Załącznik Nr 2
zarządzenia Nr **ZD – PO.120.19.2021.AK** dyrektora
Zarządu Drogowego w Sępólnie Krajeńskim
z dnia **30 grudnia 2021** r.
w sprawie wprowadzenia w życie dokumentacji
związanej z przetwarzaniem i ochroną danych osobowych
w Zarządzie Drogowym w Sępólnie Krajeńskim.

Procedura zarządzania systemami informatycznymi w Zarządzie Drogowym w Sępólnie Krajeńskim

Sępólno Krajeńskie, grudzień 2021.

Spis treści:

Rozdział 1

Postanowienia ogólne 4

Rozdział 2

Dostęp do pomieszczeń, w których przetwarzane są dane za pośrednictwem systemów informatycznych 5

Rozdział 3

Inwentaryzacja elementów systemów informatycznych, nośników oraz aplikacji służących do przetwarzania danych osobowych 6

Rozdział 4

Uprawnienia do przetwarzania danych osobowych 6

Rozdział 5

Uwierzytelnianie 7

Rozdział 6

Rozpoczęcie, zawieszenie i zakończenie pracy 8

Rozdział 7

Procedura tworzenia kopii zapasowych 9

Rozdział 8

Przegląd i konserwacja systemów i nośników informacji 10

Rozdział 9

Zabezpieczenie systemu informatycznego przed niewłaściwym oprogramowaniem 11

Rozdział 10

Środki bezpieczeństwa w urządzeniach przekazanych poza obszar przetwarzania 11

Rozdział 11

Postanowienia końcowe 12

Wykaz załączników:

Załącznik nr 1 – Uprawnienie do zarządzania elementami infrastruktury informatycznej;

Załącznik nr 2 – Lokalizacja elementów wchodzących w skład infrastruktury informatycznej;

Załącznik nr 3 – Oświadczenie o tworzeniu kopi zapasowej;

Załącznik nr 4 - Protokół zniszczenia danych osobowych w systemach informatycznych;

Załącznik nr 5 – Zgoda na korzystanie z prywatnych urządzeń informatycznych do celów służbowych;

Załącznik nr 6 – Umowa powierzenie urządzenia informatycznego;

Załącznik nr 7 – Oświadczenie o zapoznaniu się z treścią Procedury zarządzania systemami informatycznymi;

Załącznik nr 8 – Ewidencja osób zaznajomionych z Procedurą zarządzania systemami informatycznymi.

Rozdział 1
Postanowienia ogólne

§ 1.1. Niniejsza Procedurą znajduje zastosowanie w związku z przetwarzaniem danych osobowych w Zarządzie Drogowym, za pośrednictwem systemów teleinformatycznych.

2. Każda osoba przetwarzająca dane osobowe przy pomocy systemów informatycznych obowiązana jest do zapoznania się z treścią niniejszej Procedury oraz do bezwzględnego stosowania postanowień w niej zawartych, przy przetwarzaniu danych osobowych.

§ 2.1. Ilekroć w niniejszej Procedurze mowa jest o:

1) **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć Zarząd Drogowy w Sępólnie Krajeńskim reprezentowany przez dyrektora ZD;
2) **Inspektorze Danych Osobowych (IOD)** – należy przez to rozumieć osobę powołaną przez ADO zgodnie z „Polityką bezpieczeństwa i ochrony danych osobowych w Zarządzie Drogowym w Sępólnie Krajeńskim";
3) **Jednostce lub ZD** – należy przez to rozumieć Zarząd Drogowy w Sępólnie Krajeńskim;
4) **Danych osobowych** – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
5) **Przetwarzaniu danych osobowych** – należy przez to rozumieć między innymi operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
6) **Sieci komputerowej** - zbiór komputerów i innych urządzeń połączonych z sobą kanałami komunikacyjnymi oraz oprogramowanie wykorzystywane w tej sieci. Umożliwia ona wzajemne przekazywanie informacji oraz udostępnianie zasobów własnych między podłączonymi do niej urządzeniami.
7) **Sieci przewodowej** – należy przez to rozumieć sieć internetową;
8) **Systemach informatycznych** – należy przez to rozumieć zespół systemów komputerowych, sieci i oprogramowania służących do przetwarzania danych osobowych;
9) **Infrastrukturze informatycznej** – należy przez to rozumieć całokształt rozwiązań sprzętowo-programowych i organizacyjnych stanowiących podstawę wdrożenia i eksploatacji systemów informatycznych wspomagających zarządzanie ZD;
10) **Administratorze Systemu Informatycznego (ASI)** – należy przez to rozumieć osobę wyznaczona przez ADO oraz posiadającą uprawnienia do zarządzania zasobami sieci i systemów informatycznych;
11) **RODO** – należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku

z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

12) **Ustawie** – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2019 r., poz. 1781);

13) **Procedurze** – należy przez to rozumieć niniejszą Procedurę Zarządzania Systemami Informatycznymi w ZD;

14) **Polityce** – należy przez to rozumieć Politykę bezpieczeństwa i ochrony danych osobowych w Zarządzie Drogowym w Sępólnie Krajeńskim;

15) **Podmiocie przetwarzającym** – należy przez to rozumieć osobę lub instytucje, która przetwarza dane osobowe w imieniu Administratora Danych Osobowych, na podstawie upoważnienia;

16) **Zbiorze danych osobowych** – należy przez to rozumieć uporządkowany zestaw danych osobowych uszeregowanych według określonych kryteriów, niezależnie czy dany zestaw ma charakter scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

§ 3. ADO wyznacza osobę odpowiedzialną za zarządzanie systemami informatycznymi, nadając jej uprawnienia do zarządzania elementami infrastruktury informatycznej **(zał. Nr 1)**, zwaną dalej Administratorem Systemu Informatycznego (ASI).

Rozdział 2
Dostęp do pomieszczeń, w których przetwarzane są dane za pośrednictwem systemów informatycznych

§ 4.1. Pomieszczenia, w których przetwarzane są dane osobowe za pośrednictwem systemów informatycznych, muszą być zabezpieczone przed dostępem osób nieupoważnionych podczas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych zgodnie z Polityką bezpieczeństwa i ochrony danych osobowych oraz Procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w ZD.

2. Wyłączny dostęp do pomieszczeń, w których umieszczone są dyski z danymi, posiadają osoby upoważnione przez Administratora Danych Osobowych.

3. W **załączniku Nr 2** niniejszej Procedury określono lokalizacje elementów wchodzących w skład infrastruktury informatycznej.

Rozdział 3

Inwentaryzacja elementów systemów informatycznych, nośników oraz aplikacji służących do przetwarzania danych osobowych

§ 5.1. Administrator Systemu Informatycznego dokonuje inwentaryzacji elementów struktury informatycznych oraz oprogramowania służącego do przetwarzania danych osobowych nie rzadziej niż raz w roku.

2. Inwentaryzacja obejmuje w szczególności analizę:

a) sprawności i wykorzystywania w dalszym ciągu systemów informatycznych do przetwarzania danych;
b) spisu elementów wchodzących w skład infrastruktury informatycznej;
c) legalności oprogramowania służącego do przetwarzania danych osobowych oraz czy jest ono dalej wykorzystywane;

3. ASI przeprowadza aktualizacje elementów wchodzących w skład infrastruktury sieciowej;

Rozdział 4

Uprawnienia do przetwarzania danych osobowych

§ 6.1. Administrator Systemu Informatycznego zapewnia dostęp i zapobiega nieuprawnionemu dostępowi do systemów informatycznych w jednostce.

2. ASI uprawniony jest do zablokowania konta użytkownika w dowolnym momencie.

§ 7.1. Przydzielenie praw dostępu do systemu informatycznego odbywa się za zgodą Administratora Danych Osobowych.

