z nieautoryzowanych źródeł	U, P	
ZG - 5	Manipulowanie urządzeniem	U	
ZG - 6	Sfałszowanie oprogramowania	P, U	
ZG - 7	Niewłaściwe funkcjonowanie urządzeń	P	
ZG - 8	Zalanie	N, U, P	
ZG - 9	Przetwarzanie danych bez podstaw prawnych	U	
ZG - 10	Nieautoryzowane użycie urządzenia	U	
ZG - 11	Manipulowanie danymi	U	
ZG - 12	Zniszczenie urządzeń	N, U, P	
ZG - 13	Podsłuch	U	
ZG - 14	Kradzież nośników	U	
ZG - 15	Kradzież danych	U	
ZG - 16	Ujawnienie	U, P	
ZG - 17	Awaria urządzenia	P	
ZG - 18	Zniszczenie dokumentów	P, U	
ZG - 19	Przeciążenie systemu informatycznego	P, U	
ZG - 20	Niewłaściwe funkcjonowanie oprogramowania	P	
ZG - 21	Zniekształcenie danych	U	
ZG - 22	Fałszowanie praw	U	
ZG - 23	Przełamanie zabezpieczeń dostępu wewnątrz systemu	U	
ZG - 24	Przełamanie zabezpieczeń systemu z sieci zewnętrznej	U	
ZG - 25	Błędy utrzymania systemu informatycznego	U, P	
ZG - 26	Zanieczyszczenie	N, U, P	
ZG - 27	Nieuprawnione kopiowanie oprogramowania	U	
ZG - 28	Odmowa działania	P	
ZG - 29	Zakłócenie dostępności personelu	P	
ZG - 30	Utrata dostaw prądu	N, U, P	
ZG - 31	Awaria urządzenia telekomunikacyjnego	U, P	

ZG - 32	**Błąd użytkownika**	**P**	
ZG - 33	**Nieautoryzowany dostęp do informacji**	**U**	
ZG - 34	**Nieumiejętne posługiwanie się systemem przez użytkownika**	**P**	
ZG-35	**Nieprzestrzeganie zasady ograniczenia celu**	**P, U**	
ZG-36	**Nieprzestrzeganie zasady minimalizacji danych**	**U, P**	
ZG-37	**Nieprzestrzeganie zasady prawidłowości danych**	**P, U**	
ZG-38	**Nieprzestrzeganie zasady ograniczenia przechowywania**	**P, U**	

Następnym krokiem jest oszacowanie podatności (P) zasobu pod kątem jego podatności na wystąpienie danego zagrożenia z uwzględnieniem systemów zabezpieczeń, kategorii przetwarzanych danych, sposobu przetwarzania danych, sposobu pracy pracowników i ich lat pracy na danym stanowisku, liczby stażystów lub praktykantów, kanałów przekazywania danych, liczby tworzonej dokumentacji, liczby obsługiwanych petentów, częstotliwości występowania.

Skala podatności:

brak (0),

niski poziom (1-2),

średni poziom (3-4),

wysoki poziom (5-6),

ekstremalny (7)

4. Analiza ryzyka.

Ryzyko analizuje się dla każdego zasobu pod kątem integralności, poufności i dostępności zgodnie ze wzorem:

R (ryzyko)= S (skutek) x P (podatność)

Przyjęto następujące poziomy ryzyka – zgodnie z regułą Pareto

Poziomy ryzyka zmniejszają się o wartość 20% z maksymalnego ryzyka (R) tj. 28*0,2=5,6 zaokr. 6

Poziom	**Wartości**		
znikome	0	6	*akceptacja ryzyka pasywna*
niskie	7	13	*analiza + akceptacja ryzyka aktywna*
średnie	14	20	
wysokie	21	28	*nieakceptowalne ryzyko*

akceptacja pasywna	podjęcie działań gdy czynnik się uaktywni
akceptacja aktywna	podjęcie środków zaradczych

nieakceptowalne	wprowadzenie dodatkowych środków zabezpieczających lub zmiana obecnych

5. Ocena ryzyka.

Dla średniego i wysokiego poziomu ryzyka dokonuje się oceny. Ocena zawiera:

1) Opis zasobu z podaniem przyczyn wystąpienia ryzyka.
2) Środki zaradcze, z zastrzeżeniem, że dla maksymalnego poziomu ryzyka należy je podjąć niezwłocznie.
3) Konsekwencje naruszenia zasad ochrony danych osobowych dla administratora danych osobowych.
4) Konsekwencje naruszenia zasad ochrony danych osobowych dla osoby, których dane dotyczą.
5) Ewentualnie wnioski.

6. Monitorowanie analizy ryzyka.

Inspektor ochrony danych osobowych, Administrator systemów informatycznych we współpracy z Kierownikami komórek organizacyjnych raz do roku dokonuje przeglądu analizy ryzyka i w razie konieczności uaktualnia ją.

Obowiązek informacyjny w stosunku do osób, których dane dotyczą

(Nie ma zastosowania, gdy osoba poniższe informacje już zna np. składa po raz kolejny wniosek w tej samej sprawie)

1. Administratorem danych osobowych jest: *Starostwo Powiatowe w Stalowej Woli lub Starosta Stalowowolski/ Powiat Stalowowolski reprezentowany przez Zarząd Powiatu, w imieniu którego działają Starosta Stalowowolski oraz Wicestarosta Stalowowolski/ Powiat Stalowowolski reprezentowany przez Starostę Stalowowolskiego*, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. Dane kontaktowe inspektora ochrony danych: tel. 15 643 36 35, abi@stalowowolski.pl
3. Cele przetwarzania danych osobowych (*można wpisać: realizacja obowiązku prawnego i zacytować przepis prawa, realizacja umowy dotyczącej ..., działania promocyjne i wymienić ich charakter*): ……
4. Podstawa prawna przetwarzania zwykłych danych osobowych - *należy wskazać przepisy szczególne lub wybrać jedną wynikającą z RODO:*
    1) **wyrażenie zgody** - art. 6 ust. 1 lit. a) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
    2) **wykonanie umowy lub podjęcie działań przed podpisaniem umowy** - art. 6 ust. 1 lit. b) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
    3) **wypełnienie obowiązku prawnego** - art. 6 ust. 1 lit. c) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
    4) **zadanie realizowane w interesie publicznym lub w ramach sprawowanej władzy publicznej** - art. 6 ust. 1 lit. e) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);
5. Podstawa prawna przetwarzania danych osobowych kategorii szczególnej - *należy wskazać przepisy szczególne lub wybrać jedną wynikającą z RODO:*

1) **<u>wyraźne</u> wyrażenie zgody lub osoba, której dane dotyczą nie jest w stanie uchylić zakazu ich przetwarzania** - art. 9 ust. 2 lit. a) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
2) **wypełnienie obowiązków i wykonywanie praw w <u>dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej</u> w związku przepisami prawa -** art. 9 ust. 2 lit. b) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
3) **dane upublicznione przez osobę, której dane dotyczą -** art. 9 ust. 2 lit. e) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
4) **ustalenie, dochodzenie lub obrona roszczeń -** art. 9 ust. 2 lit. f) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
5) **ważny interes publiczny <u>na podstawie przepisów prawa</u> -** art. 9 ust. 2 lit. g) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
6) **cele archiwalne w interesie publicznym, badania naukowe lub historyczne, cele statystyczne <u>na podstawie przepisów prawa</u>** - art. 9 ust. 2 lit. j) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);

6. Podstawa prawna przetwarzania danych osobowych, o których mowa w art. 10 RODO tj. wyroków skazujących i czynów zabronionych:
7. Odbiorcy danych *(poza organami publicznymi prowadzącymi **konkretne** postępowanie na podstawie przepisów prawa), <u>jeżeli istnieją</u>: ……..*
8. Informacja dotycząca przekazania danych do państwa trzeciego, *jeżeli dotyczy*: ….
9. Okres, przez który dane będą przechowywane, a gdy nie jest możliwe jego ustalenie – kryteria ustalania okresu *np. wynikające z instrukcji archiwalnej (w latach, miesiącach, dniach):……..*

W obowiązku należy umieścić informacje o przysługujących osobie, której dane dotyczą prawach:

10. **Ma Pan/i prawo:**
    a) dostępu do treści swoich danych,
    b) sprostowania swoich danych osobowych,

c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych – można wskazać dane teleadresowe;

W przypadku, gdy przetwarzanie odbywa się w związku z wykonywaniem zadania realizowanego w interesie publicznym lub sprawowanej władzy publicznej, należy umieścić lit. e)

e) prawo wniesienia sprzeciwu wobec przetwarzania;

W przypadku, gdy przetwarzanie odbywa się na podstawie wyrażenia zgody lub na podstawie umowy i w sposób zautomatyzowany, należy umieścić lit. f)

f) prawo do przenoszenia danych;

11. Podanie danych jest - *wpisać odpowiednio: wymogiem ustawowym, umownym, warunkiem zawarcia umowy, dobrowolne oraz ewentualne konsekwencje niepodania danych osobowych*.

Ewentualnie:

POŚWIADCZAM, ŻE ZAPOZNAŁAM/EM SIĘ Z POWYŻSZYMI INFORMACJAMI I SĄ ONE DLA MNIE ZROZUMIAŁE.

……

Data i czytelny podpis

Obowiązek informacyjny podczas zbierania danych z innych źródeł

1. Administratorem danych osobowych jest: *Starostwo Powiatowe w Stalowej Woli lub Starosta Stalowowolski/ Powiat Stalowowolski reprezentowany przez Zarząd Powiatu, w imieniu którego działają Starosta Stalowowolski oraz Wicestarosta Stalowowolski/ Powiat Stalowowolski reprezentowany przez Starostę Stalowowolskiego*, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. Dane kontaktowe inspektora ochrony danych: tel. 15 643 36 35, abi@stalowowolski.pl
3. Cele przetwarzania danych osobowych (*można wpisać: realizacja obowiązku prawnego i zacytować przepis prawa, realizacja umowy dotyczącej ..., działania promocyjne i wymienić ich charakter*): ……
4. Kategorie danych (np. *imię, nazwisko, stan zdrowia; dane, o których mowa art. 9 ust. 1 RODO lub art. 10 RODO*): ……..
5. Podstawa prawna przetwarzania zwykłych danych osobowych - *należy wskazać przepisy szczególne lub wybrać jedną wynikającą z RODO:*
    1) **wyrażenie zgody** - art. 6 ust. 1 lit. a) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
    2) **wykonanie umowy lub podjęcie działań przed podpisaniem umowy** - art. 6 ust. 1 lit. b) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
    3) **wypełnienie obowiązku prawnego** - art. 6 ust. 1 lit. c) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
    4) **zadanie realizowane w interesie publicznym lub w ramach sprawowanej władzy publicznej** - art. 6 ust. 1 lit. e) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);
6. Podstawa prawna przetwarzania danych osobowych szczególnej - *należy wskazać przepisy szczególne lub wybrać jedną wynikającą z RODO:*

1) **<u>wyraźne</u> wyrażenie zgody lub osoba, której dane dotyczą nie jest w stanie uchylić zakazu ich przetwarzania** - art. 9 ust. 2 lit. a) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
2) **wypełnienie obowiązków i wykonywanie praw w <u>dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej</u> w związku przepisami prawa -** art. 9 ust. 2 lit. b) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
3) **dane upublicznione przez osobę, której dane dotyczą -** art. 9 ust. 2 lit. e) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
4) **ustalenie, dochodzenie lub obrona roszczeń -** art. 9 ust. 2 lit. f) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
5) **ważny interes publiczny <u>na podstawie przepisów prawa</u> -** art. 9 ust. 2 lit. g) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016),
6) **cele archiwalne w interesie publicznym, badania naukowe lub historyczne, cele statystyczne <u>na podstawie przepisów prawa</u>** - art. 9 ust. 2 lit. j) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);

7. Odbiorcy danych *(poza organami publicznymi prowadzącymi **konkretne** postępowanie na podstawie przepisów prawa), <u>jeżeli istnieją</u>: ……..*
8. Informacja dotycząca przekazania danych do państwa trzeciego, *jeżeli dotyczy*: ….
9. Okres, przez który dane będą przechowywane, a gdy nie jest możliwe jego ustalenie – kryteria ustalania okresu *np. wynikające z instrukcji archiwalnej (w latach, miesiącach, dniach):……..*

W obowiązku należy umieścić informacje o przysługujących osobie, której dane dotyczą prawach:

10. **Ma Pan/i prawo:**
    a) dostępu do treści swoich danych,
    b) sprostowania swoich danych osobowych,
    c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,

d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych – można wskazać dane teleadresowe;

W przypadku, gdy przetwarzanie odbywa się w związku z wykonywaniem zadania realizowanego w interesie publicznym lub sprawowanej władzy publicznej, należy umieścić lit. e)

e) prawo wniesienia sprzeciwu wobec przetwarzania;

W przypadku, gdy przetwarzanie odbywa się na podstawie wyrażenia zgody lub na podstawie umowy i w sposób zautomatyzowany, należy umieścić lit. f)

f) prawo do przenoszenia danych;

11. Dane zostały pozyskane od … (*podać źródło i informacje czy jest to źródło publicznie dostępne)*.

Źródłem pochodzenia danych może być:

a) rejestr publicznie dostępny np. CEIDG, KRS,
b) jednostka samorządu terytorialnego, urząd, organ, podmiot publiczny,
c) podmiot prywatny np. w przypadku danych kontaktowych pracowników;

>>

UWAGA!