2. Użytkownicy przetwarzający dane osobowe w systemach informatycznych posiadają uprawnienia, spójne z upoważnieniem nadanym przez ADO.

3. Każdy użytkownik zobowiązany jest do zapoznania się z obowiązującymi w Zarządzie Drogowym przepisami dotyczącymi ochrony danych osobowych.

4. Każdy pracownik upoważniony do przetwarzania danych za pomocą systemów informatycznych posiada identyfikator i hasło, które można przypisać tylko jemu.

5. Zabrania się dostępu do systemu informatycznego za pośrednictwem innego identyfikatora niż ten przydzielony przez Administratora Systemu Informatycznego.

§ 8. W sytuacji zmiany zakresu obowiązków pracownika Administrator Systemu Informatycznego zmienia zakres praw dostępu zgodnie z zaleceniami.

§ 9.1. Odebranie uprawnień

1) Wyrejestrowanie użytkownika z systemu informatycznego, może mieć charakter czasowy albo trwały, dokonuje go Administrator Systemu Informatycznego.
2) Wyrejestrowanie następuje przez:

   a) zablokowanie konta użytkownika;
   b) usunięcie danych użytkownika z bazy użytkowników systemu.

§ 10.1. Okresowy przegląd uprawnień

1) Osoba uprawniona dokonuje przeglądu praw użytkowników do systemów, w celu utrzymania efektywnej kontroli nad dostępem do danych i systemów informatycznych.
2) Przegląd ten obejmuje:

   a) sprawdzenie, czy każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada odrębny identyfikator do systemu, z którego korzysta;
   b) sprawdzenie, czy nie istnieją w systemie aktywne konta użytkowników, którzy nie przetwarzają danych osobowych w systemach informatycznych.

3) Przegląd uprawnień do systemów wykonywany jest w przypadku zmian kadrowych w dowolnym czasie.

§ 11. W sytuacji awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych, każdy użytkownik zobowiązany jest do niezwłocznego powiadomienia Administratora Danych Osobowych lub Inspektora Ochrony Danych.

Rozdział 5

Uwierzytelnianie

§ 12.1. System informatyczny służący do przetwarzania danych osobowych musi posiadać system uwierzytelniający użytkownika (identyfikator i hasło).

2. Użytkownik systemu w momencie pierwszego logowania do systemu zmienia hasło na indywidualnie przez siebie stworzone.

3. Hasło jest informacją o charakterze poufnym i należy zachować je w tajemnicy.

4. Obowiązuje ścisły zakaz ujawniania haseł osobom trzecim, w tym innym użytkownikom.

5. Zakazane jest zapisywanie haseł oraz pozostawianie zapisu w miejscu łatwo dostępnym.

6. Jeżeli system informatyczny nie wymusza okresowej zmiany hasła, użytkownik zobowiązany jest je zmienić, co 60 dni kalendarzowych.

7. O każdorazowej zmianie hasła w systemie informatycznym oraz o jego treści, należy poinformować Administratora Systemów Informatycznych.

8. Dla systemów, które nie wymuszają zmiany hasła, osoba uprawniona informuje użytkownika o konieczności zmiany hasła w określonym terminie.

Rozdział 6

Rozpoczęcie, zawieszenie i zakończenie pracy

§ 13.1. Przed rozpoczęciem, jak i w trakcie pracy w systemie informatycznym użytkownik systemu zobowiązany jest sprawdzić stanowisko pod kątem możliwych naruszeń ochrony danych osobowych.

2. Katalog naruszeń ochrony danych osobowych znajduje się w Polityce bezpieczeństwa i ochrony przetwarzania danych osobowych.

§ 14.1. Zabrania się użytkownikom:

a) samodzielnego instalowania nowego oprogramowania;
b) dokonywania zmian parametrów konfiguracyjnych komputerów a w szczególności tych dotyczących sieci komputerowych;
c) modyfikowania ustawień aplikacji programowych oraz systemów operacyjnych;
d) pozostawienia zalogowanego użytkownika tak, aby inny pracownik korzystał z systemu informatycznego bez wprowadzenia własnego identyfikatora i hasła do systemu informatycznego.