1. W/W INFORMACJE PODAJEMY NIEZWŁOCZNIE PO ICH POZYSKANIU, NAJPÓŹNIEJ W CIĄGU MIESIĄCA OD ICH ZEBRANIA.
2. JEŻELI DANE MAJĄ BYĆ STOSOWANE DO KOMUNIKACJI Z OSOBĄ, KTÓREJ DOTYCZĄ TO PRZY NAJBLIŻSZEJ TAKIEJ KOMUNIKACJI.

NIE MA ZASTOSOWANIA, GDY:

1. OSOBA JUŻ W/W INFORMACJAMI DYSPONUJE.
2. PODANIE INFORMACJI JEST TO NIEMOŻLIWE LUB WYMAGA NIEWSPÓŁMIERNEGO WYSIŁKU – PO WCZEŚNIEJSZYCH KONSULTACJACH Z IOD.
3. POZYSKUJEMY DANE NA PODSTAWIE PRZEPISÓW PRAWA, KTÓRE REGULUJĄ TO POZYSKIWANIE I DANE SĄ ODPOWIEDNIO ZABEZPIECZONE.
4. DANE SĄ POUFNE ZGODNIE Z OBOWIĄZKIEM ZACHOWANIA USTAWOWEJ TAJEMNICY ZAWODOWEJ.

WYRAŻENIE ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

*Ma pan/i prawo w dowolnym momencie **wycofać wyrażoną poniżej zgodę** na przetwarzanie danych osobowych. Wycofanie zgody nie wpływa na zgodność przetwarzania danych osobowych z prawem przed jej wycofaniem.*

Ja … (*wpisać imię i nazwisko*) **niżej podpisany/a, zgadzam się** na przetwarzanie moich danych osobowych: *(wymienić dane, można wpisać w zakresie wymienionym w niniejszym wniosku)* przez ……. (*nazwa administratora oraz dane teleadresowe*) w celu…….*(wpisujemy konkretne cele zbierania danych).*

<u>Podstawa prawna:</u> *Art. 6 ust. 1 lit. a) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)*

……
Data i czytelny podpis

OPIS SYSTEMÓW INFORMATYCZNYCH

FORIS

1. Logowanie użytkowników

Login i hasło, przypomnienie o braku zmiany po 30 dniach

2. Przetwarzane dane osobowe

Imię i nazwisko, adres zamieszkania, nr telefonu, nr PESEL, dokumenty poświadczające kompetencje zawodowe, zaświadczenia dotyczące karalności z KKK

3. Aktualizacja

Wykonywana ręcznie przez administratora po pojawieniu się nowej wersji

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopia zapasowa

Kopia zapasowa bazy wykonywana automatycznie, codziennie

FK i faktury

1. Logowanie użytkowników

Login i hasło, użytkownik może zmienić hasło, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

2. Przetwarzane dane osobowe

Imię i nazwisko, adres zamieszkania,

3. Aktualizacja

Wykonywana ręcznie przez administratora po pojawieniu się nowej wersji

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopia zapasowa

Wykonywana automatycznie, codziennie

Płatnik

1. Logowanie użytkowników

Login i hasło, wymuszenie zmiany co 30 dni

2. Przetwarzane dane osobowe

Imię i nazwisko, nazwisko rodowe, adres zamieszkania, nr telefonu, nr PESEL, nr i seria dowodu osobistego, dokumenty poświadczające stan zdrowia

3. Aktualizacja

Wykonywana automatycznie, wymagane połączenie internetowe, dane pobierane z serwerów ZUS

4. Usługi firm zewnętrznych

Nie są wykonywane czynności serwisowe przez firmy zewnętrzne

5. Kopia zapasowa

Wykonywana automatycznie, codziennie

KOMADRES – Płace i Kadry

1. Logowanie użytkowników

Login i hasło, użytkownik może zmienić hasło, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

2. Przetwarzane dane osobowe

Imię i nazwisko, nazwisko rodowe, adres zamieszkania, nr telefonu, nr PESEL, nr i seria dowodu osobistego, dokumenty poświadczające stan zdrowia, nr rachunku bankowego, dane członków rodziny: imiona rodziców

3. Aktualizacja

Wykonywana przez serwis producenta

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopia zapasowa

Wykonywana automatycznie, codziennie

EWOPIS

1. Logowanie użytkowników

Login i hasło, użytkownik nie może zmienić hasła, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

2. Przetwarzane dane osobowe

Nazwisko, Imiona, Pesel, Adres zamieszkania, Nr dowodu tożsamości

3. Aktualizacja

Ręczna, wykonywana przez administratora. Aktualizacje udostępniane przez producenta

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopie zapasowe

Wykonywane automatycznie, codziennie

OŚRODEK

1. Logowanie użytkowników

Login i hasło, użytkownik nie może zmienić hasła, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

2. Przetwarzane dane osobowe

Nazwisko, imiona, adres zamieszkania, NIP

3. Aktualizacja

Ręczna, wykonywana przez administratora. Aktualizacje udostępniane przez producenta

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopie zapasowe

Wykonywane automatycznie, codziennie

WINDYKACJA (nowe)

1. Logowanie użytkowników

Login i hasło, użytkownik nie może zmienić hasła, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

2. Przetwarzane dane osobowe

Nazwisko, imiona, adres zamieszkania, NIP

3. Aktualizacja

Ręczna, wykonywana przez administratora. Aktualizacje udostępniane przez producenta

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopie zapasowe

Wykonywane automatycznie, codziennie

GEOPORTAL (tryb chroniony)

1. Logowanie użytkowników

Login i hasło, wymusza zmianę hasła

2. Przetwarzane dane osobowe

Baza ewidencji gruntów i budynków

3. Aktualizacja

Wykonuje wykonawca

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych – obecnie brak umowy

5. Kopie zapasowe

Pobiera dane z bazy ewidencji gruntów i budynków, której kopia zapasowa jest wykonywana

---

EWMAPA

1. Logowanie użytkowników

Logowanie dwuetapowe,

I etap:

Login i hasło, użytkownik nie może zmienić hasła, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

II etap

Login i hasło, użytkownik nie może zmienić hasła, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

2. Przetwarzane dane osobowe

System samodzielnie nie przetwarza danych osobowych, jednak po skonfigurowaniu połączenia z programem EWOPIS, co może zrobić samodzielnie użytkownik - umożliwia wgląd w dane ewidencji gruntów i budynków, tj. nazwisko, Imiona, Pesel, Adres zamieszkania, Nr dowodu tożsamości

3. Aktualizacja

Ręczna, wykonywana przez administratora. Aktualizacje udostępniane przez producenta

4. Usługi firm zewnętrznych

Czynności serwisowe nie wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopie zapasowe

Wykonywane automatycznie, codziennie

Użytkowanie wieczyste

1. Logowanie użytkowników

Login i hasło, użytkownik nie może zmienić hasła, brak wymuszenia zmiany, nie ma przypomnienia o braku zmiany

2. Przetwarzane dane osobowe

Nazwisko, Imiona, Pesel, Adres zamieszkania, Nr dowodu tożsamości

3. Aktualizacja

Ręczna, wykonywana przez administratora. Aktualizacje udostępniane przez producenta

4. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

5. Kopie zapasowe

Wykonywane automatycznie, codziennie

PROTON

1. Logowanie użytkowników

Login i hasło, wymuszenie zmiany co 30 dni

2. Użytkownicy

Wszyscy pracownicy Starostwa

3. Przetwarzane dane osobowe

Nazwisko, Imiona, Adres zamieszkania

4. Aktualizacja

Ręczna, wykonywana przez administratora (serwer). Aktualizacje udostępniane przez producenta. Aktualizacja stacji roboczych automatyczna.

5. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

6. Kopie zapasowe

Wykonywane automatycznie, codziennie

VULCAN - Arkusz organizacyjny

1. Logowanie użytkowników

Login i hasło, wymuszenie zmiany co 30 dni

2. Użytkownicy

Wszyscy pracownicy Starostwa Starostwo: J.Zarzeczny, B.Karlik, M.Pędlowska, K.Zdun, dyrektorzy szkół ponadpodstawowych

3. Przetwarzane dane osobowe

Nazwisko, Imiona, Adres zamieszkania, wykształcenie, dane mogące ujawniać stan zdrowia (zastępstwa, fakt przebywania na zwolnieniu lekarskim lub urlopie zdrowotnym)

4. Aktualizacja

System chmurowy, aktualizowany przez producenta.

5. Usługi firm zewnętrznych

Czynności serwisowe wymagają posiadania umowy na powierzenie przetwarzania danych osobowych

6. Kopie zapasowe

Zapewnia firma VULCAN

Nabór do szkół VULCAN

1. Logowanie użytkowników

   Login i hasło, możliwość zmiany hasła – bez wymuszania

2. Użytkownicy

   Pracownicy Wydziału Edukacji, Starosta, stanowisko ds. informatyzacji

3. Przetwarzane dane osobowe

Dane rekrutacyjne uczniów składających wnioski o przyjęcie do szkół ponadpodstawowych prowadzonych przez Powiat Stalowowolski oraz ich rodziców

4. Aktualizacja
   Dokonywana przez producenta – chmurowa

5. Usługi firm zewnętrznych
   Zawarta umowa powierzenia

6. Kopie zapasowe
   Wykonywane przez producenta

---

iVMS – 4200 Client

1. Logowanie użytkowników
   Login i hasło, brak żądania zmiany hasła
2. Użytkownicy
   Inspektor Ochrony Danych, stanowiska ds. informatyzacji
3. Przetwarzane dane osobowe
   Wizerunek, nr tablic rejestracyjnych
4. Aktualizacja
   Ręczna – ogólnodostępna na stronie producenta – system do przeglądania obrazu, rejestrator – stałe oprogramowanie
5. Usługi firm zewnętrznych
   Brak.
6. Kopie zapasowe
   Brak.

Załącznik nr 14 do

POLITYKI OCHRONY DANYCH OSOBOWYCH

PRZETWARZANYCH W STAROSTWIE POWIATOWYM W STALOWEJ WOLI

……

Miejscowość, data

……..

Imię i nazwisko lub nazwa podmiotu

……..

Adres zamieszkania lub adres siedziby

……..

Skrytka ePUAP[1]

WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH

Podstawa prawna lub uzasadniony interes prawny udostępnienia:

……
……

Cel udostępnienia:

……
……
……

Opis danych osobowych/ zbioru danych osobowych podlegających udostępnieniu:

……
……
……

Forma udostępnienia (zaznaczyć właściwe):

☐ elektronicznie

☐ papierowo

☐ na nośniku zewnętrznym (np. dysk, pendrive) –
po sprawdzeniu nośnika przez informatyka

……

Czytelny podpis

Po rozpatrzeniu wniosku:

☐ Dane można udostępnić.
☐ Dane nie podlegają udostępnieniu ze względu:

……..

……

Podpis Naczelnika/Kierownika Wydziału/Referatu

EWIDENCJA OSÓB ODBIERAJĄCYCH KLUCZ Z KANCELARII OGÓLNEJ DO POMIESZCZEŃ W STAROSTWIE POWIATOWYM W STALOWEJ WOLI – stażyści, praktykanci

Imię i nazwisko	Nr pokoju	Data	Odbiór	Oddanie

…….

Imię i nazwisko pracownika

Oświadczenie o zachowaniu poufności

Zobowiązuję się do zachowania w tajemnicy kod alarmowy, który został mi powierzony do realizacji celów służbowych.

…….

Data i czytelny podpis pracownika

…….

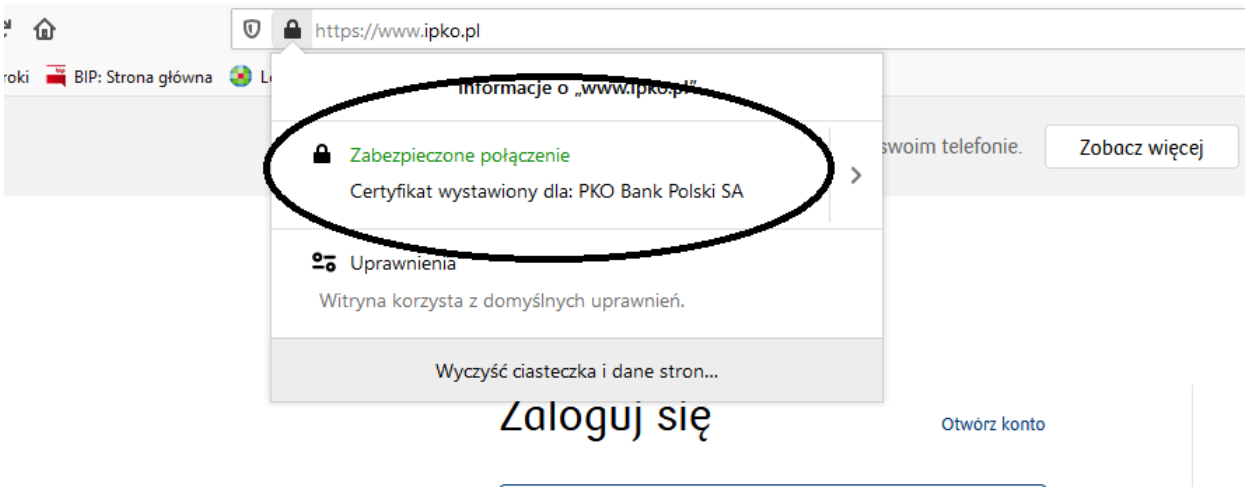
Imię i nazwisko pracownika

Oświadczenie

Oświadczam, że biorę odpowiedzialność za powierzone mi klucze do …….. (liczba egzemplarzy:……..) i będę je wykorzystywać tylko do celów służbowych.