2. Systemy informatyczne należy skonfigurować tak, by w sytuacji ich bezczynności przechodziły w stan uśpienia za pośrednictwem wygaszacza ekranu zabezpieczonego hasłem. Kontynuowanie pracy równoznaczne jest z ponownym zalogowaniem się.

3. W sytuacji opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu informatycznego.

§ 15. Kończąc pracę w systemie informatycznym użytkownik, obowiązany jest do wylogowania się z systemu informatycznego oraz do zabezpieczenia nośników danych w postaci elektronicznej w niedostępnym dla osób nieupoważnionych miejscu.

Rozdział 7
Procedura tworzenia kopii zapasowych

§ 16.1. Kopie zapasowe wykonywane są raz w miesiącu.

2. Czynności związane z tworzeniem kopii zapasowych przetwarzanych danych w systemach informatycznych, wykonywane są przez każdego pracownika przetwarzającego dane.

3. Wszyscy pracownicy przetwarzający dane osobowe zobowiązują się do tworzenia kopi zapasowych dokumentacji zawierającej dane osobowe (**załącznik Nr 3**).

4. Kopie zapasowe zapisywać należy na przyporządkowanych do pracowników przetwarzających dane nośnikach zewnętrznych, zgodnie z zawartymi umowami powierzenia urządzeń informatycznych.

5. Wszelkie czynności związane z testowaniem kopii zapasowych oraz likwidacją nośników są prowadzone przez ASI.

6. Kopie zapasowe są przechowywane w miejscu niedostępnym dla osób nieupoważnionych zamykanym na klucz w pokoju nr 9.

7. Klucz, o którym mowa w § 16 ust. 6 przechowuje Administrator Systemów Informatycznych.

8. Dostęp do kopii danych ma ADO oraz ASI.

9. Sprawdzeń z wykonywania kopii zapasowych w systemach informatycznych dokonuje Inspektor Ochrony Danych. W przypadku stwierdzenia nie zachowania obowiązku tworzenia kopii zapasowych przez pracownika przetwarzającego dane osobowe, może on zostać pociągnięty do odpowiedzialności służbowej.

Rozdział 8

Przegląd i konserwacja systemów i nośników informacji

§ **17.**1. Przegląd i konserwacja obejmuje:

a) systemy informatyczne, oprócz tych wyłącznie serwisowanych przez producenta;

b) oprogramowanie systemowe;

c) komputery;

d) inny sprzęt elektroniczny.

2. Częstotliwość prac związanych z naprawą i konserwacją elementów wchodzących w skład infrastruktury informatycznej, zależna jest od specyfiki danego elementu, zainstalowanego na nim systemu operacyjnego, oprogramowania, ilości użytkowników z niego korzystających oraz częstotliwości jego wykorzystywania.

3. W sytuacji przekazania całego urządzenia do naprawy należy zadbać o to aby przed przekazaniem urządzenia zostało ono pozbawione nośników zawierających dane lub jeśli jest to możliwe, usunąć te dane z nośnika w sposób uniemożliwiający ich odzyskanie.

4. Nośniki, które uległy uszkodzeniu, zawierające dane osobowe przekazywane są do naprawy firmie, z którą nawiązana jest umowa o współpracy oraz umowa powierzenia.

§ **18.**1. Usuwanie danych osobowych polega na:

a) trwałym, fizycznym ich zniszczeniu w stopniu niepozwalającym na ich odtworzenie przez osoby nieupoważnione przy zastosowaniu powszechnie dostępnych metod;

b) anonimizacji zbiorów danych osobowych polegających na pozbawieniu danych osobowych cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.

2. Procedura niszczenia danych osobowych:

a) niszczenie następuje wyłącznie na wniosek Administratora Danych Osobowych;

b) niszczenie musi odbywać się komisyjnie, jednym z członków komisji musi być Administrator Danych Osobowych;

c) zniszczenie danych osobowych musi zostać potwierdzone protokołem **(zał. Nr 4).**

3. Sposób usunięcia danych osobowych uzależniony jest od rodzaju nośnika, na którym są przechowywane.

Rozdział 9

Zabezpieczenie systemu informatycznego przed niewłaściwym oprogramowaniem

§ 19.1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, należy wdrożyć odpowiednie środki ochrony dla danych przetwarzanych w systemach informatycznych.

2. ASI nie rzadziej niż raz w roku dokonuje sprawdzenia systemów informatycznych pod kątem zgodności z wdrożonymi środkami bezpieczeństwa.

§ 20.1. Dostęp do sieci przewodowej w jednostce zabezpieczony jest za pośrednictwem odpowiedniego urządzenia (firewall – zapora sieciowa).

2. Na każdym stanowisku komputerowym zainstalowane zostało licencjonowane oprogramowanie antywirusowe wraz z firewallem programowym.

3. W sytuacji zainfekowania sprzętu i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, użytkownik zobowiązany jest do powiadomienia osoby uprawnionej, która podejmie działania zmierzające do usunięcia zagrożenia.

4. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na komputerach w jednostce.

5. W momencie wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.

Rozdział 10

Środki bezpieczeństwa w urządzeniach przekazanych poza obszar przetwarzania

§ 21.1. Przetwarzać dane osobowe w systemie informatycznym poza obszarem jednostki może wyłącznie użytkownik, któremu:

a) powierzone zostały urządzenia informatyczne w celu przetwarzania danych osobowych **(zał. Nr 6)**;
b) udzielona została pisemna zgoda na korzystanie z prywatnych urządzeń informatycznych do celów służbowych **(zał. Nr 5)**.

2. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar jednostki zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

3. Wysyłanie danych osobowych może następować wyłącznie za pośrednictwem sprawdzonych aplikacji i tylko przez osoby upoważnione do przetwarzania danych osobowych zgodnie z Polityką obowiązującą w ZD.

Rozdział 11
Postanowienia końcowe

§ 22.1. Każda osoba przetwarzająca dane osobowe w systemie informatycznym zobowiązana jest do zapoznania się z treścią niniejszej Procedury i dokumentacji z nią spójnej oraz do bezwzględnego stosowania postanowień w niej zawartych przy przetwarzaniu danych osobowych.

2. Wzór oświadczenia o zapoznaniu się z niniejszą Procedurą stanowi **załącznik Nr 7**. Oświadczenia należy przechowywać w aktach osobowych pracowników.

3. Ewidencje osób zaznajomionych z Procedurą zarządzania systemami informatycznymi (**załącznik Nr 8**) prowadzi Inspektor Ochrony Danych.

Załącznik Nr 1
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

.....
(pieczęć jednostki)

Uprawnienie do zarządzania elementami infrastruktury informatycznej w Zarządzie Drogowym

Działając, na podstawie art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Administrator Danych Osobowych w celu spełnienia obowiązku zapewnienia odpowiednich środków organizacyjnych i technicznych uprawnia:

.....
(imię i nazwisko)

do pełnienia funkcji Administratora Systemu Informatycznego w Zarządzie Drogowym oraz zarządzania w imieniu Administratora Danych Osobowych elementami infrastruktury informatycznej w szczególności do:

1. zabezpieczenia przed działaniem szkodliwego oprogramowania oraz zagrożeniami z sieci publicznej;
2. nadzoru nad przeglądami, konserwacją, naprawą oraz niszczeniem elementów struktury informatycznej;
3. współpracy przy ustalaniu środków organizacyjnych i technicznych, mających zapewnić ochronę przetwarzania danych osobowych;
4. zapewnienia sprawnego działania systemów informatycznych służących do przetwarzania danych osobowych;
5. zabezpieczenia systemów przed zakłóceniami w sieci zasilającej.

.....
(data i podpis Administratora Danych Osobowych)

.....
(data i podpis Administratora Systemu Informatycznego)

Załącznik Nr 2
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

Lokalizacja elementów wchodzących w skład infrastruktury informatycznej

1. Elementy infrastruktury sieciowej (modemy, routery, itp.).

Lp.	Nazwa i model urządzenia	Lokalizacja
1.		
2.		
3.		
4.		
5.		

2. Elementy służące do przetwarzania danych osobowych (serwery, stacje robocze, dyski sieciowe, itp.).

Lp.	Nazwa/ model/ nr inwentaryzacyjny	Lokalizacja i zabezpieczenia	Oprogramowanie	Osoba odpowiedzialna
1.				
2.				
3.				
4.				

3. Powierzone urządzenia (laptopy, nośniki pamięci, smart fony, itp.).

Lp.	Typ urządzenia	Nazwa/ model	Osoba, której powierzono sprzęt	Okres powierzenia
1.				
2.				
3.				
4.				

Załącznik Nr 3
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

.....
(pieczęć jednostki)

.....
(imię i nazwisko pracownika)

Oświadczenie o tworzeniu kopi zapasowej

Oświadczam, że zapoznałem(łam) się z Procedurą zarządzania systemami informatycznymi w Zarządzie Drogowym w Sępólnie Krajeńskim (zwaną dalej **Procedurą)**, w szczególności z § 16, odnoszącym się do tworzenia kopi zapasowych dokumentacji zawierającej dane osobowe.

Zobowiązuje się wykonywać kopie zapasowe na nośniku zewnętrznym, nie rzadziej niż **raz w miesiącu** (§ 16 ust. 1 Procedury), w sposób:

- terminowy;
- rzetelny;
- całkowity.

Oświadczam ponadto, że zostałem poinformowany o przeprowadzaniu cyklicznych sprawdzeń z realizacji niniejszego oświadczenia oraz o możliwości pociągnięcia do odpowiedzialności służbowej w sytuacji nie dotrzymania warunków tego oświadczenia.

.....

Podpis pracownika

Załącznik Nr 4
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

.....
(pieczęć jednostki)

Protokół zniszczenia danych osobowych w systemach informatycznych nr: .....

Data zniszczenia: .....
Nazwa zbioru danych osobowych, z którego pochodzą dane:
.....
.....
Powód zniszczenia danych osobowych:
.....
.....
Rodzaj nośnika z kopią zapasową:
.....
Sposób zniszczenia:
.....
.....

Skład komisji:

- .....
- .....
- .....

Podpisy członków Komisji:

.....
.....
.....

Załącznik Nr 5
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

.....
(pieczęć jednostki)

Zgoda na korzystanie z prywatnych urządzeń informatycznych do celów służbowych

Zgoda na korzystanie z prywatnych urządzeń informatycznych do celów służbowych obowiązuje na czas nieokreślony / określony od dnia ..... do dnia .....*
wydawana jest przez .....
.....
(Administrator Danych Osobowych)
zwanego dalej **Administratorem**.

§ 1. Administrator upoważnia:

Pana / Panią .....,

zwanego/zwaną dalej **Użytkownikiem** do korzystania z prywatnych urządzeń informatycznych do celów służbowych.

§ 2.1. Użytkownik oświadcza, że jest właścicielem sprawnych urządzeń informatycznych.

2. Użytkownik wyraża gotowość do korzystania z prywatnych urządzeń informatycznych w trakcie trwania umowy o pracę / wykonywania zlecenia.

§ 3. Zgoda na korzystanie z prywatnych urządzeń informatycznych do celów służbowych zobowiązuje Użytkownika do stosowania się do zapisów Polityki bezpieczeństwa i ochrony danych osobowych oraz Procedury zarządzania systemami informatycznymi obowiązującymi w Zarządzie Drogowym w Sępólnie Krajeńskim.

§ 4. Użytkownik oświadcza, iż wykorzystywane przez niego prywatne urządzenia informatyczne spełniają wymogi dla elementów infrastruktury informatycznej określone w Procedurze zarządzania systemami informatycznymi.

§ 5. W przypadku, gdy Użytkownik posiada upoważnienie do przetwarzania danych osobowych poza terenem Zarządu Drogowego w Sępólnie Krajeńskim nadane przez Admini-

stratora, możliwe jest korzystanie z prywatnych urządzeń informatycznych do celów służbowych poza terenem Zarządu Drogowego.

.....	.....
(podpis Administratora Danych Osobowych)	(podpis Użytkownika)

Załącznik Nr 6
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

.....
(pieczęć jednostki)

Umowa powierzenia urządzenia informatycznego

Zawarta w dniu: ..... pomiędzy:

Zarządem Drogowym w Sępólnie Krajeńskim
ul. Koronowska 5
89-400 Sępólno Krajeńskie

reprezentowanym przez dyrektora Zarządu Drogowego, zwanym dalej **Administratorem Danych Osobowych**

a

.....,

zwanym dalej **Użytkownikiem.**

§ 1. Użytkownik oświadcza, że z dniem ..... przyjmuje odpowiedzialność materialną za urządzenie elektroniczne Administratora Danych Osobowych określone w § 2 powierzone mu z obowiązkiem zwrotu.

§ 2. Powierzone urządzenie informatyczne:
Typ urządzenia: .....
Nazwa / model: .....
Numer seryjny: .....

§ 3. W związku z przyjęciem odpowiedzialności materialnej określonej w § 1 umowy, Użytkownik zobowiązany jest do:

a) sprawowania pieczy nad powierzonymi mu urządzeniami;
b) przestrzeganiu zapisów Polityki bezpieczeństwa i ochrony danych osobowych oraz Procedury zarządzania systemami informatycznymi obwiązującymi w Zarządzie Drogowym w Sępólnie Krajeńskim;
c) niezwłocznego informowania Administratora Danych Osobowych lub Administratora Systemu Informatycznego zgodnie z Procedurą zarządzania systemami informa-

tycznymi o stwierdzonych zagrożeniach dla prawidłowego zabezpieczenia powierzonego mu urządzenia bądź o brakach w tym zakresie;

d) rozliczenia się z powierzonego mienia;
e) wyrównania wszelkich szkód powstałych w urządzeniu, wynikających z zawinionego zachowania pracownika.

.....	.....
podpis Administratora Danych Osobowych	podpis Użytkownika

Załącznik Nr 7
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

.....
(pieczęć jednostki)

.....
(imię i nazwisko pracownika)

Oświadczenie

Oświadczam, że zapoznałem się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz z ustawą z dnia 10 maja 2018 o ochronie danych osobowych;

Oświadczam ponadto, że zapoznałem(-łam) się z „Procedurą zarządzania systemami informatycznymi w Zarządzie Drogowym w Sępólnie Krajeńskim" wprowadzoną zarządzeniem Nr ..... dyrektora Zarządu Drogowego z dnia ..... w sprawie .....

Zobowiązuje się do:

1. stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne przetwarzanie danych;
2. należytego zabezpieczania danych osobowych przed ich udostępnianiem osobom nieupoważnionym;
3. zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą;
4. zachowania w tajemnicy danych oraz ich sposobu zabezpieczenia, również po ustaniu stosunku pracy.

.....
(data i podpis)

Załącznik Nr 8
do Procedury zarządzania
systemami informatycznymi
w Zarządzie Drogowym
w Sępólnie Krajeńskim

.....
(pieczęć jednostki)

Ewidencja osób zapoznanych z Procedurą zarządzania systemami informatycznymi w Zarządzie Drogowym.

Oświadczam, że zapoznałem się z Procedurą zarządzania systemami informatycznymi w Zarządzie Drogowym w Sępólnie Krajeńskim.

Przyjąłem/łam do wiadomości i zobowiązuję się do stosowania zapisów Procedury zarządzania systemami informatycznymi.

Lp.	Imię i nazwisko	Data i podpis
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
...		