…….

Data i czytelny podpis pracownika


https://www.ipko.pl
BIP: Strona główna
Informacje o „www.ipko.pl"
Zabezpieczone połączenie
Certyfikat wystawiony dla: PKO Bank Polski SA
Uprawnienia
Witryna korzysta z domyślnych uprawnień.
Wyczyść ciasteczka i dane stron...
swoim telefonie.
Zobacz więcej
Zaloguj się
Otwórz konto

Imię i nazwisko	
Adres zamieszkania	
Inna dana służąca do identyfikacji w celu pozyskania kopii *np. nr IP, nr telefonu, znak sprawy, adres e-mail, nazwa skrytki ePUAP, nr PESEL*	

Wniosek o udostępnienie informacji i kopii danych osobowych

Na podstawie art. 15 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. z 2016 r. Nr 119, str. 1 z późn. zm.), **wnoszę o *(proszę zaznaczyć właściwe)*:**

☐ **I. Dostarczenie kopii moich danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli:**

1. Miejsce przetwarzania danych osobowych (nazwa referatu, nazwa wydziału):

2. Krótki opis sprawy/ sytuacji, z którą związane jest przetwarzanie danych osobowych:

☐ **II. Udzielenie informacji o:**

a) celach przetwarzania danych,
b) kategoriach danych,
c) odbiorcach lub kategoriach odbiorców danych,
d) planowany okres przechowywania lub kryteria ustalania okresu przechowywania,
e) przysługujących prawach,
f) źródłach pozyskania danych osobowych,
g) zautomatyzowanym podejmowaniu decyzji,
h) przekazywaniu danych osobowych do państwa trzeciego i stosowanych zabezpieczeniach.

III. Sposób udostępnienia kopii danych osobowych (zaznaczyć właściwe):

☐ 1. Wysyłka na ePUAP (Elektroniczna Platforma Usług Administracji Publicznej) – proszę wpisać nazwę swojej skrytki:

☐ 2. Elektronicznie (np. *płyta CD*);

☐ 3. Papierowo;

Data i czytelny podpis

Oświadczenie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli

Oświadczam, że zapoznałem/am się z następującymi dokumentami:

1. Zarządzeniem Nr ……. Starosty Stalowowolski z dnia …… w sprawie przyjęcia Polityki ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli wraz z jej ewentualnymi zmianami.
2. Rozporządzeniem 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 (Dz. Urz. UE L 119 z 04.05.2016) wraz z jego ewentualnymi zmianami.
3. Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781) wraz z jej ewentualnymi zmianami.

…….. ……..

Imię i nazwisko Data i podpis

Dodatkowe podstawowe akty prawne z zakresu spraw organizacyjnych, z którymi powinno się zapoznać przetwarzając dane osobowe:

1. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14, poz. 67 z późn. zm.).
2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2019 r. poz. 700 z późn. zm.) – *w zakresie pełnienia swoich obowiązków służbowych.*
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. Nr 206, poz. 1518) – *w zakresie pełnienia swoich obowiązków służbowych.*
4. Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (t.j. Dz. U. z 2018 r. poz. 29) – *w zakresie pełnienia swoich obowiązków służbowych.*
5. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2019 r. poz. 511 z późn. zm.).
6. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.).

Powyższe akty prawne dostępne są w Biuletynie Wewnętrznym dla pracowników Starostwa Powiatowego w Stalowej Woli: http://10.161.203.30/ >> OCHRONA DANYCH OSOBOWYCH >> PRZEPISY PRAWA DOTYCZĄCE OCHRONY DANYCH

Data wydania: ……

STAROSTA STALOWOWOLSKI

ZGODA NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

WYRAŻAM ZGODĘ na przebywanie …… w pomieszczeniach, w których przetwarzane są dane osobowe, mieszczących się w ……., w związku z wykonywaniem obowiązków służbowych……. wynikających z ……..

Zgoda wydana jest na okres ……. Traci moc w wyniku ……..

…….

Podpis Administratora Danych Osobowych

Jestem świadoma/y obowiązku zachowania w tajemnicy sposobów zabezpieczania danych osobowych, także po odwołaniu zgody na przebywanie w obszarze przetwarzania danych osobowych, a także po ustaniu współpracy.

……..

Podpis osoby, której wyrażono zgodę

Przeszkolenie z zasad ochrony danych osobowych i środków bezpieczeństwa, które należy stosować w trakcie wykonywania obowiązków służbowych zostało przeprowadzone w dniu …… .

…….

Podpis Inspektora Ochrony Danych

ZGŁOSZENIE KORZYSTANIA Z PRYWATNEGO SPRZĘTU IT

w związku z Polityką ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Stalowej Woli, zgłaszam konieczność skorzystania z prywatnego sprzętu IT:

Rodzaj sprzętu/ nazwa/ marka (np. laptop, pendrive, dysk zewnętrzny)	**Zakres danych osobowych** (np. dane zwykłe dotyczące spraw…, dane pracownicze, rejestr…)	**Cel** (np. wykonywanie czynności służbowych, rozpatrzenie wniosku0

……

Podpis zgłaszającego

Wyrażam zgodę na korzystanie z własnego sprzętu IT.

……

Podpis Administratora Systemów Informatycznych

…….

(pieczęć Administratora)

ZGODA NR ____ NA WYNOSZENIE DOKUMENTÓW POZA BUDYNKI ADMINISTRATORA

Mając na uwadze potrzeby Administratora związane z organizacją prowadzonej przez niego działalności, w oparciu o przyjętą Procedurę wynoszenia dokumentów poza budynki u administratora, **niniejszym wyrażam** następującej osobie upoważnionej do przetwarzania danych osobowych:

Pani/Panu …….

(imię i nazwisko)

zgodę na wynoszenie następującego typu dokumentów:

…….

poza miejsce pracy przydzielone przez administratora, w szczególności poza pomieszczenia lub budynki administratora.

Jednocześnie zobowiązuję Panią/Pana do korzystania z wyrażonej zgody jedynie w sytuacjach wyjątkowych, a także do dysponowania odpowiednimi środkami technicznymi i organizacyjnymi gwarantującymi przetwarzanie danych osobowych zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez administratora, w odniesieniu także do prywatnego sprzętu IT.

Zgoda wygasa z chwilą ustania Pana/Pani zatrudnienia lub współpracy (bez względu na podstawę prawną zatrudnienia lub współpracy) lub odwołania zgody.

…….

(data i podpis administratora)

OŚWIADCZENIE

W związku z udzieloną mi powyższą zgodą oświadczam, że zobowiązuję się do korzystania z niej jedynie w sytuacjach wyjątkowych, a także do dysponowania odpowiednimi środkami technicznymi i organizacyjnymi gwarantującymi przetwarzanie danych osobowych zgodnie z przepisami prawa i zasadami ochrony danych osobowych wprowadzonymi przez administratora, w odniesieniu także do prywatnego sprzętu IT, w szczególności w sposób chroniący prawa osób, których dane dotyczą oraz do dysponowania środkami technicznymi i organizacyjnymi gwarantującymi przetwarzanie zgodnie z nimi danych osobowych.

…….

(data i podpis danej osoby)

Stalowa Wola, ……

Administrator Danych Osobowych

Wniosek o nadanie upoważnienia dla osoby przetwarzającej dane osobowe

1. Imię i nazwisko/ komórka organizacyjna …….
2. Cele przetwarzania danych:

☐ realizacja czynności służbowych pracownika

☐ odbycie praktyk lub stażu

☐ inne, jakie? …….

3. Zakres upoważnienia:

a) **krótki opis czynności** (m.in. *dane zwykłe, dane art. 9 ust. 1 RODO - szczególne, dane art. 10 RODO – wyroki skazujące i czyny zabronione oraz jeżeli jest to możliwe wskazanie przepisów prawa, na podstawie których wykonywane są zadania*) - uzupełnia bezpośredni przełożony

……

……

……

……

……

b) **dostęp do zasobów informatycznych** (nazwa systemu + login, e-mail) – uzupełnia informatyk:

……

……

……

……

c) **dostęp do teczek w EZD:**

……

……

…….

Podpis bezpośredniego przełożonego

…….

Podpis informatyka

Informacja o przetwarzaniu danych osobowych w związku z wezwaniem
(art. 50-56 Kodeksu postępowania administracyjnego)

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych**: tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych:** *złożenie wyjaśnień lub zeznań w związku z prowadzonym przez organ – Starostę Stalowowolskiego, postępowaniem administracyjnym na podstawie przepisów prawa - art. 50-56 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.).*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli, strony postępowania.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00
7. **Podanie danych** niezbędnych dla rozstrzygnięcia sprawy lub dla wykonywania czynności urzędowych na podstawie przepisów prawa **jest konieczne**. Na osobę uchylającą się od stawienia się na wezwanie organu może być nałożona grzywna, jak również mogą zostać zastosowane środki przymusu przewidziane przez przepisy szczególne.

Informacja o przetwarzaniu danych osobowych w związku z zawiadomieniem o przekazaniu skargi zgodnie z właściwością

(art. 231 Kodeksu postępowania administracyjnego)

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych**: tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych**: *przekazanie skargi do organu lub podmiotu właściwego do jej rozpatrzenia na podstawie przepisów prawa - art. 231 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.).*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli oraz organy lub podmioty publiczne, którym przekazano skargę do rozpatrzenia.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00

Informacja o przetwarzaniu danych osobowych w związku z inicjatywą wszczęcia postępowania

(art. 61 Kodeksu postępowania administracyjnego)

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych:** tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych**: *wszczęcie i przeprowadzenie postępowania administracyjnego przez Starostę Stalowowolskiego na podstawie przepisów prawa - Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.) oraz przepisów szczególnych.*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli, strony postępowania.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00
7. **Podanie danych** niezbędnych dla rozstrzygnięcia sprawy lub dla wykonywania czynności urzędowych na podstawie przepisów prawa **jest konieczne**. Ich niepodanie może wpłynąć na wynik postępowania administracyjnego.

Informacja o przetwarzaniu danych osobowych w związku z zawiadomieniem o przekazaniu sprawy zgodnie z właściwością

(art. 65 Kodeksu postępowania administracyjnego)

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych**: tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych**: *przekazanie sprawy do organu lub podmiotu właściwego do jej rozpatrzenia na podstawie przepisów prawa - art. 65 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.).*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli oraz organy lub podmioty publiczne, którym przekazano sprawę do rozpatrzenia.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00

Informacja o przetwarzaniu danych osobowych, gdy podanie zawiera żądania załatwienia spraw należących do właściwości różnych organów administracji publicznej *(art. 66 Kodeksu postępowania administracyjnego)*

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych**: tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych**: *realizacja przepisów prawa na podstawie Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.) oraz przepisów szczególnych.*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00
7. **Podanie danych niezbędnych** dla rozstrzygnięcia sprawy lub dla wykonywania czynności urzędowych na podstawie przepisów prawa **jest konieczne**. Ich niepodanie może wpłynąć na wynik rozstrzygnięcia sprawy.

Informacja o przetwarzaniu danych osobowych przy milczącym załatwieniu sprawy

(art. 122a Kodeksu postępowania administracyjnego)

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych:** tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych**: *realizacja przepisów prawa na podstawie Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.) oraz przepisów szczególnych.*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli, strony postępowania.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00
7. **Podanie danych** niezbędnych dla rozstrzygnięcia sprawy lub dla wykonywania czynności urzędowych na podstawie przepisów prawa **jest konieczne**. Ich niepodanie może wpłynąć na wynik postępowania administracyjnego.

Informacja o przetwarzaniu danych osobowych w związku z wydaniem zaświadczenia

(art. 217 Kodeksu postępowania administracyjnego)

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych:** tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych**: *wydanie zaświadczenia na podstawie przepisów prawa - art. 217 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.).*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00
7. **Podanie danych** niezbędnych do wydania zaświadczenia lub w razie konieczności do przeprowadzenia postępowania wyjaśniającego **jest konieczne**. Ich niepodanie może przyczynić się do odmowy wydania zaświadczenia.

Informacja o przetwarzaniu danych osobowych w związku z zawiadomieniem skarżącego o sposobie rozpatrzenia skargi *(art. 237 § 3 Kodeksu postępowania administracyjnego)*

1. **Administratorem danych osobowych** jest Starosta Stalowowolski, siedziba: Starostwo Powiatowe w Stalowej Woli, ul. Podleśna 15 37-450 Stalowa Wola, tel. 15 643 37 09, powiat@stalowowolski.pl
2. **Dane kontaktowe inspektora ochrony danych:** tel. 15 643 36 35, abi@stalowowolski.pl
3. **Cele przetwarzania danych osobowych**: *rozpatrzenie skargi i zawiadomienie skarżącego o sposobie rozpatrzenia skargi na podstawie przepisów prawa - art. 237 § 3 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096 z późn. zm.).*
4. **Odbiorcy danych***: podmioty prywatne, z którymi zawarto stosowne umowy w związku z serwisem systemów informatycznych wykorzystywanych do elektronicznego zarządzania dokumentacją w Starostwie Powiatowym w Stalowej Woli, strony postępowania.*
5. **Dane będą przechowywane** zgodnie z okresem wskazanym w Instrukcji kancelaryjnej i archiwalnej.
6. **Ma Pan/i prawo:**
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa tel. 22 531 03 00
7. Podanie danych na podstawie przepisów prawa **jest konieczne.** Organ w toku rozpatrywania skargi może zażądać dodatkowych wyjaśnień lub informacji. Niepodanie danych może wpłynąć na sposób rozpatrzenia skargi.

Stalowa Wola,

Znak sprawy:

Informacja o przekazaniu danych osobowych do państwa trzeciego
(poza terenem Unii Europejskiej, Lichtensteinu, Norwegii i Islandii)

Nazwa państwa i podmiotu, do których następuje przekazanie:

Cel i czas trwania przekazania:

jednorazowe potwierdzenie danych i informacji zawartych w prawie jazdy w związku z następującymi przepisami prawa krajowego:

Podstawa prawna:

motyw 113 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. z 2016 r. Nr 119, str. 1 z późn. zm.)

Sposób przekazania danych osobowych:

- ☐ e-mail
- ☐ list
- ☐ telefonicznie
- ☐ ustnie

Inne informacje:

Brak decyzji Komisji Europejskiej (organu wykonawczego Unii Europejskiej) uznającej, że państwo zapewnia odpowiedni stopień ochrony danych osobowych z zakresu administracji publicznej.

POŚWIADCZAM, ŻE ZAPOZNAŁAM/EM SIĘ Z POWYŻSZYMI INFORMACJAMI I SĄ ONE DLA MNIE ZROZUMIAŁE.

……

Data i czytelny podpis

Zgłoszenie naruszenia ochrony danych do ADO

1. **Imię i nazwisko zgłaszającego ……**

2. Na czym polegało naruszenie?

☐ Zgubienie lub kradzież nośnika/urządzenia

☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ Nieuprawnione uzyskanie dostępu do informacji

☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ Niezamierzona publikacja

☐ Dane osobowe wysłane do niewłaściwego odbiorcy

☐ Ujawnienie danych niewłaściwej osoby

☐ Ustne ujawnienie danych osobowych

3. Rodzaj danych osobowych

☐ Dane o pochodzeniu rasowym lub etnicznym

☐ Dane o poglądach politycznych

☐ Dane o przekonaniach religijnych lub światopoglądowych

☐ Dane o przynależności do związków zawodowych

☐ Dane dotyczące seksualności lub orientacji seksualnej

☐ Dane dotyczące zdrowia

☐ Dane genetyczne

☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

☐ Dane zwykłe (wpisać jakie np. PESEL, adres zamieszkania, imię i nazwisko):

……

……

……

……

☐ Dane art. 10 RODO (wyroki skazujące, naruszenia prawa)

4. **Szczegółowy opis naruszenia i kogo ono dotyczy** (opis osób, których dane zostały naruszone np. pracownicy, uczniowie, nauczyciele oraz opis naruszenia – miejsce, data i godzina, osoby biorące udział w naruszeniu, podjęte środki zaradcze, skutki, możliwe przyczyny)

……

……

……

Podpis

1. **Wagę naruszenia szacuję się zgodnie ze wzorem: WN = KPD*PI+ON**
   WN – waga naruszenia
   KPD – kontekst przetwarzania danych osobowych
   PI – prawdopodobieństwo identyfikacji
   ON – okoliczności naruszenia
2. **Kontekst przetwarzania danych osobowych wylicza się według schematu poniżej:**
   KPD=A+B
   A – rodzaj wrażliwości
   B – kontekst przetwarzania

A	
Dane podstawowe	1
Dane dotyczące zachowania	2
Dane finansowe	3
Dane szczególne	4
Dane art. 10	5

B		
Szeroki zakres danych	1	
Charakter danych	1	-1
Specyfika administratora	1	-1
Negatywne skutki dla podmiotu	1	
Publiczna dostępność		-1
Nieważność danych		-1

Prawdopodobieństwo identyfikacji szacuje się zgodnie z wartościami podanymi poniżej:

PI (prawdopodobieństwo identyfikacji)	
0,25	**Znikome**
0,5	**Ograniczone**
0,75	**Wysokie**
1	**Maksymalne**

3. **Okoliczności naruszenia wylicza się następująco:**

   ON=naruszenie integralności+naruszenie poufności+naruszenie dostępności+intencjonalne działanie sprawcy+skutki naruszenia dla ochrony danych

   Wartości poszczególnych składników sumy ON zostały podane w tabeli poniżej.

Naruszenie poufności		*Naruszenie integralności*		*Naruszenie dostępności*		*Intencjonalne działanie sprawcy*	*Skutki naruszenia dla osoby, której dane dotyczą*	
odbiorcy danych są znani	0,25	możliwe jest ich odzyskanie	0,25	czasowa	0,25	0,5	Przejściowe skutki bez rażących szkód materialnych i niematerialnych	0,25
nieznana liczba odbiorców	0,5	brak możliwości odzyskania	0,5	pełna i brak możliwości ich odzyskania	0,5		Duże szkody materialne lub niematerialne niedające się naprawić w krótkim czasie lub niedające się wyeliminować	0,5

4.

Naruszenie poufności		*Naruszenie integralności*		*Naruszenie dostępności*		*Intencjonalne działanie sprawcy*	*Skutki naruszenia dla osoby, której dane dotyczą*	
odbiorcy danych są znani	0,25	możliwe jest ich odzyskanie	0,25	czasowa	0,25	0,5	Przejściowe skutki bez rażących szkód materialnych i niematerialnych	0,25
nieznana liczba odbiorców	0,5	brak możliwości odzyskania	0,5	pełna i brak możliwości ich odzyskania	0,5		Duże szkody materialne lub niematerialne niedające się naprawić w krótkim czasie lub niedające się wyeliminować	0,5

5. **Skutki naruszenia ochrony danych osobowych ocenia się następująco:**

Wynik	Waga naruszenia	Opis
WN<2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2<=WN<3	Średnia	Osoby mogą napotkać niedogodności, które są możliwe do pokonania
3<=WN<4	Wysoka	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4<=WN	Bardzo wysoka	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

REJESTR KLAUZUL WYRAŻEŃ ZGODY W STAROSTWIE POWIATOWYM W STALOWEJ WOLI

Lp.	Komórka organizacyjna	Cel przetwarzania danych	Rodzaj danych	Okres przetwarzania

ANALIZA INTERESU NADRZĘDNEGO ADMINISTRATORA

1. **Rodzaj przetwarzania danych:** ……

……

2. **Realizowane zadanie publiczne i wynikające z tego tytułu uprawnienia administratora:**

……

……

……

……

……

3. **Negatywne konsekwencje przetwarzania danych, dla osoby której dane dotyczą:**

……

……

……

……

……

4. **Potrzeby społeczne oraz rezultaty realizacji zadania publicznego:**

……

……

……

5. **Decyzja dotycząca uwzględnienia sprzeciwu:**

……

……

……

Podpis Administratora Danych Osobowych

PRZYKŁADOWE OKRESY PRZECHOWYWANIA DANYCH OSOBOWYCH

Rodzaj i cel przetwarzania	Okres przechowywania	Zalecana forma przeglądu	Zalecana forma usunięcia
Teczki spraw w komórkach organizacyjnych	Zgodny z kategorią archiwalną	Zgodnie z Instrukcją kancelaryjną	Przekazanie teczki spraw do Archiwum Zakładowego, brakowanie
Teczki w Archiwum Zakładowym	Zgodny z kategorią archiwalną	Zgodnie z Instrukcją archiwalną	Brakowanie lub oddanie do Archiwum Państwowego
Szablony pism i inne pliki	Na czas trwania celu przetwarzania np. rozpatrywania sprawy	Raz na miesiąc	Usunięcie do kosza systemowego
Folder pobrane	Na czas trwania celu pobrania	Raz na miesiąc	Usunięcie do kosza systemowego
Dyski wydziałowe	Na czas trwania celu przetwarzania np. rozpatrywania sprawy	Raz na kwartał	Usunięcie do kosza systemowego
Dyski wspólne	Na czas trwania celu przetwarzania	Raz na kwartał	Usunięcie do kosza systemowego
Folder skanowane	Na czas trwania celu przetwarzania	Raz na miesiąc	Usunięcie do kosza systemowego
Poczta elektroniczna	Na czas trwania celu przetwarzania np. rozpatrywania sprawy	Raz na kwartał	Trwałe usunięcie i opróżnienie kosza
System EZD	Zgodny z kategorią archiwalną	Zgodnie z Instrukcją kancelaryjną	Przekazanie teczki spraw do Archiwum Zakładowego
Inne systemy	Zgodny z kategorią archiwalną lub na czas trwania celu przetwarzania np. rozpatrywania sprawy lub na podstawie przepisów prawa	Zgodnie z Instrukcją kancelaryjną lub raz na kwartał	Trwałe usunięcie lub archiwizacja
Kosz systemowy	Maksymalnie kwartał	Raz na miesiąc	Opróżnienie kosza
Dokumentacja ZFŚS	Zgodny z kategorią archiwalną i przepisami prawa	Raz do roku	Przekazanie teczki spraw do Archiwum Zakładowego lub trwałe usunięcie – *w zależności do rodzaju dokumentu*
Dokumentacja kadrowa i kadrowo-finansowa	Zgodny z kategorią archiwalną i przepisami prawa m.in. Rozporządzeniem Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej	Na bieżąco	Archiwizacja lub trwałe usunięcie – *w zależności do rodzaju dokumentu*
Dokumentacja księgowo-finansowa	Zgodny z kategorią archiwalną i przepisami prawa m.in. Ustawą z dnia 29 września 1994 r. o rachunkowości.	Na bieżąco	Archiwizacja lub trwałe usunięcie – *w zależności do rodzaju dokumentu*

§ ....

Ochrona danych osobowych

1. Administratorem danych osobowych jest: *wpisujemy tego, kto zawiera umowę po stronie Powiatu np. Zleceniodawca.*
2. Dane kontaktowe inspektora ochrony danych: tel. 15 643 36 35, abi@stalowowolski.pl
3. Celem przetwarzania danych osobowych jest realizacja niniejszej umowy.
4. Podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. b) Ogólnego Rozporządzenia o ochronie danych osobowych 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).
5. Odbiorcami danych osobowych są: podmioty prywatne, z którymi zawarto umowę na obsługę serwisową systemów informatycznych lub hosting, strony postępowania.
6. Dane będą przechowywane zgodnie z kryteriami wskazanymi w instrukcji kancelaryjnej.
7. Przysługują prawa:
   a) dostępu do treści swoich danych,
   b) sprostowania swoich danych osobowych,
   c) w przypadkach wymienionych w ogólnym rozporządzeniu o ochronie danych – do usunięcia danych lub ograniczenia przetwarzania danych,
   d) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych – można wskazać dane teleadresowe.
8. Podanie danych osobowych jest niezbędne do zawarcia i realizacji umowy.
9. Niepodanie danych osobowych skutkuje utrudnieniami lub brakiem możliwości zawarcia oraz realizacji umowy.
10. Zleceniobiorca zobowiązuje się do przekazania informacji zawartych w ust. 1-9 osobom, których dane osobowe w związku z realizacją umowy są przetwarzane przez Zleceniodawcę.

PYTANIA KONTROLNE POMAGAJĄCE W WYBORZE PROCESORA

1. Procesor przetwarza dane zgodnie z obowiązującymi przepisami prawa ☐

2.Procesor przeprowadził analizę ryzyka naruszenia praw i wolności osób, których dane są przetwarzane ☐

3.Procesor wdrożył wewnętrzny dokument regulujący zasady przetwarzania danych osobowych ☐

4.Procesor wdrożył procedury kontroli dostępu☐

5.Procesor przyjął zasady monitorowania realizacji zamówienia☐

6.Procesor przeprowadza kontrole lub wdraża inne środki sprawdzające podwykonawców ☐

7.Procesor przeprowadza szkolenia pracowników w zakresie bezpieczeństwa danych ☐

8.Procesor zapewnia, że pracownicy mają jasno sprecyzowane obowiązki i nadane odpowiednie upoważnienia do przetwarzania danych ☐

9.Procesor wdrożył zabezpieczenia sieci informatycznych w postaci szyfrowanych połączeń (VPN lub https)☐

10.Procesor wdrożył zabezpieczenia infrastruktury informatycznej (oprogramowanie antywirusowe)☐

11.Procesor jasno sprecyzował zasady korzystania z infrastruktury informatycznej przez pracowników☐

12.Procesor zapewnia, że ma możliwość sprawdzenia, które dane osobowe zostały wprowadzone do systemów przetwarzania danych, zmienione lub usunięte oraz kiedy i przez kogo dane zostały wprowadzone, zmienione lub usunięte☐

13.Doświadczenie na rynku (liczba lat działania):

14.Współpraca z podmiotami administracji publicznej: