Dariusz Wasiak
Tomasz Soczyński
Krzysztof Wygoda

Ochrona danych osobowych w strażach gminnych (miejskich)

Praktyczny poradnik
Polityka ochrony danych

Społeczna Akademia Nauk
Łódź

Dariusz Wasiak
Tomasz Soczyński
Krzysztof Wygoda

Ochrona danych osobowych w strażach gminnych (miejskich)

Praktyczny poradnik
Polityka ochrony danych

Społeczna Akademia Nauk
Łódź

Recenzenci: Prof. dr hab. Adam Sulikowski, Dr hab. Joanna Juchniewicz

Korekta językowa: Beata Siczek
Skład i łamanie: Małgorzata Pająk
Projekt okładki: Marcin Szadkowski

ISBN: 978-83-64971-95-2

Publikacja sfinansowana ze środków Wyższej Szkoły Bankowej we Wrocławiu.

WYDAWNICTWO
SPOŁECZNEJ AKADEMII NAUK

Wydawnictwo Społecznej Akademii Nauk
Kilińskiego 109
90-011 Łódź
tel. (42) 664 22 39
(42) 676 25 29 w. 339

Spis treści

I. Wstęp

Zasadniczym celem autorów niniejszej publikacji była próba stworzenia kompendium wiedzy w formie poradnika, które w możliwie szeroki i zarazem praktyczny sposób przedstawi wymagania, w szczególności te stawiane komendantom straży gminnych (miejskich) ulokowanych w strukturach urzędów, określone w rozdz. 5 (a zwłaszcza w art. 31–45 tego rozdziału) ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125).

Nie oznacza to jednak, że poradnik ten, pomimo nacisku położonego na jego wymiar praktyczny, jest jedynym źródłem wiedzy o zmiennych, które muszą zostać ujęte i właściwie opisane w polityce ochrony danych osobowych, którą każdy komendant straży gminnej (miejskiej) obowiązany jest na mocy przywołanego przepisu opracować, wdrożyć i aktualizować.

Autorzy mają jednak nadzieję, że jest to opracowanie na tyle merytoryczne i szczegółowe, a zarazem przystępne, iż przedstawioną w nim propozycję można potraktować jako pewnego rodzaju wzorzec w zakresie niezbędnych informacji i dokumentacji, które winny zostać uwzględnione przez komendantów straży w tworzonych przez nich, na podstawie przywołanej ustawy, politykach ochrony danych osobowych.

Poradnik ten ze względu na praktyczne ujęcie i zakres tematyczny niewątpliwie może być użyteczny nie tylko dla administratorów danych w strażach gminnych (miejskich), ale również dla każdej osoby, której chęć gruntownego poznania opisywanej problematyki jest następstwem konieczności opracowania dokumentacji ochrony danych osobowych lub po prostu wynika z potrzeby zgłębienia, bądź poszerzenia wiedzy na temat działań i ochrony danych osobowych przetwarzanych przez strażników w ramach zadań realizowanych przez straże gminne (miejskie) ulokowane przede wszystkim w strukturze urzędu gminy.

W ocenie autorów, niniejsza publikacja może (a nawet powinna) stanowić również podwaliny dla dalszych opracowań na potrzeby straży gminnych (miejskich) zrzeszonych w Krajowej Radzie Komendantów Straży

Miejskich i Gminnych. Ich celem powinno być – z założenia – przedłożenie odpowiednio zaprojektowanych rozwiązań, które obejmowałby pozostałe płaszczyzny i obszary przetwarzania danych osobowych przez komendantów straży gminnych (miejskich). Optymalnym rozwiązaniem byłoby oczywiście stworzenie i zatwierdzenie (oczywiście w odniesieniu do działań podejmowanych na gruncie dyrektywy Paramentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89), czyli DODO, kodeks taki miałby charakter nieformalny, a jego „akceptacja" wynikałaby z prowadzonych konsultacji) przez Prezesa UODO, branżowego kodeksu postępowania w rozumieniu przepisu art. 40 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 osobowych) (Dz.U.UE.L.2016.119.1).

Należy zaznaczyć, że odwoływanie się w politykach ochrony danych osobowych do pozaprawnych regulacji, takich jak normy techniczne (np. ISO), jest równie ważnym elementem budowania kompleksowego systemu bezpieczeństwa informacji, a nie „tylko" systemu w zakresie zapewnienia ochrony danych osobowych w strażach gminnych (miejskich), który ukształtować można przy wykorzystaniu m.in. następujących opracowań:

- PN-ISO/IEC 29151 – Kodeks postępowania przy ochronie danych identyfikujących osobę
- PN-ISO/IEC 27018 – Praktyczne zasady ochrony PII w chmurach publicznych działających jako przetwarzających PII
- PN-EN ISO/IEC 27002 – Praktyczne zasady zabezpieczenia informacji
- PN-ISO/IEC 29100 – Ramy prywatności
- PN-ISO/IEC 15408-3 – Kryteria oceny zabezpieczeń informacyjnych
- PN-ISO/IEC 18045 – Metodyka oceny zabezpieczeń informatycznych
- PN ISO/IEC 29134 – Ocena skutków dla prywatności

- PN-ISO 31000 – Zarządzanie ryzykiem Zasady i wytyczne
- PN-EN ISO/IEC 27001 – Systemy zarządzania bezpieczeństwem informacji[1]

Wskazanie modelowych rozwiązań w obszarze wdrożenia ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125) nie może być traktowane jako zwieńczenie działań mających na celu wsparcie straży gminnych (miejskich) w zakresie realizacji zasad ochrony danych osobowych. Jak każde rozwiązanie modelowe wymaga bowiem adaptacji do warunków lokalnych i uwzględnienia funkcjonujących w określonych urzędach przyjętych i obowiązujących polityk ochrony danych – optymalnym rozwiązaniem jest doprowadzenie do stanu jak największej spójności wszystkich stosowanych w celu ochrony rozwiązań prawno-organizacyjnych. Potrzeba ta wynika ze skomplikowanej struktury przedmiotowej regulacji prawnych dotyczących ochrony danych osobowych, które – w myśl zasady legalizmu – muszą być zastosowane w obszarze funkcjonowania tego typu podmiotów. Oczywistym jest bowiem, że straże funkcjonujące w strukturze urzędu gminy nie powinny stosować innych rozwiązań (w odniesieniu do obszarów regulowanych w RODO) wprowadzonych przez administratora niż sam urząd. Już sam ten fakt implikuje równoległe stosowanie co najmniej dwóch polityk ochrony danych: pierwszej – ogólnej, właściwej dla całego urzędu[2] oraz drugiej – szczegółowej, która jest przedmiotem niniejszego opracowania.

Linia podziału stosowania procedur i zasad wynikających z przyjętych polityk w zasadzie nie będzie jednak przebiegać (w ramach struktury straży) w sposób uwzględniający kryteria personalne (niektórzy pracownicy/funkcjonariusze działają tylko w ramach RODO, a inni wyłącznie w oparciu o ustawę o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125) – choć nie jest to wykluczone w przypadku pracowników niewykonujących jakichkolwiek czynności zarezerwowanych dla

[1] Przywołane normy można zakupić za pośrednictwem Polskiego Komitetu Normalizacyjnego (www.pkn.pl).

[2] Oczywistym jest stosowanie rozwiązań opartych o RODO nie tylko w odniesieniu do kwestii związanych z zatrudnieniem, ale również do wymiany informacji pomiędzy komórkami organizacyjnymi urzędu czy pomiędzy strażą a innym organem.

strażników), ale opierać się będzie na konieczności wyraźnego rozgraniczenia zadań poddanych rygorom różnych regulacji wewnętrznych.

Konieczność wskazania rygorów realizacji konkretnych czynności podejmowanych w ramach działalności straży jest istotna również w kontekście wyłączenia stosowania samej ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości opisanego w jej art. 3 pkt 1 (Dz.U. 2019.125). Ustawodawca wskazuje tam na brak możliwości stosowania przepisów tej ustawy do danych znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie:

- ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz.U.1982.35.228);
- ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz.U.1997. 90.557 ze zm.);
- ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U.1997.88.555 ze zm.);
- ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz.U.1999. 83.930 ze zm.);
- ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U.2001. 106.1148 ze zm.);
- ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz.U.2014. 24 ze zm.);
- ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz.U.2016.177 ze zm.).

Lista ta ma charakter enumeratywny, zatem wszelkie czynności, które nie są objęte RODO i których realizacja nie wymaga stosowania wymienionych ustaw, podejmowane będą w ramach przedstawionej niżej Polityki[3]. Z drugiej strony,

[3] Należy podkreślić, że straże nie zostały powołane do realizacji zadań związanych z zapewnieniem bezpieczeństwa narodowego, o których mowa w art. 3 pkt 2 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Nie ma zatem w praktyce możliwości zastosowania pełnego wyłączenia przepisów tej ustawy w oparciu

oznacza to, że należy dokonać przeglądu działań straży potencjalnie opartych na stosowaniu przepisów wskazanych w art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125), pod kątem oceny rozwiązań mających chronić dane osobowe. W praktyce straże gminne (miejskie) nie będą miały możliwości podejmowania czynności w oparciu o większość z nich, jednak – z uwagi na brak kryterium podmiotowego – nie jest wykluczone stosowanie przez straże części ze wskazanych ustaw. Dotyczy to zwłaszcza ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U.2001.106.1148 ze zm.) i ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U.1997.88.555 ze zm.). Zaznaczyć należy, że regulacje te, w odniesieniu do rozwiązań chroniących dane osobowe, nie mogą być oceniane jako wyczerpujące (nie zawierają bowiem wszystkich elementów wymaganych przez DODO), zatem to administrator zobowiązany będzie do przygotowania szczegółowych procedur pozwalających na działania godzące dotychczasową praktykę stosowania zawartych w nich przepisów z ich interpretacją dokonywaną w zgodzie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89). Takie podejście podyktowane jest regułą konstytucyjną nakazującą tzw. przychylną interpretację prawa krajowego, pozwalającą na możliwie pełne stosowanie prawa unijnego – w tym wypadku oznacza to konieczność takiej reinterpretacji przepisów proceduralnych, która zapewni realizację zasad DODO bez ingerencji w literalne brzmienie przywołanych wyżej aktów prawnych.

---

o to kryterium. Oczywiście w przypadku pojawienia się ustawowej podstawy dla realizacji tego typu zadań przez straże mogłoby się to stać możliwe, gdyż stosowanie go wyłącznie do: Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego nie wynika z tego przepisu, ponieważ lista instytucji nie ma charakteru enumeratywnego.

Fundamentem właściwej recepcji zasad ochrony danych w strażach gminnych (miejskich) jest zatem dokonanie pełnego przeglądu procesów przetwarzania i wyraźne wskazanie tych czynności, których realizacja odbywa się w oparciu o:

- RODO (i ustawę o ochronie danych osobowych (Dz.U.2018.1000 ze zm.)[4] – co przekłada się na stosowanie doń polityk i procedur właściwych dla całego urzędu, w którego strukturze działa konkretna straż;
- DODO (i ustawę o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) – co wymaga przyjęcia i wdrożenia polityki ochrony (której modelowe ujęcie stanowi główną część niniejszej publikacji) przez komendanta straży;
- DODO (i wyłączenia wskazane w art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) – co przekłada się na sprawdzenie, które i w jakim zakresie ustawy znajdują zastosowanie do działań realizowanych przez straże. Jeśli zidentyfikowane zostaną konkretne czynności realizowane na ich podstawie, wymagana będzie analiza stosowanych praktyk pod kątem dostosowania ich do zasad wynikających z samego DODO.

Jedynie takie kompleksowe podejście pozwoli na realne wdrożenie zasad ochrony danych w zakresie wszystkich działań realizowanych przez straże gminne (miejskie).

Mając na uwadze zapewnienie możliwie szerokiego odbioru przedstawionych poniżej propozycji modelowych, autorzy akceptują wykorzystanie tego wzorca przez odbiorców publikacji na wszelkich polach eksploatacji (w tym konieczność dokonywania przeróbek i adaptacji modelowej procedury wraz z załącznikami) w oparciu o licencję otwartą przy uwzględnieniu klauzuli uznania autorstwa (czyli konieczności wskazania autorstwa pierwotnego źródła całości lub fragmentu dokumentacji).

[4] Należy pamiętać, że ustawa ta podobnie jak tzw. ustawa wdrożeniowa przyniosła wiele zmian (m.in. w związku ze stosowaniem kpa), zatem przyjęte w urzędzie procedury muszą je uwzględniać.

II. Wprowadzenie

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), będąca efektem implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89), jak również skorelowane z nią przepisy:

1. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz.U.UE.L.2016.119.1);
2. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);

wskazują na:

1. konieczność dokumentowania przez komendanta wszystkich realizowanych przez Straż Gminną (Miejską) w [...] działań, w ramach których dochodzi do przetwarzania danych osobowych na mocy przepisów ustawy dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) wraz z aktami wykonawczymi,
2. obowiązek opracowania, przyjęcia i wdrożenia Polityki ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...]

ZAŁĄCZNIKI

Załącznik nr 1. Wzór strony tytułowej Polityki ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 1.1. Wzór Zarządzenia w sprawie wdrożenia polityki ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

III. Postanowienia ogólne

I.

1. Niniejsza Polityka ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...] (dalej: **Polityka** lub **Polityka ODO**) została ustanowiona i wdrożona przez Komendanta Straży Gminnej (Miejskiej) w [...] (dalej: **komendanta** lub **administratora**) na mocy przepisów:
   a. Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U.1997.78.483 ze zm.);
   b. ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) wraz z aktami wykonawczymi;
   c. ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) stanowiącej implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89).

2. Niniejsza Polityka nie stoi w sprzeczności z ustanowionymi w Urzędzie Gminy (Miejskim) w [...] standardami ochrony i przetwarzania informacji, w tym danych osobowych.

3. Polityka stanowi także element zbioru zasad ochrony informacji obowiązujących w Urzędzie Gminy (Miejskim) w [...] realizowanych na podstawie Polityki ochrony danych osobowych, która została opracowana i przyjęta w zgodzie z dobrymi praktykami oraz przepisami:
   a. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1);
   b. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.).

4. Polityka uwzględnia wymogi wynikające z norm ISO, takich jak np. PN-EN ISO/IEC 27002:2017 Technika informatyczna – Technika bezpieczeństwa – Praktyczne zasady zabezpieczania informacji. Warto przy tym zaznaczyć, że wyraźnie podkreśla się w nich fakt, że polityka bezpieczeństwa informacji powinna być dostępna w formie udokumentowanej informacji, ogłoszona wewnątrz organizacji oraz dostępna dla zainteresowanych stron, jeśli jest to właściwe. Jak wskazuje przywołana norma, w procesie budowy Polityki należy bezwzględnie uwzględnić:

a. zarządzanie aktywami (przetwarzanymi zbiorami danych),
b. kontrolę dostępu (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych),
c. środki ochrony kryptograficznej (polityka stosowania zabezpieczeń, zarządzanie kluczami),
d. bezpieczeństwo fizyczne i środowiskowe oraz bezpieczeństwo eksploatacji (zarządzanie zmianami, zarządzanie pojemnością, zapewnienie ciągłości działania, rejestrowanie zdarzeń i monitorowanie),
e. bezpieczeństwo komunikacji (zabezpieczenie, rozdzielenie sieci),
f. pozyskiwanie, rozwój i utrzymywanie systemów,
g. relacje z dostawcami (umowy, w tym umowy powierzenia przetwarzania),
h. zarządzanie incydentami związanymi z bezpieczeństwem informacjzarządzanie ciągłością działania,
i. zgodność z wymaganiami prawnymi i umownymi.

5. Niniejsza Polityka stanowi zbiór wymogów, zasad i regulacji ochrony danych osobowych obowiązujących w straży miejskiej, których administratorem danych jest jej komendant na mocy przepisów ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) z uwzględnieniem aktów wykonawczych skorelowanych z przepisami ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125).

6. Polityka zakresem swojego oddziaływania reguluje wymagania stawiane przez przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), a także wymagania wyłączone spod regulacji przywołanej ustawy, gdy przetwarzane dane znajdują się w aktach sprawy lub

czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie następujących przepisów:

a. ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz.U. 1982.35.228);
b. ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz.U.1997. 90.557 ze zm.);
c. ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. 1997. 88.555 ze zm.);
d. ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz.U. 1999. 83.930 ze zm.);
e. ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. 2001. 106.1148 ze zm.);
f. ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz.U. 2014. 24 ze zm.);
g. ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz.U. 2016.177 ze zm.).

7. Polityka stanowi o rozliczalności prawidłowego i zgodnego z prawem przetwarzania danych osobowych przez Straż Gminną (Miejską) w [...] w ramach realizowanej przez nią działalności.
8. Polityka skoncentrowana jest w szczególności na określeniu:
   a. zasad i warunków ochrony danych osobowych przetwarzanych przez straż w sposób:
      - całkowicie lub częściowo zautomatyzowany,
      - inny niż zautomatyzowany, w przypadku gdy dane te stanowią lub maja stanowić część zbioru danych,

      w celu realizacji zadań określonych w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) z uwzględnieniem aktów wykonawczych;
   b. praw osób, których dane osobowe są przetwarzane przez straż;
   c. sposobów prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez straż,
   d. obowiązków administratorów i podmiotów przetwarzających oraz inspektorów ochrony danych i tryby ich wyznaczania,

e. zasad współpracy pomiędzy współadministratorami danych,
f. sposobów zabezpieczenia danych osobowych,
g. zasad realizowania zadań z wykorzystaniem monitoringu wizyjnego,
h. metod podnoszenia świadomości wśród strażników.

II.

1. Niniejsza Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, właściwej ochrony wraz z zachowaniem ich autentyczności, poufności, integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz procedur karnych, o których mowa w przepisach ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125).
2. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych osobowych, obowiązujące procedury, instrukcje i inne dokumenty związane z Polityką muszą być stale weryfikowane i dostosowywane w ramach zaplanowanych przeglądów lub w następstwie ogłoszonych lub wprowadzonych zmian prawnych. Przeglądy dokumentacji odbywają się nie rzadziej niż co sześć miesięcy.
3. Pierwszy przegląd niniejszej Polityki pod kątem jej aktualności oraz skuteczności w zapewnieniu odpowiedniego poziomu bezpieczeństwa danych osobowych winien zostać przeprowadzony przez komendanta straży nie później niż w 2021 roku.[5]
4. W ramach realizowanych przeglądów Polityki niezbędne jest także ponowne dokonanie oceny skutków występujących operacji przetwarzania danych, w ramach których dochodzić może do wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych.

[5] Należy przyjąć, że rok, w którym wprowadzono Politykę jest rokiem, w którym należy dokonać przeglądu i który należy wskazać.

III.

1. Administratorem danych osobowych przetwarzanych w ramach realizacji zadań określonych w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.197.123.779 ze zm.), z uwzględnieniem aktów wykonawczych, jest komendant straży.
2. Administrator nie jest pracodawcą w stosunku do strażników w rozumieniu przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U.1974.24.141 ze zm.).
3. Polityka swoim zakresem obowiązywania obejmuje wszystkich odbiorców usług, dostawców, pracowników straży (w tym pracowników urzędu miejskiego), których dane osobowe straż w ramach występujących realizacji zadań przetwarza.
4. Każdy pracownik straży i urzędu miejskiego ma obowiązek zapoznania się z treścią niniejszej Polityki w zakresie odpowiadającym roli, jaką pełni w straży lub w związku z realizowanymi zadaniami. W tym celu wszystkie osoby dopuszczone do przetwarzania danych chronionych (w tym danych osobowych) w straży muszą zostać pouczone o warunkach i zasadach przetwarzania danych osobowych wynikających z obowiązujących w tym zakresie regulacji prawnych i wewnętrznych w straży i urzędzie, a także zobowiązane do zachowania w tajemnicy wszelkich danych oraz zasad i procedur ich przetwarzania oraz zabezpieczania.
5. Zasady określone w niniejszej Polityce stosuje się do informacji stanowiących dane chronione bez względu na formę ich zapisu oraz sposób ich przetwarzania.
6. Niniejsza Polityka ma zastosowanie zarówno do danych przetwarzanych w systemach informatycznych, za pośrednictwem urządzeń końcowych, w tym stacjach roboczych, komputerach przenośnych oraz w urządzeniach bezprzewodowych (w tym w urządzeniach mobilnych) bądź innych nośnikach danych, jak i danych przetwarzanych w sposób tradycyjny (w formie papierowej), z tym że za bezpieczeństwo systemów teleinformatycznych odpowiada wójt przy zaangażowaniu WOP oraz komendant i IOD.
7. Stosowanie niniejszej Polityki jest istotnym elementem procesu zarządzania ciągłością działania w rozumieniu ISO/EOC 22301:2014, za który odpowiedzialny jest wójt oraz komendant straży w zdefiniowanych procesach ochrony danych osobowych oraz innych informacji..

8. Poszczególne załączniki do Polityki objęte są tajemnicą i nie mogą być ujawniane bez dokonania przez komendanta uprzedniej analizy ich zawartości, z uwzględnieniem tego, że ujawnienie informacji tam zawartych może wpłynąć na bezpieczeństwo danych osobowych oraz na naruszenie praw i wolności osób, których dane są przetwarzane.
9. Nieprzestrzeganie postanowień zawartych w Polityce może skutkować zastosowaniem w pełnym zakresie sankcji dopuszczonych przez stosunek pracy oraz obowiązujące przepisy prawa.
10. Odpowiedzialny za opracowanie, wdrożenie i utrzymanie niniejszej Polityki jest komendant straży.

IV.

1. Ilekroć używa się w Polityce takich określeń jak:
   a. administrator – rozumie się przez to: właściwy organ, który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych; podmiot wskazany przez ustawę jako administrator, jeżeli cele i sposoby przetwarzania danych osobowych są określone w ustawie albo podmiot wskazany przez prawo Unii Europejskiej lub prawo państwa członkowskiego Unii Europejskiej, albo podmiot wyznaczony zgodnie z kryteriami określonymi w prawie tego państwa, z tym że:
      - administratorem danych osobowych przetwarzanych w związku z realizacją zadań, o których mowa w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.1123.779 ze zm.), z uwzględnieniem aktów wykonawczych, jest komendant;
      - administratorem danych osobowych przetwarzanych w szczególności w związku z prowadzonymi przez Urząd Gminy (Miejski) w […] czynnościami oraz postępowaniami administracyjnymi, a także przetwarzanymi na mocy 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 osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.) w celu realizacji

czynności kadrowo-płacowych i pokrewnych w stosunku do straży oraz samych strażników jest wójt;

b. autentyczność – rozumie się przez to właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących podmiot praw są takie jak deklarowane;

c. ABI – rozumie się przez to administratora bezpieczeństwa informacji odpowiedzialnego za bezpieczeństwo całości informacji w urzędzie (z wyłączeniem zakresu wynikającego z odrębności ochrony informacji niejawnych), ale nie jest on tutaj tożsamy z ABI funkcjonującym na gruncie ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U.1997.133.883 ze zm.), który zajmował się działaniami związanymi z ochroną danych osobowych;

d. ASI – rozumie się przez to administratora systemów informatycznych odpowiedzialnego za bezpieczeństwo danych przetwarzanych za pośrednictwem systemów informatycznych, w tym za bazy danych w rozumieniu przepisów ustawy z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U.2018.2339), usytuowanego w strukturach WOP;

e. bezpieczeństwo danych – rozumie się przez to całość działań skoncentrowanych na zapewnieniu przetwarzanym danym autentyczności, poufności, integralności, dostępności oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i organizacyjnych, zapewniających ochronę przed nieuprawnionym przetwarzaniem tych danych i odpowiednich do zagrożeń i kategorii danych objętych ochroną;

f. dane biometryczne – rozumie się przez to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, które umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Dane osobowe (np. wizerunek twarzy, nagranie poruszającej się osoby) nie stanowią jednak danych biometrycznych do czasu podjęcia specjalnego przetwarzania technicznego pozwalającego na osiągnięcie wskazanych cech osobowych.

g. dane dotyczące zdrowia – rozumie się przez to dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym dane

o korzystaniu z usług opieki zdrowotnej, które ujawniają informacje o stanie jej zdrowia;

h. dane genetyczne – rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby;

i. dane osobowe – rozumie się przez to dane osobowe, o których mowa w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz.U.UE.L.2016.119.1);

j. dane wrażliwe – rozumie się przez to dane osobowe o których mowa w art. 14 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), czyli dane ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej;

k. dane osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony – rozumie się przez to dane, o których mowa w art. 19 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);

l. dane osób skazanych za czyn zabroniony – rozumie się przez to dane, o których mowa w art. 19 pkt 2 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);

m. dane pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego – rozumie się przez to dane, o których mowa w art. 19 pkt 3 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych

przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);

n. dane innych osób związanych z czynem zabronionym – rozumie się przez to dane, o których mowa w art. 19 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), czyli dane osobowe takich osób, jak osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub uczestniczyć w postępowaniu na jego dalszych etapach , osoby, które mogą dostarczyć informacji o czynach zabronionych lub osoby, które mają kontakty lub powiązania z jedną z osób skazanych za czyn zabroniony lub pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;

o. dobra osobiste – rozumie się przez to dobra osobiste człowieka, w szczególności takie jak: zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa lub artystyczna bądź wynalazcza i racjonalizatorska, które pozostają objęte ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach, o których mowa w ustawie z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U.1964.16.93 ze zm.);

p. dokument – rozumie się przez to każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa bądź stosunku prawnego, bądź okoliczności mającej znaczenie prawne – w znaczeniu art. 115 §14 ustawy z dnia 6 czerwca 1997 r – Kodeks karny (Dz.U.1987.88.553 ze zm.);

q. dostępność – rozumie się przez to właściwość gwarantującą osobie upoważnionej nieutrudniony dostęp do danych osobowych;

r. dron – rozumie się przez to bezzałogowe urządzenie zdolne do unoszenia się w atmosferze na skutek oddziaływania powietrza innego niż oddziaływanie powietrza odbitego od podłoża, w znaczeniu art. 2 ust 1 ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U.2002.130.1112 ze zm.), które może być wyposażone w rejestrator danych lub inne urządzenia rejestrujące;

s. eog – rozumie się przez to europejski obszar gospodarczy;

t. ewidencja osób upoważnionych do przetwarzania danych osobowych/ wykaz osób uprawnionych – rozumie się przez to ewidencję i wykaz, o której mowa w art. 42 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);

u. fotopułapka – rozumie się przez to rejestrator danych umożlwiający rejestrację i/lub przesył informacji na odległość, którego obudowa umożliwia jego zamaskowanie;

v. hasło – rozumie się przez to ciąg znaków alfanumerycznych znany jedynie użytkownikowi;

w. identyfikator – rozumie się przez to ciąg znaków literowych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

x. incydent ochrony danych osobowych – rozumie się przez to zdarzenie albo serię niepożądanych lub niespodziewanych zdarzeń dotyczących ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań dokonywanych w ramach procesów przetwarzania danych oraz powstania zagrożenia ochrony danych osobowych;

y. informacja – rozumie się przez to każdy komunikat o jakimś fakcie wyrażony i utrwalony w dowolnej formie, który jest możliwy do zinterpretowania i odczytania zarówno przez jego twórcę, jak i odbiorcę;

z. integralność – rozumie się przez to właściwość zapewnienia dokładności i kompletności posiadanych aktywów (zasobów);

aa. IOD – rozumie się przez to inspektora ochrony danych:

- IOD w Urzędzie Gminy (Miejskim) w [...] powołanego na podstawie przepisów 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 osobowych) (Dz.U.UE.L.2016.119.1) realizującego zadania określone dla IOD w tym akcie prawnym;
- IOD w Straży Gminnej (Miejskiej) w [...] powołanego na podstawie przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem

przestępczości (Dz.U.2019.125) i realizującego zadania określone dla IOD w tym akcie prawnym
lub w zależności od przyjętego modelu;

- IOD powołanego na podstawie przepisów 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 osobowych) (Dz.U.UE.L.2016.119.1) oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) realizującego zadania określone dla IOD w tych aktach prawnych;

bb. komendant – rozumie się przez to Komendanta Straży Gminnej (Miejskiej) w [...] w rozumieniu przepisów ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.);

cc. kpa – rozumie się przez to ustawę z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U.1960.30.168 ze zm.);

dd. KRI – rozumie się przez to rozporządzenie 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 (Dz.U. 2012 poz. 526);

ee. mapowanie procesów – rozumie się przez to ujawnienie i opisanie oraz powiązanie wszystkich występujących procesów w celu zidentyfikowania zasobów informacyjnych i czynności przetwarzania danych osobowych, a także innych elementów, które mogą mieć wpływ na prawidłowość przetwarzania danych osobowych;

ff. naruszenie ochrony danych – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

gg. niezaprzeczalność – rozumie się przez to brak możliwości zanegowania uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w takiej wymianie;

hh. niezawodność – rozumie się przez to właściwość oznaczającą spójne, zamierzone zachowanie i skutki;

ii. obszar przetwarzania danych – rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione, a także inne miejsce, w tym miejsce w sferze publicznej, w którym dochodzi do przetwarzania danych osobowych w imieniu administratora;

jj. odbiorca – rozumie się przez to osobę fizyczną lub prawną, organ władzy publicznej, jednostkę organizacyjną lub inny podmiot, któremu ujawnia się dane osobowe, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego Unii Europejskiej, a przetwarzanie tych danych jest zgodne z przepisami o ochronie danych mającymi zastosowanie do ich celów przetwarzania;

kk. ograniczenie przetwarzania – rozumie się przez to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

ll. organ nadzorczy w innych państwach Unii Europejskiej – rozumie się przez to niezależny organ publiczny ustanowiony przez inne niż Rzeczpospolita Polska państwo członkowskie Unii Europejskiej, powołany dla ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej;

mm. operacje w przestrzeni powietrznej – rozumie się przez to lot w określonym celu, po spełnieniu wymagań prawnych;

nn. operator systemu – rozumie się przez to dowolną osobę prawną lub fizyczną eksploatującą lub zamierzającą eksploatować co najmniej jeden bezzałogowy system powietrzny (w skład bezzałogowego systemu wchodzi bezzałogowy statek i wyposażenie do zdalnego sterowania nim);

oo. organizacja międzynarodowa – rozumie się przez to organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;

pp. osoba, podmiot danych – rozumie się przez to osobę, której dane dotyczą;

qq. organ nadzorczy – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych (z siedzibą przy ulicy Stawki 2, 00–193 Warszawa);

rr. państwo trzecie – rozumie się przez to państwa spoza eog oraz te, które nie stosują ustaleń z Schengen;

ss. pilot systemu – rozumie się przez to osobę fizyczną odpowiedzialną za bezpieczne wykonanie operacji dronem;

tt. podmiot przetwarzający – rozumie się przez to osobę fizyczną lub prawną, organ władzy publicznej, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

uu. poufność – rozumie się przez to właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom;

vv. profilowanie – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na ich wykorzystaniu do oceny niektórych cech osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

ww. Polityka – rozumie się przez to niniejszą Politykę ochrony danych osobowych w Straży Gminnej (Miejskiej) w […];

xx. pracodawca – rozumie się przez to Urząd Gminy (Miejski) w […] reprezentowany przez wójta;

yy. pracownik urzędu – rozumie się przez to pracownika, o którym mowa w ustawie z dnia 21 listopada 2008 r. o pracownikach samorządowych (Dz.U.2008.223.1458 ze zm.);

zz. przetwarzanie – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie bądź niszczenie;

aaa. pseudonimizacja – rozumie się przez to przetworzenie danych osobowych w taki sposób, aby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

bbb. rcpd – rozumie się przez to rejestr czynności przetwarzania danych osobowych w znaczeniu art. 30 RODO;

ccc. rejestrator danych – rozumie się przez to każde urządzenie, które umożliwia rejestrację obrazu, dźwięku lub innych informacji, na podstawie których można ustalić konkretną osobę fizyczną;

ddd. rkpd – rozumie się przez to rejestr kategorii czynności przetwarzania danych osobowych w znaczeniu art. 35 ustawy o ochronie;

eee. RODO – rozumie się przez to 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 osobowych) (Dz.U.UE.L.2016.119.1);

fff. rozliczalność – rozumie się przez to właściwość pozwalającą przypisać określone działanie konkretnej osobie fizycznej lub procesowi oraz umiejscowić je w czasie, a także właściwość zapewniającą, że administrator wypełniana wszystkie obowiązki określone w katalogu zasad dotyczących przetwarzania danych osobowych, w tym przede wszystkim te związane z zapewnieniem bezpieczeństwa, ochrony i dostępu do danych osobowych wyłącznie osobom uprawnionym i jest w stanie daną właściwość przypisać konkretnej osobie fizycznej;

ggg. strażnik – rozumie się przez to strażnika, o którym mowa w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.);

hhh. straż – rozumie się przez to Straż Gminną (Miejską) w [...], funkcjonującą w strukturach organizacyjnych Urzędu Gminy (Miejskiego) w [...] jako wydział;

iii. sygnalista – rozumie się przez to osobę dokonującą zgłoszenia o naruszeniu prawa, której należy zapewnić szczególną ochronę danych osobowych;

jjj. ustawa – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);

kkk. ustawa o dostępności – rozumie się przez to ustawę z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U 2019.848);

lll. ustawa o ochronie – rozumie się przez to ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);

mmm. ustawa o informatyzacji – rozumie się przez to ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2005.64.565 ze zm.);

nnn. udip – rozumie się przez ten skrót ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001.112.1198 ze zm.)

ooo. ustawa o strażach – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.);

ppp. uwierzytelnianie – rozumie się przez to uwiarygodnienie tożsamości pozwalającej na dostęp do zasobów;

qqq. urząd – rozumie się przez to Urząd Gminy (Miejski) w [....];

rrr. urządzenia rejestrujące dane – rozumie się przez to w szczególności urządzenia, o których mowa w art. 10 ust 2a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) oraz rozporządzeniu Rady Ministrów z dnia 16 grudnia 2009 r. w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną/ miejską (Dz.U. 2009.220.1720), a także inne urządzenia, których zasoby informacyjne zebrane w innym celu niż przetwarzanie danych osobowych umożliwiają zidentyfikowanie konkretnej osoby fizycznej;

sss. użytkownik – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator;

ttt. wkcp – rozumie się przez to wykaz kategorii czynności przetwarzania danych osobowych;

uuu. właściwy organ – rozumie się przez to organ władzy publicznej, jednostkę organizacyjną lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych;

vvv. WOP – rozumie się przez to Wydział Organizacyjno-Prawny, w strukturach którego znajduje się ASI i ABI;

www. wójt – rozumie się przez to Wójta Gminy [...];

xxx. współadministrowanie – rozumie się przez to co najmniej dwóch administratorów, którzy wspólnie ustalają cele i sposoby przetwarzania danych osobowych, a w wyniku wspólnych uzgodnień w przejrzysty sposób wspólnie określają odpowiednie zakresy swojej odpowiedzialności dotyczące wypełniania obowiązków wynikających z przepisów prawa wobec podmiotu praw, których dane wspólnie przetwarzają;

yyy. zbiór danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego czy jest scentralizowany, zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie;

zzz. zgoda – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, w ramach którego dana osoba przyzwala na przetwarzanie dotyczących jej danych osobowych.

IV. Zasady przetwarzania danych osobowych

1. Dopuszczalny zakres przetwarzania danych osobowych:
   a. Straż może przetwarzać dane osobowe wyłącznie w zakresie niezbędnym w celu zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
   b. Straż może przetwarzać dane osobowe zebrane pierwotnie w jednym z celów związanych z realizacją zadań, o których mowa w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.), w innych nowych celach, o których mowa w tej samie ustawie, o ile:
      - administrator wykaże, że wolno przetwarzać mu takie dane osobowe w innym nowym celu na mocy odrębnych przepisów;

- przetwarzanie jest niezbędne i proporcjonalne w tym innym nowym celu na mocy odrębnych przepisów.

c. Straż może przetwarzać dane osobowe w innych celach niż określone w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.), jeżeli przepisy prawa wymagają ich przetwarzania.

d. Straż może przetwarzać dane osobowe zebrane do celów, o których mowa w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.), w zakresie niezbędnym do ich archiwizacji w interesie publicznym oraz do celów naukowych, statystycznych lub historycznych, o ile proces ten podlega odpowiednim zabezpieczeniom praw i wolności osób, których dane dotyczą (np. pseudonimizacja lub nawet anonimizacja).

2. Przetwarzanie danych wrażliwych:

a. Niedopuszczalne jest przetwarzanie danych wrażliwych, czyli danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej.

b. Dopuszcza się przetwarzanie danych wrażliwych jeżeli:

- inne przepisy prawa wymagają na ich przetwarzanie lub
- jest to niezbędne dla ochrony życia lub zdrowia lub interesów osoby, której dane dotyczą bądź innej osoby, lub
- dane takie zostały upublicznione przez osobę, której dotyczą (a posługiwanie się nimi nie łamie zasady minimalizacji i niezbędności).

3. Zautomatyzowane podejmowanie rozstrzygnięć w indywidualnych przypadkach:

a. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, mające dla niej niekorzystne skutki prawne lub poważnie na nią wpływające, wyłącznie w wyniku przetwarzania danych osobowych w sposób zautomatyzowany, w tym w wyniku profilowania, chyba że dopuszczają to przepisy prawa, którym podlega administrator i które przewidują odpowiednie zabezpieczenia praw

i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ze strony administratora.

b. Rozstrzygnięcia, o których mowa w pkt a, nie mogą opierać się na danych wrażliwych, chyba że istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.

c. Niedopuszczalne jest dokonywanie profilowania osób fizycznych na podstawie danych wrażliwych skutkującego dyskryminacją tych osób.

4. Weryfikacja danych osobowych:

a. Administrator przeprowadza mapowanie procesów według załączonego wzoru mapy procesów.

b. Administrator dokonuje weryfikacji danych osobowych w terminach określonych przez przepisy szczególne, regulujące działania właściwego organu, a jeżeli przepisy te nie określają terminu – nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych, z czego sporządza protokół według załączonego wzoru protokołu przeglądu zasobów informacyjnych. Pierwszy przegląd administrator obowiązany był przeprowadzić w 2020 r. Administrator prowadzi, aktualizuje, monitoruje i chroni Rejestr przeglądów według załączonego wzoru Rejestru przeglądów.

c. Weryfikacji dokonuje się w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane usuwa się, z zastrzeżeniem zawartym w pkt 5 (poniżej) oraz przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U.1983.38.173 ze zm.) oraz przepisów ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.).

5. Anonimoizacja – przekształcanie danych osobowych nie wymagających czynnika identyfikującego osobę, tj. tego typu dane można przekształcić w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobowych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej.

6. Anonimizacja danych osobowych przetwarzanych w związku z dokumentowaniem czynności organów. Jest to elektroniczna kopia akt kontrolnych. W tym przypadku dane pozostawia się po ich zanonimizowaniu.

7. Rozróżnianie danych osobowych przy ich przetwarzaniu – administrator zapewnia rozróżnienie, o ile jest ono możliwe lub nie jest dalece utrudnione, na dane osobowe dotyczące:

- osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
- osób skazanych za czyn zabroniony;
- pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;
- innych osób związanych z czynem zabronionym, takich jak: osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania; osoby, które mogą dostarczyć informacji o czynach zabronionych lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa powyżej.

8. Rozróżnianie danych osobowych przy ich przetwarzaniu – administrator zapewnia rozróżnienie, o ile jest ono możliwe lub nie jest dalece utrudnione, na:

- dane osobowe mające swoje źródło w faktach;
- dane osobowe mające swoje źródło w indywidualnych ocenach.

9. Przesyłanie lub udostępnianie danych osobowych innym organom, państwom trzecim lub organizacjom międzynarodowym:

a. Straż może przesyłać lub udostępniać dane osobowe innym właściwym organom, państwu trzeciemu lub organizacji międzynarodowej po uprzednim zweryfikowaniu, w miarę potrzeby i możliwości, prawidłowości, kompletności i aktualności tych danych.

b. Straż przesyłając dane osobowe odbiorcy, o którym mowa w ppkt a, przekazuje, w miarę potrzeby i możliwości, niezbędne dodatkowe informacje pozwalające temu odbiorcy ocenić stopień prawidłowości, kompletności oraz aktualności przesłanych danych osobowych.

c. Straż, gdy prześle odbiorcy, o którym mowa w ppkt a, nieprawdziwe, niekompletne lub nieaktualne dane osobowe lub przesłał te dane z naruszeniem przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), jest obowiązana bez zbędnej zwłoki poinformować o tym tego odbiorcę oraz:

- sprostować, uzupełnić lub uaktualnić te dane, a także przesłać temu odbiorcy dane właściwe, chyba że z uwagi na upływ czasu jest to oczywiście nieuzasadnione, albo

- usunąć lub ograniczyć przetwarzanie tych danych, a także poinformować o tym tego odbiorcę w celu usunięcia lub ograniczenia przez tego odbiorcę przetwarzania tych danych.

d. Ograniczenie przetwarzania danych, o którym mowa w ppkt. c następuje w przypadku gdy:
   - osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić, lub
   - dane osobowe muszą zostać zachowane do celów dowodowych.

e. Ograniczeń przetwarzania danych określonych w ppkt. a–d nie stosuje się w przypadku gdy przesłanie lub udostępnienie danych osobowych odbiorcy, o którym mowa w ppkt a, mogłoby stanowić zagrożenie praw i wolności człowieka i obywatela, a także w przypadkach gdy:
   - osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić;
   - dane osobowe, które podlegają usunięciu, muszą zostać zachowane do celów dowodowych.

f. Jeżeli szczególne przepisy prawa zezwalają, straż przesyłając dane, jest obowiązana do poinformowania odbiorcy takich danych osobowych o tych warunkach i obowiązku ich przestrzegania.

ZAŁĄCZNIKI

Załącznik nr 2. Wzór Mapy procesów w Straży Gminnej (Miejskiej) w […].

V. Zasady i mechanizmy utrzymania merytorycznej poprawności przetwarzania danych osobowych

1. Administrator przy przetwarzaniu danych osobowych obowiązany jest do przestrzegania określonych zasad, takich jak:
   a. Zasada legalności – administrator może przetwarzać dane osobowe, o ile wykaże podstawę prawną w celu przestrzegania obowiązujących norm prawnych zgodnie z koncepcją źródeł prawa przyjętą w Konstytucji RP.
   b. Zasada rzetelności – administrator przetwarzając dane osobowe, zobowiązany jest nadzorować procesy przetwarzania danych osobowych, tak

aby były one precyzyjne, dokładne i poprawne; w tym wypełnienie obowiązku informacyjnego

c. Zasada niezbędności stosowania środków ochrony danych – administrator zapewniając bezpieczeństwo danych w procesie przetwarzania danych, zobowiązany jest wziąć pod uwagę rodzaj, zakres i skalę przetwarzanych danych, a także liczbę podmiotów danych, których dotyczy przetwarzanie.

d. Zasada celowości – administrator może przetwarzać dane osobowe, zgodnie z pierwotnym celem ich pozyskania o ile zamierzony cel ich przetwarzania jest konkretny i uzasadniony.

e. Zasada adekwatności (tzw. minimalizacja danych – dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane) – administrator przetwarza dane osobowe wyłącznie w minimalnym, niezbędnym do osiągnięcia określonego celu zakresie, a okres ich przechowywania powinien być nie dłuższy niż jest to konieczne do osiągnięcia tego celu. Innymi słowy, zasada minimalizmu wskazuje, że zakres przetwarzanych danych musi korespondować z celem przetwarzania danych bez nadmiernego gromadzenia danych (zasada tzw. minimalizacji danych).

f. Zasada merytorycznej poprawności – administrator może przetwarzać dane osobowe tylko wtedy, gdy są zgodne z rzeczywistością, czyli stanem faktycznym. W przypadku ich nieaktualności obowiązany jest do podjęcia działań zmierzających do zapewnienia ich merytorycznej poprawności.

g. Zasada ograniczenia czasowego przetwarzania – administrator obowiązany jest przechowywać dane w formie umożliwiającej identyfikację osób, których one dotyczą przez okres nie dłuższy niż jest to niezbędne do celów przetwarzania. Czasowym wyznacznikiem przechowywania danych jest czas, w którym zostanie osiągnięty zamierzony przez administratora cel. Po osiągnięciu celu dane osobowe winny utracić walor danych osobowych na skutek poddania ich co najmniej procesowi pozbawienia cech identyfikacyjnych lub też wskutek usunięcia ich ze zbioru danych.

h. Bezpieczeństwo danych – administrator obowiązany jest zapewnić przetwarzanym danym:

- poufność – czyli właściwość polegającą na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
- dostępność – czyli właściwość polegającą na tym, że informacja jest dostępna i użyteczna na żądanie autoryzowanego podmiotu lub autoryzowanej osoby;
- integralność – czyli właściwość polegającą na tym, że informacja jest dokładna i kompletna;
- autentyczność i rozliczalność – czyli właściwość polegającą na tym, że informacje są merytorycznie poprawne oraz zapewnione zostały odpowiednie mechanizmy logowania zdarzeń w zgodzie z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (KRI). Rozliczalność rozumiana jest jako właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.

2. Każda operacja przetwarzania danych osobowych prowadzona w zautomatyzowanych systemach przetwarzania musi być ewidencjonowana w co najmniej następującym zakresie:
   a. zbieranie,
   b. modyfikowanie,
   c. przeglądanie,
   d. ujawnianie wraz z przekazywaniem,
   e. łączenie,
   f. usuwanie.
3. Ewidencja, o której mowa w pkt 2 winna być prowadzona automatycznie oraz pozwalać w każdym czasie uzyskać następujące zmienne:
   a. datę i godzinę operacji,
   b. tożsamość osoby, która przeglądała, ujawniła lub usunęła dane.
4. Za poprawność i funkcjonowanie ewidencji odpowiada WOP oraz administrator systemu.
5. Za nadzór i monitorowanie ewidencji odpowiada komendant.
6. Ewidencja winna być przechowywana przez system z możliwością jej wygenerowana na żądanie osoby uprawnionej.
7. Wygenerowana ewidencja powinna zawierać poza żądanymi danymi także:
   a. datę i godzinę wygenerowania,

b. datę i godzinę wydruku,
c. oznaczenie osoby, która wygenerowała ewidencje,
d. oznaczenie osoby, która dokonała wydruku ewidencji.

8. Wszelkie wątpliwości z zakresu ochrony danych powstałe w szczególności w ramach procesu realizacji praw osób, których dane dotyczą oraz obsługi naruszeń administrator obowiązany jest rozwiązywać w ramach konsultacji z IOD.

VI. Przegląd procesów

1. Administrator obowiązany jest do:
   a. ujawnienia wszystkich występujących w straży procesów, w ramach których dochodzi do przetwarzania danych osobowych;
   b. oceny wszystkich występujących w straży procesów, w ramach których dochodzi do przetwarzania danych osobowych pod kątem ich bezpieczeństwa i prawidłowości;
   c. stałego monitorowania i aktualizowania występujących w straży procesów, w ramach których dochodzi do przetwarzania danych osobowych;
   d. przeprowadzania co najmniej raz do roku kompleksowego przeglądu wszystkich występujących w straży procesów, w ramach których dochodzi do przetwarzania danych osobowych.
2. Administrator dokonuje przeglądu i aktualizacji występujących w straży procesów, w ramach których dochodzi do przetwarzania danych osobowych, mając na uwadze w szczególności określone kompetencje (zadania), takie jak:
   a. ochrona spokoju i porządku w miejscach publicznych;
   b. czuwanie nad porządkiem i kontrola ruchu drogowego;
   c. kontrola publicznego transportu zbiorowego;
   d. współdziałanie z właściwymi podmiotami w zakresie ratowania życia i zdrowia, udzielania pomocy w usuwaniu awarii, usuwaniu skutków klęsk żywiołowych oraz usuwaniu innych zagrożeń w innych miejscach;
   e. realizacja zadań zleconych przez inne organizacje w zakresie innym niż wymienione powyżej (w pdpkt d);
   f. zabezpieczenie miejsca przestępstwa, katastrofy lub innego podobnego zdarzenia albo miejsc zagrożonych takim zdarzeniem przed dostępem osób postronnych lub zniszczeniem śladów i dowodów, do momentu

przybycia właściwych służb, a także ustalenie, w miarę możliwości, świadków zdarzenia;

g. ochrona obiektów komunalnych i urządzeń użyteczności publicznej;

h. współdziałanie z organizatorami i innymi służbami w ochronie porządku podczas zgromadzeń i imprez publicznych;

i. doprowadzanie osób nietrzeźwych do izby wytrzeźwień lub miejsca ich zamieszkania, jeżeli osoby te zachowaniem swoim dają powód do zgorszenia w miejscu publicznym, znajdują się w okolicznościach zagrażających ich życiu lub zdrowiu albo zagrażają życiu i zdrowiu innych osób;

j. informowanie społeczności lokalnej o stanie i rodzajach zagrożeń, a także inicjowanie i uczestnictwo w działaniach mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi;

k. konwojowanie dokumentów, przedmiotów wartościowych lub wartości pieniężnych na potrzeby gminy;

l. prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, w przypadku gdy czynności te są niezbędne do wykonywania zadań;

m. realizacja uchwał;

n. realizacja poleceń wójta;

o. wnioski związane z realizacją praw, osób których dane dotyczą;

p. wnioski w zakresie innym niż powyżej;

q. skargi;

r. ewidencja;

s. sprawozdania;

t. inne.

3. Proces przetwarzania danych może obejmować realizację jednego lub kilku zadań straży. W uzasadnionych przypadkach administrator decyduje o wyodrębnieniu kilku procesów pozwalających na pełną realizację jednego zadania.

4. Po przeprowadzaniu przeglądu administrator dokonuje niezwłocznie niezbędnych działań naprawczych oraz zaradczych, o ile taka niezbędność wystąpi.

5. Dane z przeprowadzonego przeglądu administrator wykorzystuje w celu zapewnienia bezpieczeństwa danych oraz do oceny zagrożeń dla realizowanych procesów, w ramach których dochodzi do przetwarzania danych.
6. Administrator prowadzi rejestr przeglądów zgodnie ze wzorem Rejestru przeglądów procesów.

ZAŁĄCZNIKI
Załącznik nr 3. Wzór Protokołu przeglądu zasobów informacyjnych w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 4 .Wzór Rejestru przeglądów zasobów informacyjnych w Straży Gminnej (Miejskiej) w [...]..

VII. Wykaz niezbędnych środków technicznych i organizacyjnych

1. Administrator obowiązany jest stosować odpowiednie środki techniczne i organizacyjne przy uwzględnieniu wprowadzonych w urzędzie polityk, procedur i regulaminów.
2. Wykaz przykładowych zaleceń w zakresie wymaganych środków technicznych i organizacyjnych zawiera załącznik nr 5.
3. Wskazany niezbędny zakres środków technicznych i organizacyjnych winien być przez administratora wdrożony oraz sukcesywnie modyfikowany, monitorowany i nadzorowany.
4. Wykaz winien być aktualizowany nie rzadziej niż następuje aktualizacja niniejszej Polityki.
5. Wzór ewidencji zmian, wdrożeń, przeglądów i zaleceń zawiera załącznik nr 6.
6. Wzór ewidencji nośników informatycznych zawiera załącznik nr 7.
7. Wzór Ewidencji rejestrów, ewidencji i wykazów zawiera załącznik nr 8.
8. Wzór Rejestru systemów i aplikacji zawiera załącznik nr 9.
9. Rejestry prowadzi i aktualizuje komendant.
10. Rejestry mogą być prowadzone w formie elektronicznej zapewniającej rozliczalność.

ZAŁĄCZNIKI

Załącznik nr 5. Wzór Wykazu przykładowych zaleceń w zakresie wymaganych środków technicznych i organizacyjnych w Straży Gminnej (Miejskiej) w [...]

Załącznik nr 6. Wzór Rejestru ewidencji zmian, wdrożeń, przeglądów i zaleceń w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 7. Wzór Rejestru nośników informatycznych w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 8. Wzór Ewidencji rejestrów ewidencji i wykazów w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 9. Wzór Rejestru systemów i aplikacji w Straży Gminnej (Miejskiej) w [...].

VIII. Metody i środki uwierzytelniania

1. Nazwa i hasło użytkownika:
   a. Uwierzytelnienie użytkownika w systemie informatycznym następuje po podaniu nazwy użytkownika i hasła.
   b. Nazwa użytkownika stanowi identyfikator, który w sposób jednoznaczny przypisany został konkretnemu użytkownikowi.
   c. Identyfikator składa się z ciągu znaków identyfikujących osobę (proponuje się stosowanie unikalnych ciągów znaków trudnych do odgadnięcia dla osób trzecich).
   d. Niedopuszczalne jest funkcjonowanie kilku takich samych nazw użytkowników. Raz przypisana nazwa nie podlega zmianie i nie może zostać wykorzystana w przyszłości przez innego użytkownika.
   e. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, WOP nadaje inny identyfikator, odstępując od zasady określonej w ppkt d.
   f. Hasło powinno składać się z unikalnego zestawu co najmniej 12 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne, w tym znaki o różnej charakterystyce, wielkości i znaczeniu.

g. Hasło nie może:
   - być identyczne z identyfikatorem użytkownika;
   - być identyczne z imieniem lub nazwiskiem użytkownika;
   - odnosić się do innych cech szczególnych użytkownika;
   - być ponowieniem hasła stosowanego wcześniej, jeżeli od ostatniego zastosowania danej kombinacji nie upłynął rok.

h. Niedopuszczalne jest zapamiętywanie haseł przez system.

i. Pierwsze nadane hasło ulega zmianie przez użytkownika.

j. W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg liczbowy wprowadzonych błędnych haseł na 2–3. Po przekroczeniu limitu powinna nastąpić automatyczna blokada konta.

k. Użytkownik odpowiada za działania wykonywane w systemie przy użyciu jego nazwy oraz za zachowanie hasła w tajemnicy.

l. Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 90 dni.

m. W przypadku braku okresowej zmiany hasła przez użytkownika, zmiana hasła winna być wymuszana przez system.

2. Zasady korzystania ze stacji roboczej:

a. Przed rozpoczęciem pracy użytkownik obowiązany jest sprawdzić stan urządzeń oraz dokonać oględzin swojego stanowiska pracy w celu wykrycia ewentualnych nieprawidłowości mogących świadczyć o naruszeniu bezpieczeństwa danych osobowych.

b. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika lub administratora.

c. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), a także wydruki leżące na biurkach oraz w otwartych szafach.

d. Zasady rozpoczęcia pracy:
   - włączenie napięcia w listwie podtrzymującej napięcie,
   - włączenie monitora i stacji roboczej,
   - zalogowanie się poprzez wprowadzenie nazwy użytkownika i hasła,
   - uruchomienie programu użytkowego.

e. Zasady czasowego opuszczenia stanowiska pracy:
   - zablokowanie sesji na stacji roboczej,
   - odblokowanie sesji po podaniu hasła.

f. W przypadku bezczynności stacji roboczej przez czas przekraczający 1 minutę automatycznie włącza się wygaszacz ekranu, który powinien być zaopatrzony w hasło umożliwiające ponowne podjęcie pracy na stacji roboczej.

g. Zasady zakończenia pracy:
   - zakończenie pracy programu zgodnie z instrukcją obsługi,
   - wylogowanie z systemu,
   - wyłączenie stacji roboczej i monitora,
   - wyłączenie napięcia w listwie podtrzymującej napięcie.

h. Krótkotrwała przerwa w pracy, podczas której użytkownik nie opuszcza stanowiska roboczego, nie wymaga zamykania aplikacji, wylogowania.

i. Każdorazową zmianę użytkownika stacji roboczej musi poprzedzać wylogowanie się użytkownika, który poprzednio z niej korzystał.

3. Zasady korzystania z komputerów przenośnych:

a. Przetwarzanie danych poza obszarem przetwarzania na komputerze przenośnym wymaga uzyskania uprzedniej indywidualnej zgody administratora.

b. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują zasady określone dla pracy na komputerach stacjonarnych, w tym także obowiązują następujące wymogi:
   - zabezpieczenie dostępu do systemu i zasobów oddzielnym hasłem – podwójne uwierzytelnianie;
   - zastosowanie oprogramowania i zabezpieczeń analogicznie do rozwiązań przyjętych na stacjonarnych stacjach roboczych;
   - szyfrowanie dysku;
   - komputer przenośny nie może być podstawowym oraz jedynym nośnikiem danych na nim zgromadzonych.

c. Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są opatrzone hasłem dostępu.

d. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

e. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów.

f. Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na serwerze administratora, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.

g. Osoba wykorzystująca komputer przenośny obowiązana jest do:
   - wykorzystywania go wyłącznie do określonych celów, mieszczących się w zakresie upoważnienia;
   - nieudostępniania komputera nieupoważnionym osobom;
   - zachowania szczególnej ochrony przed kradzieżą, zwłaszcza podczas transportu;
   - zaniechania jakichkolwiek zmian oprogramowania.

h. W przypadku konieczności dokonania zmiany, aktualizacji albo naprawy komputera należy zgłosić ten fakt administratorowi.

i. Należy zapewnić szyfrowane połączenie/ tunel VPN pomiędzy mobilnym urządzeniem a serwerem z jednoczesnym ograniczeniem dostępu przez niezaufanych dostawców telekomunikacyjnych (zakaz korzystania z niezaufanych access point - punktów dostępowych do Internetu).

j. Administrator w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:
   - postępowania w razie nieobecności w pracy dłuższej niż 30 dni – jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym administratora i uzgodnić z nim zwrot komputera;
   - zwrotu sprzętu w razie ustania stosunku zatrudnienia.

4. Zasady korzystania z telefonów komórkowych.

Wymagania w zakresie użytkowania oraz ochrony i zapewnienia bezpieczeństwa odnoszące się do komputerów przenośnych mają zastosowanie również do telefonów komórkowych, w szczególności wyposażonych w systemy gromadzenia danych.

IX. Bezpieczeństwo systemu informatycznego i danych osobowych

1. Ochrona antywirusowa:
   a. W straży istnieje bezwzględny wymóg instalacji oprogramowania antywirusowego na każdym stanowisku roboczym, zarówno na komputerach stacjonarnych, jak i przenośnych wykorzystywanych do przetwarzania danych.
   b. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez administratora za pośrednictwem WOP.
   c. Oprogramowanie, o którym mowa w ppkt b, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
   d. Niezależnie od ciągłego nadzoru, o którym mowa w ppkt c, administrator za pośrednictwem WOP przeprowadza, nie rzadziej niż raz na 3 miesiące, pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
   e. Niedopuszczalne jest wyłączanie lub zmiana ustawień oprogramowania antywirusowego przez użytkowników.
   f. Użytkownik jest obowiązany zawiadomić administratora o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
   g. Do obowiązków administratora za pośrednictwem WOP należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
   h. Administrator za pośrednictwem WOP przeprowadza cyklicznie kontrole antywirusowe na każdym stanowisku komputerowym wykorzystywanym do przetwarzania danych, w tym na komputerach przenośnych.
   i. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym z sieci komputerowej administratora wyłącznie po uprzednim sprawdzeniu zawartości przypisanego im nośnika oprogramowaniem antywirusowym.

j. Niedopuszczalne jest otwieranie plików pobranych z Internetu lub korzystania z zewnętrznych nośników bez uprzedniego przeskanowania zawartości nośnika przez program antywirusowy.

k. Przesyłanie danych osobowych pocztą elektroniczną dopuszczalne jest tylko w postaci zaszyfrowanej.

2. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych:

a. System informatyczny umożliwia automatycznie:
   - przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu;
   - sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych);
   - sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego co najmniej:
     – datę pierwszego wprowadzenia danych do systemu administratora danych,
     – identyfikator użytkownika wprowadzającego te dane,
     – źródła danych – w przypadku zbierania danych nie od osoby, której one dotyczą,
     – informacje o odbiorcach danych, którym dane osobowe zostały udostępnione.

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

c. Rejestr uwzględniający elementy, o których mowa w pkt 2a , prowadzony jest przez administratora w formie elektronicznej lub papierowej.

d. Nadzór nad prawidłowym wprowadzaniem, przetwarzaniem i udostępnianiem danych sprawuje administrator.

e. Nadzór wykonywany jest w sposób niezapowiedziany lub zapowiedziany z jednodniowym wyprzedzeniem. Ponadto czynności kontrolne przeprowadzane są obligatoryjnie w przypadku uzasadnionego podejrzenia/ naruszenia bezpieczeństwa systemu.

f. Nadzór, o którym mowa obejmuje m.in.:
   - sprawdzenie, czy wprowadzanie, przetwarzanie oraz udostępnianie danych w systemie odbywa się z poszanowaniem obowiązujących zasad;

- sprawdzenie, czy przetwarzanie danych w systemie odbywa się z poszanowaniem niniejszych zasad;
- sprawdzanie zabezpieczeń mających na celu zapewnienie ochrony danych, w tym zabezpieczeń fizycznych, organizacyjnych oraz technicznych;
- kontrolę rejestrów;
- oględziny urządzeń służących do przetwarzania danych, m.in.: serwerów, stacji roboczych.

3. Bezpieczeństwo oprogramowania:
   a. Oprogramowanie stosowane w straży może pochodzić wyłącznie ze źródeł legalnych oraz posiadać aktualną i kompletną dokumentację użytkownika, eksploatacyjną i techniczną, a w przypadku gdy za jego pomocą przetwarzane są dane osobowe – spełniającą wymogi RODO.
   b. Instalacja i deinstalacja dokonywana jest wyłącznie przez administratora za pośrednictwem WOP.
   c. Użytkownicy obowiązani są do powstrzymania się od jakiejkolwiek ingerencji w oprogramowanie.
   d. Wszelkie oprogramowanie wykorzystywane w jednostce musi być użytkowane z poszanowaniem praw własności intelektualnej, a w szczególności zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U.1994.24.83 ze zm.).
   e. Za określanie standardów sprzętu i oprogramowania oraz zmiany w już obowiązujących odpowiada administrator. Standard sprzętu i oprogramowania powinien być zgodny z potrzebami, uwzględniać opłacalność ekonomiczną oraz wymagania w zakresie bezpieczeństwa. Sprzęt i oprogramowanie powinny być eksploatowane, serwisowane i wycofywane z eksploatacji z zachowaniem właściwych procedur bezpieczeństwa.
   f. Wszelkie działania związane z utrzymaniem i eksploatacją systemu informatycznego mogą być podejmowane wyłącznie przez upoważniony, wykwalifikowany personel lub upoważnione przez administratora osoby.
4. Przegląd i konserwacja urządzeń:
   a. Przegląd i konserwacja urządzeń systemu powinny być dokonywane zgodnie z zaleceniami producenta, lecz nie rzadziej niż raz w roku.

b. Przeglądu i konserwacji systemu dokonuje doraźnie administrator za pośrednictwem WOP, które odpowiedzialne jest za terminowość i rzetelność przeglądów i konserwacji urządzeń.
c. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) administrator za pośrednictwem WOP dokonuje nie rzadziej niż raz na kwartał.
d. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale WOP nie rzadziej niż raz w roku.
e. Zapisy logów systemowych powinny być przeglądane codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
f. Kontrole i przeprowadzane testy powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.
g. Wszelkie nieprawidłowości wykryte w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny oraz okoliczności sprzyjające ich zaistnieniu przeanalizowane. O ile to możliwe, stosuje się odpowiednie środki w celu zapobieżenia występowania nieprawidłowości w przyszłości.
h. Przegląd programów i narzędzi przeprowadzany jest w przypadku zmiany wersji oprogramowania lub zmiany systemu operacyjnego, chyba że zmiany te wynikają z aktualizacji automatycznej.

5. Naprawy urządzeń komputerowych z chronionymi danymi osobowymi:
a. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym przeprowadzane są – o ile to możliwe – przez pracowników urzędu lub podmiot zewnętrzny pod nadzorem WOP.
b. Naprawy i zmiany w systemie informatycznym przeprowadzane przez serwisanta prowadzone są pod nadzorem administratora, w tym osób przez niego upoważnionych (wyznaczonych), w siedzibie administratora – o ile to możliwe – lub poza siedzibą administratora, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
c. Jeśli nośnik danych (dysk płyta, pendrive lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć zgodnie ze wskazaniami zawartymi w niniejszej Polityce.

6. Ewidencjonowanie informacji o odbiorcach danych:
   a. Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym, w systemie powinna zostać odnotowana uwaga o udostępnieniach danych odbiorcom zawierająca informacje, komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.
   b. Szczegółowy sposób oraz formę odnotowania informacji, o których mowa w ppkt a, zawiera dokumentacja techniczna danego systemu informatycznego.
7. Cel i zasady tworzenia kopii zapasowych:
   a. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania jednostki tworzy się regularnie zgodnie z harmonogramem kopie zapasowe danych.
   b. Kopie zapasowe tworzy się wykorzystując narzędzia programowe oraz narzędzia systemu.
   c. W systemie informatycznym wykorzystującym technologię klient-serwer kopie zapasowe wykonuje się po stronie serwera.
   d. Dostęp do kopii bezpieczeństwa mają tylko administrator oraz WOP.
   e. Pozostałe kopie tworzy się na oddzielnych nośnikach informatycznych.
   f. Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/ tygodniowa/ miesięczna" wraz z podaniem daty sporządzenia.
   g. Kopie ulegają niezwłocznie zniszczeniu w sposób uniemożliwiający ich użycie, jeżeli zostanie stwierdzona ich nieprzydatność albo pojawią się okoliczności wyłączające legalność archiwizowania danych.
   h. Administrator za pośrednictwem WOP obowiązany jest do prowadzenia rejestru kopii zapasowych.
8. Procedura tworzenia kopii zapasowych.
   a. Kopie zapasowe zbiorów danych wykonywane są zgodnie z harmonogramem przez administratora za pośrednictwem WOP.
   b. Kopie zapasowe tworzy się w systemach według następującego harmonogramu:
      - codziennie – na koniec dnia tworzy się kopię wszystkich danych, które uległy zmianie tego dnia;
      - raz w tygodniu – na koniec tygodnia tworzy się kopię wszystkich aplikacji;

- raz w miesiącu – na koniec miesiąca tworzy się kopię zarówno danych, jak i aplikacji, w tym także systemu operacyjnego.

c. Administrator za pośrednictwem WOP obowiązany jest do wykonywania kopii zgodnie z harmonogramem.

d. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy co najmniej raz w tygodniu poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych.

e. Archiwizacja przeprowadzana jest automatycznie w godzinach wieczornych i nocnych, za pomocą wbudowanych w system funkcji.

f. Przed uruchomieniem archiwizacji wszystkie procesy (zadania) niewylogowanego użytkownika są usuwane z systemu, a administrator oraz WOP otrzymują informację o tym zdarzeniu.

g. Archiwizacje wykonywane są według następującego harmonogramu:

- kopie aktualnych baz danych oraz istotnych elementów systemu operacyjnego serwera są wykonywane codziennie/ raz w tygodniu/ raz w miesiącu;
- kopie baz archiwalnych są wykonywane codziennie/ raz w tygodniu/ raz w miesiącu.

Uwaga:
zasadne jest, aby kopie były przyrostowe.

9. Nośniki danych wykorzystywane do sporządzenia kopii zapasowych:

a. Kopie zapasowe baz danych są nagrywane na zewnętrzne nośniki, takie jak:

- pamięć USB,
- CD/DVD,
- zewnętrzne dyski pamięci,
- taśmy magnetyczne.

b. Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/ tygodniowa/ miesięczna" wraz z podaniem daty sporządzenia.

10. Przechowywanie kopii zapasowych.

a. Wszystkie nośniki bez względu na ich rodzaj są zabezpieczane przed nieautoryzowaną zmianą, zniszczeniem i dostępem.

b. Kopie zapasowe przechowuje się w zamykanej szafie w siedzibie administratora lub urzędu.

11. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe.
    a. Zbiory danych przechowywane są na serwerze obsługującym system informatyczny administratora. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonych każdemu użytkownikowi.
    b. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną bez uprzedniego ich zaszyfrowania.
    c. Na nośnikach, o których mowa w ppkt b, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
    d. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go za pomocą programu antywirusowego na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
    e. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów pomimo usunięcia danych i podlegają ochronie w trybie określonym w niniejszej Polityce.
    f. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.
12. Likwidacja nośników zawierających kopie.
    a. Nośniki, które uległy uszkodzeniu lub zawierają nieaktualne kopie danych powinny zostać bezzwłocznie zniszczone.
    b. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w sposób określony w niniejszej Polityce, czyli tak, by nie można było odczytać ich zawartości.
    c. Nośniki wielorazowego użytku, takie jak: dyski twarde, pendrive, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.
    d. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć w sposób określony w niniejszej Polityce.
    e. Proces niszczenia kopii powinien zostać odnotowany w rejestrze kopii zapasowych, który prowadzi WPO.

13. Bezpieczeństwo nośników informacji.
    a. Zasady ogólne:
        - Wszystkie nośniki informacji podlegają właściwej ochronie stosownie do klasyfikacji informacji, na wszystkich etapach ich używania, od momentu zapisu informacji aż do momentu ich wycofania z użycia lub fizycznego zniszczenia opisanego w niniejszej Polityce.
        - Za zapewnienie właściwej ochrony nośników informacji odpowiada ich użytkownik.
        - Osoby korzystające z nośników informacji powinny zostać w ramach szkolenia uświadomione o skali zagrożeń i zobowiązane są do zachowania należytej staranności poprzez zastosowanie obowiązujących środków organizacyjno-technicznych i prawnych opisanych w niniejszej Polityce.
        - W przypadku wycofywania z użycia nośników informacji zawierających informacje stanowiące tajemnicę na osobie, której nośnik przekazano do używania, spoczywa obowiązek wykonania procedury opisanej w niniejszej Polityce.
    b. Zasady szczegółowe:
        - Komputery przenośne należy przewozić w służbowych torbach.
        - Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu. Zakaz dotyczy także pozostawiania dokumentów, nośników danych i sprzętu bez kontroli w samochodach.
        - Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.
        - Wykorzystywanie komputerów przenośnych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.
        - W trakcie przebywania w domu niedozwolone jest udostępnianie przez użytkownika innym domownikom komputera przenośnego

należącego do administratora lub urzędu. Użytkownik powinien zachować w tajemnicy przed domownikami i innymi osobami identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym.

X. Zasady postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych

1. Nie każdy incydent jest naruszeniem danych osobowych, ale każdy incydent wymaga odnotowania, gdyż w przyszłości możemy uzyskać nowe informacje o tym incydencie umożliwiające stwierdzenie naruszenia danych osobowych. Dla przykładu zagubienie pendrive'a zawierającego zaszyfrowane dane osobowe jest incydentem, dlatego że administrator jest w stanie wykazać, iż procedury oraz informacje pozyskane od pracownika gwarantują że osoba trzecia nie odczyta zawartych danych osobowych. Aczkolwiek w przyszłości może on otrzymać informację, że hasło umożliwiające odczytanie danych również zostało utracone lub powstała nowa technika odszyfrowania danych umożliwiająca odczytanie danych osobowych i w takim przypadku będzie można stwierdzić, że incydent został zakwalifikowany jako naruszenie danych osobowych.
2. Za naruszenie bezpieczeństwa systemu informatycznego uznawany jest każdy stwierdzony fakt oraz uzasadnione podejrzenie, w szczególności zajścia zdarzeń, takich jak:
   a. nieuprawnione ujawnienie danych, udostępnienie;
   b. naruszenie hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);
   c. częściowy lub całkowity brak danych albo dostęp do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;
   d. brak dostępu do właściwej aplikacji lub zmiana zakresu wyznaczonego dostępu do zasobów serwera;
   e. wykrycie wirusa komputerowego;
   f. zauważenie elektronicznych śladów próby włamania do systemu informatycznego;
   g. znaczne spowolnienie działania systemu informatycznego;
   h. podejrzenie kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe;

i. istotna zmiana położenia sprzętu komputerowego;
j. zauważenie śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf;
k. umożliwienie dostępu do pomieszczeń lub zamykanych szaf osobom nieupoważnionym,
l. zabranie danych przez osobę nieupoważnioną;
m. uszkodzenie lub zniszczenie danych lub jakiegokolwiek elementu systemu informatycznego;
n. działanie wbrew postanowieniom niniejszej Polityki.

3. Do zachowań generujących ryzyko naruszeń zaliczyć należy w szczególności:
a. dopuszczenie do przetwarzania danych osobowych osób zatrudnionych (w tym na podstawie umów cywilnoprawnych) bez odpowiednich upoważnień i oświadczenia o zachowaniu poufności;
b. udostępnienie informacji osobie upoważnionej do przetwarzania informacji w zakresie wykraczającym poza zakres upoważnienia;
c. udostępnianie informacji osobom nieupoważnionym (np. przekazywanie do naprawy sprzętu komputerowego zawierającego dane osobowe firmie zewnętrznej bez ich bezpiecznego usunięcia lub zabezpieczenia kryptograficznego);
d. powierzanie przetwarzania danych osobowych innym podmiotom bez pisemnej umowy;
e. przetwarzanie danych bez zgody podmiotu danych;
f. pozyskiwanie informacji z nielegalnych źródeł;
g. przetwarzanie informacji niezgodne z uprawnionym celem i zakresem;
h. przetwarzanie informacji w okresie dłuższym niż uprawniony;
i. wykonanie nieuprawnionych kopii danych;
j. brak aktualnych kopii bezpieczeństwa danych;
k. niewłaściwe niszczenie nośników z danymi, pozwalające na ich odczyt osobom postronnym;
l. nieautoryzowany dostęp do informacji przez połączenie sieciowe;
m. nieautoryzowane usunięcie, modyfikacja, kopiowanie danych osobowych przez osobę uprawnioną/nieuprawnioną na nośniku elektronicznym lub papierowym;
n. nieautoryzowany dostęp do pomieszczeń, w których przetwarza się dane osobowe (np. za pomocą prywatnie dorobionych kluczy);

o. niedopełnienie obowiązku ochrony danych przez umożliwienie dostępu do danych osobom nieuprawnionym, w tym w szczególności:
- pozostawienie bez nadzoru danych (np. pozostawienie dokumentów na biurku zarówno trakcie pracy, jak i po godzinach pracy);
- niezablokowanie dostępu do systemu informatycznego (np. stacji roboczej podczas przerwy w pracy);
- brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi, przebywającymi w pomieszczeniach, gdzie przetwarza się dane osobowe;
- działanie wirusów komputerowych lub innych programów naruszających integralność systemu informatycznego;
- ujawnienie indywidualnych haseł dostępu do systemu, w którym przetwarzane są dane osobowe zarówno osobie postronnej, jak i współpracownikowi;
- przesyłanie dokumentów papierowych z danymi podlegającymi ochronie bez zabezpieczenia w postaci zamkniętej koperty;
- przesyłanie nośników elektronicznych z danymi bez zabezpieczenia kryptograficznego;
- kradzież nośników zawierających dane osobowe należące lub powierzone straży;
- zgubienie nośnika zawierającego dane osobowe niezabezpieczone kryptograficznie;
- kradzież sprzętu służącego do przetwarzania danych osobowych;
- wykorzystywanie własnego nośnika danych.

4. O możliwości zaistnienia przypadku naruszenia ochrony danych osobowych może świadczyć m.in.:

a. podejrzana praca systemu teleinformatycznego, w którym przetwarza się informacje;
b. korzystanie z zasobów systemu teleinformatycznego poza godzinami pracy (bez zgody przełożonego);
c. nowe, podejrzane konta użytkowników;
d. wysoka aktywność kont, które długo pozostawały niewykorzystane;
e. odnotowanie w krótkim czasie dużej liczby nieudanych prób logowania do systemu teleinformatycznego;

f. odnotowanie udanych logowań oraz transferów danych odbiegających od standardowych, tj. np. dokonywanych spoza terytorium RP czy też poza godzinami pracy itp. anomalie;
g. anomalie w pracy systemu teleinformatycznego lub programu (świadczące np. o obecności wirusa);
h. naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których przetwarza się informacje (wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się okna itp.);
i. wszelkie zapisy w logach systemów świadczące o naruszeniu bezpieczeństwa, wykonywaniu niedozwolonych operacji itp.;
j. pozostawione ślady włamania komputerowego, np.: zmiany konfiguracji w systemie teleinformatycznym;
k. samodzielne akcje podejmowane przez system teleinformatyczny (nawiązywanie połączeń, wysyłanie e-maili itp.);
l. odkrycie (znalezienie) niezniszczonych nośników informacji prawnie chronionych (wydruk, płyta CD) w sytuacjach wskazujących na ich zagubienie lub porzucenie (np. w koszu na śmieci);
m. niewłaściwe parametry środowiska, takie jak: temperatura, wilgotność w pomieszczeniach, w których są przetwarzane dane osobowe;
n. skargi osób, których dane są przetwarzane.

5. Do zdarzeń stwarzających wyższe ryzyko naruszenia praw i wolności osoby należy zaliczyć w szczególności:
a. Zdarzenia naruszające poufność danych osobowych polegające na:
- udostępnieniu danych osobowych osobie działającej z upoważnienia administratora do przetwarzania informacji w zakresie wykraczającym poza zakres polecenia przetwarzania wydanego przez administratora lub zakres wskazany przez obowiązujący porządek prawny;
- udostępnieniu danych osobowych osobie nieuprawnionej wskutek np. wglądu w pozostające na biurku dokumenty lub otwarte okna aplikacji wizualizujących dane osobowe, przekazania danych osobowych przez telefon, pocztą elektroniczną;
- zagubieniu dokumentów zapisanych zarówno na nośniku klasycznym, jak i nośniku teleinformatycznym (w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów

realizujących zadania publiczne (Dz.U.2005.64.565 ze zm.) zawierających dane osobowe bez osłony kryptograficznej;
- włamaniu do systemu straży i kradzieży plików zawierających dane osobowe;
- udostępnieniu danych osobowych podmiotowi zewnętrznemu bez zabezpieczeń umownych zgodnie z obowiązującą Polityką;
- realizacji nieuprawnionych kopii dokumentów zawierających dane osobowe;
- realizacji korespondencji zawierającej dane osobowe pod błędny adres;
- realizacji dostępu do systemu teleinformatycznego straży przez osobę nieuprawnioną na podstawie przekazanych przez osobę uprawnioną danych uwierzytelniających;
- skopiowanie danych uwierzytelniających do oprogramowania, urządzeń służących do przetwarzania danych osobowych – poprzez ich ujawnienie osobom nieuprawnionym;
- braku realizacji obowiązków związanych z powiadamianiem odbiorców danych, o usunięciu danych, pomimo posiadania takich możliwości (w tym braku związanego z tym niewspółmiernie dużego wysiłku).

b. Zdarzenia naruszające dostępność danych osobowych polegające na:
- bezpowrotnym usunięciu danych osobowych z zasobów systemów teleinformatycznych (ze względu na brak posiadanych w tym zakresie kopii zapasowych);
- długotrwałej awarii infrastruktury teleinformatycznej (awaria serwera, bazy danych, zasilania);
- niedopełnieniu obowiązków informacyjnych podczas zbierania danych osobowych;
- braku realizacji prawa do usunięcia danych pomimo istnienia przesłanek zapewniających realizację tego uprawnienia;
- braku realizacji prawa do kopii danych osobowych, nieprzekazaniu informacji związanych z przetwarzaniem danych osobowych osobie, której dane te dotyczą (m.in. dotyczących celu i kategorii przetwarzanych danych, odbiorców danych osobowych, czasu przechowywania danych i ich źródła, jeśli były pozyskane nie od osoby, której dane dotyczą);
- braku prawa do ograniczenia przetwarzania pomimo istniejących przesłanek uprawomocniających realizację tego uprawnienia;

- braku realizacji prawa do przenoszenia danych pomimo istniejących przesłanek uprawomocniających realizację tego uprawnienia;
- braku realizacji prawa do wniesienia sprzeciwu wobec przetwarzania danych;
- braku realizacji obowiązków związanych z powiadamianiem odbiorców danych o ograniczeniu przetwarzania danych pomimo posiadania takiej możliwości (w tym braku związanego z tym niewspółmiernie dużego wysiłku).

c. Zdarzenia naruszające integralność danych osobowych polegające na:
- zaistnieniu awarii baz danych powodujących uszkodzenie, usunięcie rekordów w bazach;
- pozyskiwaniu i wykorzystywaniu danych niekompletnych, nieprawdziwych, nieaktualnych;
- braku realizacji prawa osoby, której dane dotyczą do sprostowania danych pomimo, iż administrator danych posiadł wiedzę o ich nieprawidłowości w kontekście celów, w jakich te dane są przetwarzane.
- braku realizacji obowiązków związanych z powiadamianiem odbiorców danych, o sprostowaniu danych pomimo posiadania takiej możliwości (w tym braku związanego z tym niewspółmiernie dużego wysiłku).

6. Każdy użytkownik systemu posiadający informacje o naruszeniu albo uzasadnione podejrzenie naruszenia bezpieczeństwa systemu informatycznego obowiązany jest bezzwłocznie poinformować o danym fakcie administratora, WOP lub IOD.

7. Użytkownik do czasu przybycia na miejsce administratora, WOP lub IOD podejmuje tylko takie czynności, które zmierzają do:

a. zabezpieczenia śladów naruszenia,
b. zapobieżenia dalszym zagrożeniom,
c. powstrzymania skutków naruszenia,
d. ustalenia przyczyny i sprawcy naruszenia ochrony,
e. rozważenia wstrzymania bieżącej pracy w celu zabezpieczenia miejsca zdarzenia,
f. przygotowania opisu zdarzenia.

8. Użytkownik nie opuszcza bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia administratora lub osoby przez niego wskazanej.

9. Administrator po otrzymaniu zawiadomienia o naruszeniu bezpieczeństwa systemu informatycznego obowiązany jest niezwłocznie:
   a. powiadomić IOD i WOP,
   b. przeprowadzić postępowanie wyjaśniające w celu ustalenia:
      • czy doszło do naruszenia ochrony danych osobowych,
      • okoliczności naruszenia ochrony danych osobowych,
   c. podjąć działania chroniące system przed ponownym naruszeniem.
10. W każdym przypadku stwierdzenia naruszenia bezpieczeństwa systemu administrator obowiązany jest:
   a. odnotować ten fakt w Rejestrze naruszeń/ podejrzeń naruszeń ochrony danych osobowych, który obowiązany jest prowadzić (zob. załącznik nr 10). Rejestr może być prowadzony w formie elektronicznej zapewniającej rozliczalność.
   b. sporządzić Raport z oceny naruszenia/ podejrzeń naruszenia ochrony danych osobowych zgodnie ze wzorem zawartym w załączniku do niniejszej Polityki (zob. załącznik nr 11).
   c. otrzymać od IOD Raport z oceny naruszenia/ podejrzeń naruszenia (zob. załącznik nr 11).
   d. dokonać analizy, czy wystąpienie naruszeń powoduje wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą.
11. Wynik analizy wskazujący na istnienie ryzyka na poziomie wyższym niż niskie powoduje konieczność zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki nie później jednak niż do 72 h od stwierdzenia naruszenia. Analizę przeprowadza administrator przy udziale IOD i WOP. Przekroczenie wskazanego terminu rodzi konieczność informowania w zgłoszeniu o przyczynie opóźnienia. Zgłoszenie naruszenia musi zawierać w minimalnym zakresie:
   a. informacje o charakterze naruszenia, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. imię i nazwisko IOD oraz jego dane kontaktowe lub oznaczenie innego punktu kontaktowego, dającego możliwość uzyskania więcej informacji;
   c. informacje o możliwych konsekwencjach naruszenia ochrony danych osobowych;

d. informacje o zastosowanych lub proponowanych przez administratora środkach w celu zaradzenia naruszeniu ochrony danych osobowych, w tym o środkach służących zminimalizowaniu jego ewentualnych negatywnych skutków.

12. Wynik analizy wskazujący na istnienie wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą powoduje dodatkowo konieczność poinformowania jej o tym naruszeniu, przy tym należy sformułować ten komunikat w zrozumiały i prosty sposób.

13. Zawiadomienie osoby, której prawa lub wolności zostały naruszone, musi jako minimum zawierać opis charakteru naruszenia oraz:

a. imię i nazwisko IOD oraz jego dane kontaktowe lub oznaczenie innego punktu kontaktowego, dającego możliwość uzyskania więcej informacji;
b. informacje o możliwych konsekwencjach naruszenia ochrony danych osobowych;
c. informacje o zastosowanych lub proponowanych przez administratora środkach w celu zaradzenia naruszeniu ochrony danych osobowych, w tym o środkach służących zminimalizowaniu jego ewentualnych negatywnych skutków.

14. Administrator może odstąpić od powiadomienia osoby, której dane dotyczą o naruszeniu w sytuacji, gdy:

a. wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczyło naruszenie, (np. szyfrowanie);
b. zastosował w ramach działań korygujących środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą (zastosowanie strategii redukcji ryzyka);
c. wymagałoby ono niewspółmiernie dużego wysiłku, a dotarcie do poszkodowanych osób będzie realizowane na podstawie publicznego komunikatu lub środka równoważnego, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób;
d. wskazuje na to przeprowadzona ocena ryzyka, którą to ocenę każdorazowo obowiązany jest przeprowadzić komendant przy udziale IOD.

15. Komendant obowiązany jest prowadzić rejestr naruszeń ochrony danych, w którym odnotowuje wszystkie naruszenia ochrony danych niezależnie od wagi szkód, które mogą nastąpić w wyniku jego wystąpienia.

16. Administrator może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętego zdarzeniem od pozostałej jego części.
17. W razie odtwarzania danych z kopii zapasowych administrator obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem zdarzenia (dotyczy to zwłaszcza przypadków infekcji wirusowej).
18. Administrator podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

ZAŁĄCZNIKI
Załącznik nr 10. Wzór Rejestru naruszeń/ podejrzeń naruszeń ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 11. Wzór Raportu IOD z ceny naruszenia/ podejrzenia naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

XI. Zgłaszanie naruszeń

1. W przypadku wystąpienia niezbędności zgłoszenia do Prezesa UODO naruszenia ochrony danych osobowych administrator obowiązany jest zgłosić ujawnione naruszenie za pośrednictwem dedykowanej strony WWW: https://www.biznes.gov.pl/pl/usluga/889 lub https://uodo.gov.pl/pl/134/233.
2. Administrator dokonuje zgłoszenia i przekazuje informacje w zakresie określonym w Formularzu zgłoszenia naruszenia ochrony danych osobowych (zob. załącznik nr 12).
3. Zgłoszenia należy dokonać niezwłocznie, lecz nie później niż w ciągu 72 h od uzyskania informacji o naruszeniu.
4. Decyzję o klasyfikacji zagrożenia komendant podejmuje w konsultacji z IOD i WOP.
5. Decyzję o zgłoszeniu lub niezgłoszeniu zagrożenia podejmuje komendant.
6. Podmiot przetwarzający obowiązany jest poinformować administratora o podejrzeniu wystąpienia naruszenia nie później niż 24 h od uzyskania informacji.

Załącznik nr 12. Wzór Formularza zgłoszenia naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

XII. Zasady obsługi praw jednostki i udostępnień danych

1. W przypadku wystąpienia incydentów, w ramach których może dojść do naruszenia praw i wolności osób, których dane dotyczą, administrator wraz z IOD oraz WOP niezwłocznie:
   a. ustala i podejmuje działania skoncentrowane na ochronie tych osób przed negatywnymi skutkami naruszeń;
   b. informuje osoby o zaistniałym zdarzeniu za pośrednictwem dostępnych kanałów przekazu oraz o przysługujących im prawach, o ile taka niezbędność wystąpi.
2. Udostępnianie informacji dotyczących przetwarzania.
   a. Administrator obowiązany jest do udostępnienia publicznie informacji w następującym zakresie:
      - nazwa, siedziba i dane kontaktowe administratora;
      - dane kontaktowe IOD;
      - cele, do których ma posłużyć przetwarzanie danych;
      - informacje o prawie wniesienia skargi do odpowiedniego organu nadzorczego wraz z jego danymi kontaktowymi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych;
      - informacje o prawach przysługujących osobie, której dane dotyczą;
   b. Administrator jest zobowiązany udostępnić na stronie WWW urzędu, BIPie lub w siedzibie straży wzór Klauzuli informacyjnej (zob. załącznik nr 13).
3. Przekazywanie informacji dotyczących przetwarzania.
   a. Administrator obowiązany jest do przekazywania dodatkowych informacji, poza wskazanymi w pkt 2a osobie, której dane dotyczą w następującym zakresie:
      - podstawa prawna przetwarzania;
      - okres przechowywania danych osobowych lub – gdy nie jest to możliwe – kryteria służące określaniu tego okresu;
      - informacje o odbiorcach lub kategoriach odbiorców, którym dane zostały ujawnione.

4. Udzielanie informacji dotyczących przetwarzania na wniosek osoby, której dane dotyczą:
   a. Administrator obowiązany jest do przekazania na wniosek informacji osoby, której dane dotyczą w następującym zakresie:
      - cel i podstawa prawna przetwarzania danych;
      - kategorie danych osobowych i danych, które są przetwarzane;
      - odbiorcy lub kategorie odbiorców, którym dane osobowe zostały ujawnione;
      - okres przechowywania danych lub kryteria służące określeniu tego celu, o ile określenie okresu przechowywania danych nie jest możliwe;
      - możliwości wniesienia wniosku do administratora o sprostowanie lub usunięcie danych osobowych, lub ograniczenie przetwarzania danych osobowych dotyczących tej osoby;
      - prawa wniesienia skargi do Prezesa UODO lub innego organu nadzorczego sprawującego nadzór na podstawie odrębnych przepisów osobowych wraz z jego danymi kontaktowymi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych.

5. Obowiązek informacyjny ma za zadanie zapewnić możliwość kontaktu z administratorem/ IOD, z przyczyn technicznych, np. realizowanie kontroli z wykorzystaniem urządzeń technicznych rejestrujących dane, nie wyklucza przekazania klauzuli w formie papierowej czy elektronicznej, dopuszczalne jest stosowanie komunikatów głosowych informujących o nazwie i danych kontaktowych administratora oraz poinformowanie, gdzie informowany może odnaleźć pełną treść klauzuli informacyjnej.
6. Realizacja prawa dostępu do danych.
   a. Każdej osobie, której dane dotyczą, przysługuje prawo dostępu do jej danych osobowych.
   b. Osobie, której dane dotyczą prawo, o którym mowa w ppkt a przysługuje po złożeniu wniosku.
   c. Administrator obowiązany jest do:
      - przyjęcia wniosku;
      - rozpatrzenia wniosku;
      - udostępnienia lub przekazania kopii danych albo sporządzonych wyciągów z tych danych, o ile nie wystąpią przesłanki uzasadniające odmowę;

- poinformowania osoby, której dane dotyczą, o przyczynach odmowy lub ograniczeniu dostępu oraz o możliwości wniesienia skargi do Prezesa UODO;
- udokumentowania prawnych i faktycznych przesłanek odmowy, a także dokonania weryfikacji wniosku pod kątem jego autentyczności.

7. Odmowa realizacji prawa dostępu do danych osobowych:
   a. Każda osoba, która wniosła o udostępnienie jej danych osobowych, a jej prawo do udostępnienia danych osobowych nie zostało zrealizowane z uwagi na odmowę lub ograniczenie dostępu do danych, musi zostać pisemnie poinformowana przez administratora o przyczynach faktycznych i prawnych tej decyzji.
8. Realizacja wniosku o sprostowanie lub usunięcie danych:
   a. Administrator jest zobowiązany do realizacji wniosków, bez zbędnej zwłoki, lecz w terminie nieprzekraczającym miesiąca, z zakresu:
      - prawa żądania uzupełnienia danych;
      - prawa do uaktualnienia danych;
      - prawa do sprostowania danych;
      - prawa do żądania usunięcia danych.
9. Ograniczenie czasowe przetwarzania danych.
   a. W przypadku uznania przez administratora wniosku o czasowe ograniczenie przetwarzania danych w określonym zakresie jest on obowiązany do nieudostępniania ich odbiorcom przez czas trwania ograniczenia.
   b. Obowiązek wskazany w ppkt a dotyczy także współadministrującego danymi.
10. Zakaz udostępniania danych w razie zagrożenia życia lub zdrowia.
    a. Administrator nie może przekazywać informacji lub udostępniać danych osobowych, jeżeli ich zakres może skutkować:
       - utrudnieniem lub uniemożliwieniem rozpoznania:
         – czynów zabronionych,
         – wykrywania lub zwalczania czynów zabronionych;
       - utrudnieniem prowadzenia postępowania wyjaśniającego, karnego;
       - wystąpieniem zagrożenia:
         – życia lub zdrowia ludzkiego,
         – bezpieczeństwa i porządku publicznego;

- zagrożeniem bezpieczeństwa narodowego;
- istotnym naruszeniem dóbr osobistych innych osób.

11. Dane zgromadzone w postępowaniach na podstawie ustaw oraz innych aktów normatywnych.
    a. Prawa osób, których dane są zgromadzone i przetwarzane przez administratora w związku z realizacją postępowań określonych przez akty normatywne wymienione w ppkt b mogą być realizowane wyłącznie na podstawie i w zakresie przewidzianym w tych aktach.
    b. Do postępowań tego rodzaju zaliczyć należy:
        - postępowanie w sprawach o wykroczenia prowadzone na podstawie przepisów ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U.2001.106.1148 ze zm.);
        - postępowanie karne prowadzone na podstawie przepisów ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U.1997.88.555 ze zm.);
        - postępowanie wykonawcze prowadzone na podstawie przepisów ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz.U.1997.90. 557 ze zm.);
        - postępowanie karnoskarbowe prowadzone na podstawie przepisów ustawy z dnia z dnia 10 września 1999 r. Kodeks karny skarbowy (Dz.U.1999.83.930 ze zm.);
        - postępowanie w sprawach nieletnich prowadzone na podstawie przepisów ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz.U.1982.35.228 ze zm.);
        - postępowanie wobec osób z zaburzeniami psychicznymi prowadzone na podstawie przepisów ustawy z dnia z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U.1994.111.535 ze zm.).

12. Zakres danych wymaganych we wniosku.
    a. Wnioskodawca występując z wnioskiem o realizację przysługujących mu praw, obowiązany jest do podania danych, takich jak:
        - imię,
        - nazwisko,
        - adres korespondencyjny, którym może być również adres poczty elektronicznej.

b. Przekroczenie wskazanego w ppkt a zakresu danych wymaga wykazania w szczególności niezbędności jego rozszerzenia.

13. Pouczenie o możliwości wniesienia skargi do Prezesa UODO.
   a. Administrator obowiązany jest pouczyć wnioskującego o prawie wniesienia skargi do Prezesa UODO w przypadkach, o których mowa w pkt 9.
14. Komunikacja administratora z osobą zainteresowaną:
   a. Komunikacja prowadzona z administratorem przez osobę, której dane dotyczą, a także osobę zainteresowaną, w każdej sprawie musi charakteryzować się tym, że:
      • nie może być odpłatna;
      • może być prowadzona z wykorzystaniem wszystkich dostępnych i bezpiecznych środków przekazu;
      • musi być prowadzona za pomocą prostego i jasnego języka, zrozumiałego i dostosowanego do poziomu percepcji odbiorcy.
   b. Od zasady wyrażonej w ppkt a wyjątek stanowią następujące sytuacje:
      • wniesienie przez osobę, której dane dotyczą, nieuzasadnionego żądania;
      • ujawnienie przez administratora nadmierności żądań.
   c. W przypadku ziszczenia się przesłanek wskazanych w ppkt b administrator może naliczyć opłatę, której wysokość winna być ustalona na podstawie rzeczywistych kosztów obsługi żądania. Administrator obowiązany jest dokonać realizacji żądania w ciągu 14 dni liczonych od momentu uiszczenia opłaty.
15. Administrator obowiązany jest prowadzić Rejestr udostępnień danych i informacji, w którym odnotowuje wszystkie udostępnienia (zob. załącznik nr 14).

ZAŁĄCZNIKI

Załącznik nr 13 . Wzór przykładowej Klauzuli informacyjnej dla Straży Gminnej (Miejskiej) w [...].

Załącznik nr 14. Wzór Rejestru udostępnień danych i informacji w Straży Gminnej (Miejskiej) w [...].

XIII. Metodyka oceny ryzyka stopnia naruszenia[6]

1. Administrator przy udziale IOD i WOP ma obowiązek przeprowadzić dla każdego odnotowanego w prowadzonym Rejestrze naruszeń ochrony danych osobowych ocenę określnego ryzyka stopnia naruszenia zgodnie z metodyką zawartą w niniejszej Polityce.
2. Administrator uzyskane wyniki oceny wagi naruszenia dokumentuje w Raporcie oceny naruszenia ochrony danych osobowych, który dołącza się do Rejestru naruszeń ochrony danych osobowych.
3. Decyzję o klasyfikacji wagi naruszenia podejmuje komendant po konsultacji z IOD i WOP.
4. Do kategorii szkód, które mogą wystąpić w następstwie naruszenia zasad ochrony danych zaliczyć należy w szczególności:
   a. nieuprawnioną modyfikację danych;
   b. kradzież tożsamości;
   c. oszustwo w następstwie kradzieży tożsamości;
   d. straty finansowe;
   e. naruszenie dobrego imienia oraz innych dóbr osobistych;
   f. stygmatyzację;
   g. dyskryminację.
5. Metodyka analizy naruszeń.

Wzór na ocenę ryzyka stopnia naruszenia:

W = K x P + O, gdzie K = A + B

W = (A + B) x P + O

- Kryteria oceny ryzyka stopnia naruszenia:

K (K = A + B) – kontekst przetwarzania danych, przy czym:
A – rodzaj i poziom wrażliwości danych (zob. tabela 1),
B – poziom wrażliwości kontekstu przetwarzania danych (zob. tabela 2);
P – prawdopodobieństwo identyfikacji osoby, której dane dotyczą (zob. tabela 3);
O – okoliczności naruszenia (zob. tabela 4, tabela 5, tabela 6, tabela 7).

[6] Metodyka oparta na modelach opianych w wykorzystanej literaturze.

Tabela 1. Zmienne oceny ryzyka stopnia naruszenia dla rodzaju i poziomu wrażliwości danych (A)

Lp.	Zmienna	Wartość zmiennej	Uwagi
1.	Dane podstawowe/zwykłe	1	
2.	Dane identyfikujące zachowania	2	
3.	Dane o naruszeniach prawa	3	
4.	Dane wrażliwe	4	
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 2. Zmienne oceny ryzyka stopnia naruszenia dla poziomu wrażliwości kontekstu przetwarzania danych (B)

Lp.	Zmienna	Wartość zmiennej	Uwagi
1.	Szeroki zakres danych	+1 lub -1	
2.	Charakter danych	+1 lub -1	
3.	Wielkość gminy	+1 lub -1	
4.	Negatywne skutki dla podmiotu danych	+1 lub -1	
5.	Publiczny dostęp do danych	+1 lub -1	
6.	Aktualność danych	+1 lub -1	
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 3. Poziom prawdopodobieństwa identyfikacji osoby, której dane dotyczą (P):

Lp.	Prawdopodobieństwo	Poziom (wartość)	Uwagi
1.	Znikome	0,25	
2.	Ograniczone	0,5	
3.	Wysokie	0,75	
4.	Realne	1	
Przyjęty poziom:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 4. Zmienne poziomu okoliczności naruszenia poufności – dane zostały ujawnione (O)

Lp.	Zmienna	Wartość zmiennej	Uwagi
1.	Dane w posiadaniu znanych odbiorców	0,25	
2.	Dane w posiadaniu nieznanych odbiorców	0,5	
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 5. Zmienne poziomu naruszenia integralności danych (O)

Lp.	Zmienna	Wartość zmiennej	Uwagi
1.	Istnieje możliwość przywrócenia/ odzyskania danych	0,25	
2.	Nie istnieje możliwość przywrócenia/ odzyskania danych	0,5	
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 6. Zmienne poziomu naruszenia dostępności danych – brak dostępu do danych (O)

Lp.	Zmienna	Wartość zmiennej	Uwagi
1.	Czasowy brak dostępu do danych	0,25	
2.	Stały brak dostępu do danych, w tym brak możliwości ich odzyskania	0,5	
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 7. Zmienne dotyczące charakteru działań naruszających bezpieczeństwo danych (O)

Lp.	Zmienna	Wartość zmiennej	Uwagi
1.	Działanie nieświadome	0,25	
2.	Działanie świadome	0,5	
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Uzyskane wyniki (W = (A+B) x P + O) wskazują na działania, które na ich podstawie powinien podjąć komendant (zob. tabela 8).

Tabela 8. Wyniki i wskazania do dalszych działań, które winien podjąć komendant

Uzyskany wynik (W = (A + B)x P + Q)	Waga naruszenia	Dokonać zgłoszenia do Prezesa UODO	Zlecić kompleksowy przegląd/audyt	Zawiadomić osobę, której dane dotyczą	Ujawnić w rejestrze naruszeń	Podjąć działania	
						Zaradcze	Naprawcze
Do 2	Niska	NIE	NIE	NIE	TAK	TAK	NIE
w przedziale od 2 do 3	Średnia	NIE	TAK	NIE	TAK	TAK	TAK
w przedziale od 3 do 4	Wysoka	NIE	TAK	NIE	TAK	TAK	TAK
od 4	Bardzo wysoka	TAK	TAK	TAK	TAK	TAK	TAK

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

ZAŁĄCZNIKI
Załącznik nr 15. Wzór Raportu z oceny ryzyka stopnia (wagi) naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

XIV. Metodyka oceny ryzyka

1. Przetwarzanie danych osobowych możliwe jest jedynie ma poziomie niskiego ryzyka co oznacza, że jeśli ryzyko jest na poziomie wysokim, to konieczne jest zastosowanie takich rozwiązań organizacyjno-technicznych, aby znacząco zmniejszyć poziom ryzyk lub zaprzestać przetwarzania danych osobowych.
2. Decyzję o klasyfikacji ryzyk podejmuje komendant w konsultacji z IOD i WOP.
3. Dla potrzeb metodyki przyjmuje się, że ryzyko przetwarzania danych osobowych ma trzy wymiary, i należy je rozpatrywać jednocześnie jako:
   a. ryzyko naruszenia poufności,
   b. ryzyko naruszenia integralności,
   c. ryzyko niedostępności do danych.
4. Dla potrzeb ustalenia poziomu występujących ryzyk przyjmuje się następujące czynniki:
   a. liczebność gminy (miasta);
   b. kategoria danych;
   c. skala przetwarzanych danych;
   d. rodzaj nośnika danych;
   e. możliwość nałożenia kary;
   f. możliwość wystąpienia roszczeń cywilnych;
   g. możliwość wszczęcia postępowania karnego.

I. Ustalanie poziomu poszczególnych wymiarów ryzyka przetwarzania danych osobowych (zob. tabela 1, tabela 2, tabela 3).

Tabela 1. Ryzyko utraty poufności danych osobowych – ustalenie poziomu

Poufność	Skutki naruszenia		
Ryzyko naruszenia	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 2. Ryzyko utraty integralności danych osobowych – ustalenie poziomu

Integralność	Skutki naruszenia		
Ryzyko naruszenia	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 3. Ryzyko utraty dostępności do danych osobowych – ustalenie poziomu

Dostępność	Skutki naruszenia		
Ryzyko naruszenia	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

II. Ustalenie poziomu ryzyka ze względu na przyjęte do analizy czynniki, tj. liczebność gminy (zob. tabela 4), kategoria danych, w tym: danych podstawowych (zob. tabela 5), danych o naruszeniach prawa (zob. tabela 6), danych wrażliwych (zob. tabela 7); skala przetwarzania danych (zob. tabela 8); rodzaj nośnika danych, w tym: nośniki tradycyjne (zob. tabela 9), nośniki elektroniczne (zob. tabela 10); możliwość nałożenia kary (zob. tabela 11); możliwość roszczeń cywilnych (zob. tabela 12); możliwość wszczęcia postępowania karnego (zob. tabela 13).

Tabela 4. Ryzyko liczebności gminy (miasta) – ustalenie poziomu

Przypisany poziom ryzyka	Niskie	Średnie	Wysokie
	1	2	3
Liczba mieszkańców gminy (miasta)	powyżej 100 tys. osób	w przedziale od powyżej 10 tys. do 999 tys. osób	poniżej 10 tys. osób
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 5. Ryzyko kategorii danych podstawowych – ustalenie poziomu

Dane podstawowe	Skutki naruszenia		
Ryzyko naruszenia	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 6. Ryzyko kategorii danych o naruszeniach prawa – ustalenie poziomu

Dane o naruszeniach prawa	Skutki naruszenia		
Ryzyko naruszenia	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 7. Ryzyko kategorii danych wrażliwych – ustalenie poziomu

Dane wrażliwe	Skutki naruszenia		
Ryzyko naruszenia	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 8. Ryzyko skali przetwarzania danych osobowych – ustalenie poziomu

Liczba osób upoważnionych do przetwarzania danych osobowych	Ryzyko naruszenia	Liczba posiadanych rekordów danych osobowych		
		do 10 tys. osób	w przedziale od powyżej 10 tys. do 50 tys. osób	poniżej 50 tys. osób
		Niskie	Średnie	Wysokie
		Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
do 4	Niskie	1	2	3
	Przypisana wartość 1			
od 5 do 20	Średnie	2	4	6
	Przypisana wartość 2			
powyżej 20	Wysokie	3	6	9
	Przypisana wartość 3			
Przyjęta wartość:				
Uzasadnienie:				

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 9. Ryzyko tradycyjnych/elektronicznych nośników danych osobowych – ustalenie poziomu

Nośnik tradycyjny	Skutki utraty danych		
Ryzyko utraty	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niska Przypisana wartość 1	1	2	3
Średnia Przypisana wartość 2	2	4	6
Wysoka Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 10. Ryzyko tradycyjnych/elektronicznych nośników danych osobowych – ustalenie poziomu

Nośnik elektroniczny	Skutki utraty		
Ryzyko utraty	Niskie	Średnie	Wysokie
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niska Przypisana wartość 1	1	2	3
Średnia Przypisana wartość 2	2	4	6
Wysoka Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 11. Ryzyko nałożenia kary – ustalenie poziomu

Ryzyko nałożenia kary	Możliwość nałożenia kary		
	Niska	Średnia	Wysoka
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 12. Ryzyko roszczeń cywilnych – ustalenie poziomu

Ryzyko roszczeń	Możliwość roszczeń		
	Niska	Średnia	Wysoka
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Tabela 13. Ryzyko wszczęcia postępowania karnego – ustalenie poziomu

Ryzyko wszczęcia	Możliwość wszczęcia		
	Niska	Średnia	Wysoka
	Przypisana wartość 1	Przypisana wartość 2	Przypisana wartość 3
Niskie Przypisana wartość 1	1	2	3
Średnie Przypisana wartość 2	2	4	6
Wysokie Przypisana wartość 3	3	6	9
Przyjęta wartość:			
Uzasadnienie:			

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Na podstawie otrzymanych wyników ustala się określone działania (zob. tabela 14).

Tabela 14. Interpretacja wyników

Przypisana wartość oceny	Przypisany poziom ryzyka		Wymagane postępowanie z ryzykiem
do 3	Niski	Poziom ryzyka akceptowalny	Działania mitygujące muszą zostać podjęte w ustalonym czasie przy uwzględnieniu wymagań własnych i prawnych
od 4 do 6	Średni	Poziom ryzyka akceptowalny, lecz wymagający utrzymania wzmożonej ostrożności.	Obowiązek podjęcia działań mitygujących bez zbędnej zwłoki
od 7	Wysoki	Poziom ryzyka nieakceptowalny	Obowiązek podjęcia natychmiastowych działań mitygujących

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

Interpretacja wyników zawartych w raporcie (zob. tabela 15).

Tabela 15. Interpretacja uzyskanych wyników

Przypisana wartość oceny	Przypisany poziom ryzyka		Wymagane postępowanie z ryzykiem
do 26	Niski	Poziom ryzyka akceptowalny	Działania mitygujące muszą zostać podjęte w ustalonym czasie przy uwzględnieniu wymagań własnych i prawnych
od 27 do 77	Średni	Poziom ryzyka akceptowalny, lecz wymagający utrzymania wzmożonej ostrożności.	Obowiązek podjęcia działań mitygujących bez zbędnej zwłoki
od 78	Wysoki	Poziom ryzyka nieakceptowalny	Obowiązek podjęcia natychmiastowych działań mitygujących

Źródło: opracowanie własne na podstawie wykorzystanej literatury.

ZAŁĄCZNIKI

Załącznik nr 16. Wzór Raportu z oceny ryzyka naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

XV. Plan ciągłości działania

1. Administrator obowiązany jest do:
   a. pseudonimizacji i szyfrowania danych osobowych;
   b. utrzymania stałej zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c. utrzymania stałej zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie wystąpienia incydentu fizycznego lub technicznego;
   d. regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Plan ciągłości działania winien wskazywać w szczególności:
   a. procesy krytyczne, czyli procesy których niedostępność będzie miała wpływ na poprawne funkcjonowanie straży;

b. właścicieli procesów krytycznych;
c. zasoby ludzkie oraz techniczne, którym należy zapewnić ciągłość działania;
d. zasoby finansowe, które zagwarantują zaplanowane działania;
e. dostawców usług krytycznych wraz z danymi kontaktowymi;
f. maksymalne czasy reakcji i niedostępności aktywów i zasobów dla dostawców usług;
g. umowy z dostawcami usług krytycznych – SLA.

3. Z planem ciągłości działania powinien zapoznać się każdy strażnik zaangażowany w jego realizację.
4. Obowiązujący w urzędzie plan ciągłości działania dotyczy bezpieczeństwa wszystkich zasobów informacyjnych, technicznych i ludzkich, a także wszystkich przydzielonych straży aktywów .
5. Administrator obowiązany jest prowadzić przy udziale WPO oraz strażników aktywne przeglądy skuteczności obowiązującego planu ciągłości działania dla poszczególnych procesów.
6. Przeglądy winny być przeprowadzane co najmniej 2 razy w roku.
7. Pierwszy przegląd winien zostać przeprowadzony w 2021 roku.
8. Czas odtworzeniowy zasobów informacyjnych, technicznych i organizacyjnych nie może przekraczać 24 godzin.
9. Administrator obowiązany jest prowadzić rejestr zasobów krytycznych (zob. załącznik nr 17)
10. Z każdego przeglądu administrator obowiązany jest sporządzić raport z przeglądu planów ciągłości (zob. załącznik nr 17.1).
11. Administrator prowadzi rejestr przeglądów planów ciągłości działania (zob. załącznik nr 18).

ZAŁĄCZNIKI

Załącznik nr 17. Wzór Rejestru zasobów krytycznych w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 17.1. Wzór Raportu z przeglądu planów ciągłości działania w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 18. Wzór Rejestru przeglądów planów ciągłości działania w Straży Gminnej (Miejskiej) w [...].

XVI. Zasady współadministrowania danymi

1. Komendant obowiązany jest do monitorowania wszystkich występujących procesów przetwarzania danych osobowych w celu ustalenia, czy w ramach danego procesu dochodzi do współadministrowania danymi, ze szczególnym uwzględnieniem procesów zachodzących pomiędzy administratorem a urzędem. Dotyczy to w szczególności procesów, w ramach których wykorzystywane są:
   a. wspólna infrastruktura informatyczna,
   b. wspólny zasób danych osobowych.
2. Każdy proces, w ramach którego dochodzi do współadministrowania danymi osobowymi, musi zostać bezwzględnie sformalizowany a jego zakres musi zostać dookreślony w:
   a. w ramach przepisu prawa,
   b. uchwale,
   c. zarządzeniu lub,
   d. umowie (zob. załącznik nr 19).
3. Przed zawarciem umowy administrator obowiązany jest:
   a. przeprowadzić uprzednią ocenę ryzyka zwarcia umowy;
   b. dokonać oceny wdrożenia przez współadministratora odpowiednich środków technicznych i organizacyjnych.

ZAŁĄCZNIKI

Załącznik nr 19. Wzór Umowy o współadministrowaniu danymi w Straży Gminnej (Miejskiej) w [...].[7]

XVII. Zasady powierzania przetwarzania danych osobowych

1. Komendant obowiązany jest do monitorowania wszystkich występujących procesów przetwarzania danych osobowych w celu ustalenia, czy w ramach danego procesu dochodzi do powierzenia przetwarzania, ze szczególnym uwzględnieniem procesów zachodzących pomiędzy administratorem

[7] Wzór umowy o współadministrowaniu danymi powinien być każdorazowo adaptowany dla potrzeb określonego w umowie procesu.

a urzędem lub podmiotami zewnętrznymi, które dostarczają określonych usług lub produktów.

2. Każdy proces, w ramach którego dochodzi do powierzenia przetwarzania danych osobowych, musi zostać bezwzględnie sformalizowany.
3. Komendant może uregulować powierzenie przetwarzania danych:
   a. w ramach zawartej umowy (zob. załącznik nr 20),
   b. wykorzystując inne instrumenty prawne, do których zaliczyć należy uchwały rady gminy lub zarządzenia wójta.
4. Przed zawarciem umowy administrator obowiązany jest:
   a. przeprowadzić uprzednią ocenę ryzyka zwarcia umowy;
   b. dokonać oceny wdrożenia przez podmiot przetwarzający odpowiednich środków technicznych i organizacyjnych.

ZAŁĄCZNIKI

Załącznik nr 20. Wzór Umowy powierzenia przetwarzania danych w Straży Gminnej (Miejskiej) w [...].[8]

XVIII. Wykaz kategorii czynności przetwarzania, za które odpowiada administrator oraz wykaz kategorii przetwarzania danych dokonywanych w imieniu administratora

1. Komendant obowiązany jest do prowadzenia wykazu kategorii czynności przetwarzania (wkcp), który winien być traktowany przez administratora jako narzędzie pozwalające:
   a. usystematyzować realizowane czynności przetwarzania;
   b. dokonać przeglądu czynności przetwarzania pod kątem zgodności z:
      • celami przetwarzania danych osobowych,
      • wymaganiami prawnymi.
2. Wykaz prowadzi komendant (zob. załącznik nr 21).
3. Wykaz może zostać udostępniony przez administratora:

[8] Wzór umowy powierzenia przetwarzania danych osobowych, powinien być każdorazowo adaptowany dla potrzeb określonego w umowie procesu.

a. Prezesowi UODO na jego żądanie;
b. IOD.

4. Wykaz może być prowadzony w formie elektronicznej zapewniającej rozliczalność.

ZAŁĄCZNIKI
Załącznik nr 21. Wzór Wykazu kategorii czynności przetwarzania danych, za które odpowiada komendant Straży Gminnej (Miejskiej) w [...].

Załącznik nr 22. Wzór Wykazu kategorii przetwarzania danych w imieniu komendanta Straży Gminnej (Miejskiej) w [...].

XIX. Zasady niszczenia nośników danych osobowych

1. Przepis art. 40 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) nakłada na komendanta następujące obowiązki i zakazy:
   a. obowiązek trwałego zniszczenia nośników z danymi osobowymi,
   b. zakaz ich zbywania,
   c. obowiązek sporządzania Protokołu wskazującego na sposób zniszczenia nośników z danymi osobowymi (zob. załącznik nr 23).
2. Nośniki informacji mogą być niszczone wyłącznie wówczas, gdy ich sposób zniszczenia:
   a. odpowiada co najmniej poziomowi P-3 według normy DIN 6639 – dotyczy to zarówno nośników tradycyjnych, jak i informatycznych;
   b. nastąpi wskutek ich zdegradowania w kwasie solnym;
   c. polegać będzie na rozmagnesowaniu nośnika danych – co najmniej 18000 Gatuss (Gs);
   d. polegać będzie na nadpisaniu danych osobowych przy wykorzystaniu specjalistycznych narzędzi programowych, które nadpisują dane kilkukrotnie (co najmniej trzykrotnie) zgodnie z uznaną specyfiką.
3. Nośniki mogą być niszczone wyłącznie w obecności komisji powołanej do zniszczenia nośników.

4. Nie zaleca się przekazywania nośników do zniszczenia podmiotom zewnętrznym, gdy proces niszczenia nośników nie będzie gwarantował stałego udziału w niszczeniu nośnika osobie wyznaczonej z komisji powołanej do zniszczenia nośników, którą powołuje komendant lub pisemnie upoważniona przez niego osoba.

ZAŁĄCZNIKI
Załącznik nr 23. Wzór Protokołu zniszczenia informatycznych nośników danych w Straży Gminnej (Miejskiej) w [...].

XX. Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych może być dopuszczona wyłącznie:
   a. osoba posiadająca zdolność do zapewnienia bezpieczeństwa przetwarzanych danych osobowych, czyli zdolność do zapewnienia poufności, dostępności i integralności tych danych;
   b. osoba, której nadano upoważnienie do przetwarzania danych osobowych w ramach danej kategorii czynności przetwarzania danych;
   c. osoba, która została przeszkolona w zakresie przestrzegania zasad bezpieczeństwa informacji, w tym ochrony danych osobowych oraz obowiązujących zasad przetwarzania danych w straży, a także obsługi systemów i programów występujących w procesach przetwarzania określonych kategorii danych osobowych;
   d. osoba, która zobowiązała się do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem;
   e. osoba, która złożyła oświadczenie jako osoba upoważniona do przetwarzania danych osobowych;
   f. osoba, która otrzymała imienny identyfikator w systemach informatycznych (o ile jest to niezbędne).
2. Zasady prowadzenia szkoleń – osoby uprawnione do prowadzenia szkoleń:

a. szkolenia z zakresu bezpieczeństwa informacji, w tym ochrony danych osobowych oraz obowiązujących zasad przetwarzania danych w straży, przeprowadza osobiście IOD;
b. szkolenia z zakresu obsługi systemów i programów używanych w procesach przetwarzania określonych kategorii danych osobowych przeprowadza osobiście WOP.

3. Dokumentację z odbytych szkoleń przechowuje IOD.
4. Z wnioskiem:
   a. o przeszkolenie do IOD lub WOP;
   b. o nadanie imiennego identyfikatora w systemach informatycznych do WOP na zasadach obowiązujących w urzędzie;
   c. występuje komendant.
   d. o nadanie upoważnienia do przetwarzania danych osobowych do komendanta
   e. występuje zastępca komendanta.
5. Wniosek o nadanie upoważnienia do przetwarzania do danych osobowych zatwierdzany jest przez komendanta bezpośrednio po sprawdzeniu jego poprawności i niezbędności.
6. Zatwierdzony przez komendanta wniosek o nadanie upoważnienia do przetwarzania danych osobowych w określonych kategoriach danych jest uznawany za upoważnienie do przetwarzania danych osobowych w kategoriach danych określonych we wniosku.
7. Wnioski o nadanie upoważnienia do przetwarzania danych osobowych rejestruje i zabezpiecza komendant, który prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz rejestr wniosków o nadanie upoważnień do przetwarzania danych osobowych (zob. załącznik nr 24, załącznik nr 25 i załącznik nr 26).
8. Dokumentacja może być prowadzona w formie elektronicznej.

ZAŁĄCZNIKI

Załącznik nr 24. Wzór Wniosku o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych przetwarzanych w Straży Gminnej (Miejskiej) w […].

Załącznik nr 25. Wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 26. Wzór Rejestru wniosków o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w Straży Gminnej (Miejskiej) w [...].

XXI. Zasady wyboru IOD oraz zakres jego zadań

1. Komendant na podstawie przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) obowiązany jest do wyznaczenia IOD, który musi spełniać następujące warunki:
   a. ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
   b. posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w pkt 2;
   c. nie był skazany prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.
2. Kwalifikacje IOD ocenia się na podstawie takich zmiennych, jak:
   a. okres posiadanego doświadczenia w strukturach organizacyjnych straży gminnych lub pokrewnych;
   b. okres posiadanego doświadczenia w zarządzaniu i ochronie danych osobowych;
   c. poziom wykształcenia (preferowane wykształcenie co najmniej wyższe);
   d. posiadanie odpowiedniego wykształcenia kierunkowego (preferowane kierunki: prawo, ochrona danych osobowych, bezpieczeństwo informacji, cyberbezpieczeństwo, zarządzanie bezpieczeństwem);
   e. posiadanie wyksztalcenia uzupełniającego (preferowane kierunki wykształcenia uzupełniającego: prawo, ochrona danych osobowych, bezpieczeństwo informacji, cyberbezpieczeństwo, zarządzanie bezpieczeństwem);
   f. posiadanie uprawnień (preferowane uprawnienia audytora wiodącego wg norm ISO w zakresie bezpieczeństwa informacji i zapewnienia ciągłości działania).

3. Komendant obowiązany jest powołać IDO oraz zawiadomić Prezesa UODO o jego wyznaczeniu w terminie 14 dni od dnia powołania, a także zaistnienia zmiany lub odwołania IOD, oraz udostępnić jego dane niezwłocznie po jego wyznaczeniu na swojej stronie WWW, a jeżeli nie prowadzi własnej strony internetowej w sposób ogólnie dostępny w siedzibie straży.
4. Komendant zawiadamiając Prezesa UODO o wyznaczeniu IOD w straży, podaje zarazem jego imię, nazwisko, adres poczty elektronicznej lub numer telefonu. Zawiadomienie winno zostać sporządzone w postaci elektronicznej i być opatrzone kwalifikowanym podpisem elektronicznym albo podpisem zaufanym zgodnie z wytycznymi Prezesa UODO na stronie WWW: https://uodo.gov.pl/p/zawiadomienia-prezesa-uodo-zwiazane-z-iod. Zawiadomienie może zostać dokonane przez pełnomocnika. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej.
5. IOD w zakresie prowadzonych działań podlega komendantowi.
6. Komendant zapewnia odpowiednie i niezwłoczne włączenie IOD we wszystkie sprawy dotyczące ochrony danych osobowych, które związane są z działalnością straży.
7. Komendant wspiera IOD w wypełnianiu powierzonych mu zadań, zapewniając środki, pomieszczenie lub stanowisko biurowe niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania oraz umożliwiając podnoszenie wiedzy fachowej.
8. Komendant może powierzyć IOD wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań IOD oraz nie spowoduje konfliktu interesów, przy czym odmowa wykonania innych obowiązków przez IOD nie może wpływać negatywnie na status IOD w następstwie próby powierzenia mu innych obowiązków.
9. Do zadań IOD, wyznaczonego na mocy przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), należy wyłącznie:
   a. informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) oraz innych przepisów dotyczących ochrony danych;

b. prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania;
c. monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) oraz innymi przepisami dotyczącymi ochrony danych;
d. monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem danych;
e. współpraca z Prezesem Urzędu Ochrony Danych Osobowych;
f. monitorowanie realizacji zaleceń, o których mowa w art. 38 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), oraz przedstawianie Prezesowi UODO stanu ich realizacji;
g. pełnienie funkcji punktu kontaktowego wobec Prezesa UODO w kwestiach związanych z przetwarzaniem danych, w tym z uprzednimi konsultacjami, o których mowa w art. 38 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), oraz prowadzenie z Prezesem UODO konsultacji we wszelkich innych sprawach;
h. pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących jej praw, o których mowa w rozdz. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);
i. przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), oraz monitorowanie wykonania tych zaleceń;
j. realizowanie zdań z uwzględnieniem określonego ryzyka związanego z operacjami przetwarzania danych osobowych;

k. sporządzanie i przekazywanie administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

10. Zadania, o których mowa w pkt 9 realizowane są przez IOD zgodnie z przepisami rozporządzenia Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych (Dz.U.2019.1041) oraz w sposób uwzględniający specyfikę przetwarzania danych przez straż, ryzyka związane z przetwarzaniem danych, a także w sposób umożliwiający wykazanie prowadzonych przez niego działań oraz ich zgodności z przepisami o ochronie danych osobowych. W tym też celu komendant oraz wójt obowiązani są do skutecznego informowania IOD o planowanych decyzjach i innych wydarzeniach lub uzyskanych informacjach, które mogą mieć wpływ na bezpieczeństwo i przetwarzanie danych osobowych w straży.

a. Informacje potwierdzające realizację zadań, o których mowa w pkt 1–2 przechowuje IOD i komendant, a także wójt (WOP) oraz IOD powołany na mocy przepisów RODO w zakresie, który nie wpłynie na naruszenie zasad przetwarzania danych, a tym samym na prawa osób, których dane dotyczą, a zarazem jest niezbędny do zrealizowania określonego zadania lub czynności.

b. Do zadań IOD wyznaczonego na mocy przepisów RODO należy w szczególności:

c. nadzorowanie zadań związanych z prawidłowym i bezpiecznym przetwarzaniem danych osobowych, które występują w ramach działalności urzędu miejskiego, poza procesami (zadaniami) wyszczególnionymi w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.2019.1795) z uwzględnieniem aktów wykonawczych;

d. wypełnianie zdań z uwzględnieniem określonego ryzyka związanego z operacjami przetwarzania danych osobowych;

e. współpraca straży z IOD w każdym przypadku, a w szczególności wtedy, gdy wynika ona wprost z przepisów prawa lub jest niezbędna dla zapewnienia bezpieczeństwa i prawidłowości przetwarzania danych osobowych w straży – obowiązek ten dotyczy również przypadków związanych z realizacją żądań podmiotów praw, których dane dotyczą oraz zaistniałych w wyniku wszczętych kontroli lub prowadzonych audytów;

f. nadzorowanie czynności związanych z zatrudnieniem, utrzymaniem, obsługą, w tym obsługą kadrowo-płacową a także rozwiązaniem umowy ze strażnikiem i rozliczeniem go włącznie.

11. IOD dokumentuje realizację powierzonych mu zadań zgodnie z wymaganiami określonymi w załącznikach (zob. załącznik nr 27, załącznik nr 28 i załącznik nr 29).

ZAŁĄCZNIKI

Załącznik nr 27. Wzór Miesięcznego sprawozdania z działań IOD w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 28. Wzór Rocznego sprawozdania z działań IOD w Straży Gminnej (Miejskiej) w [...].

Załącznik nr 29. Wzór Rejestru sprawozdań z działań IOD w Straży Gminnej (Miejskiej) w [...].

XXII. Arkusz oceny ryzyka procesów przetwarzania danych osobowych w zakresie wydanych przez IOD rekomendacji

1. IOD obowiązany jest do realizowania powierzonych mu zdań z uwzględnieniem określonego ryzyka związanego z operacjami przetwarzania danych osobowych.
2. Wydane przez IOD rekomendacje mają wpływ na prawidłowość realizowania operacji przetwarzania danych osobowych.
3. Od prawidłowości wydanych przez IOD rekomendacji zależy zgodność przetwarzania danych osobowych z przepisami prawa, a tym samym prawidłowość realizacji przez administratora obowiązków, o których mowa w aktach regulujących ochronę danych osobowych.
4. Wydane przez IOD rekomendacje muszą opierać się na:
   a. ustalonej,
   b. powtarzalnej

c. obiektywnej metodyce oceny ryzyka procesów przetwarzania danych, na podstawie której IOD ustali również poziom istotności ujawnionych zagrożeń, jak i ryzyka wydanej rekomendacji.

5. Wydanie przez IOD określonej rekomendacji jest możliwe wyłącznie, gdy ustalony poziom ryzyka jest niski lub średni.
6. Decyzje o klasyfikacji ryzyk podejmuje IOD.
7. Na potrzeby prawidłowości arkusza przyjmuje się, że ryzyko przetwarzania danych osobowych wymaga ustalenia zmiennych, których zakres i ważność powinny być wyznaczane procesem poddanym ocenie.
8. IOD dokonuje oceny według załączonego arkusza, mając na uwadze przyjęty poziom ryzyka zawodowego (zob. załącznik nr 30, załącznik nr 31).

ZAŁĄCZNIKI

Załącznik nr 30. Wzór Arkusza oceny ryzyka procesów przetwarzania w zakresie wydanych rekomendacji przez IOD w Straży Gminnej (Miejskiej) w […].

Załącznik nr 31. Wzór Rejestru przeprowadzonych ocen ryzyka procesów przetwarzania w zakresie wydanych rekomendacji przez IOD w Straży Gminnej (Miejskiej) w […].

XXIII. Zasady i formy podnoszenia świadomości

1. Główną formą podnoszenia świadomości są szkolenia prowadzone na terenie siedziby straży.
2. Szkolenia odbywają się nie rzadziej niż raz na kwartał z uwzględnieniem procesu rekrutacji oraz zmian w prawie.
3. Szkolenia prowadzi IOD.
4. Zakres szkoleń:
   a. część I:
      - Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U.1997.78.483 ze zm.);
      - rozporządzenie 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 95/56/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1);
- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);
- ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.2019.1795) z uwzględnieniem aktów wykonawczych;
- dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89);
- ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);
- inne akty prawne, w tym wewnętrzne regulacje:
  – .....
  – .....

b. część II:
- administrator danych osobowych;
- inspektor ochrony danych;
- zasady przetwarzania informacji, w tym danych osobowych;
- zasady ochrony informacji, w tym danych osobowych;
- typowe zaniedbania podczas przetwarzania informacji, w tym danych osobowych;
- incydenty;
- naruszenia zasad ochrony informacji, w tym danych osobowych;
- zasady postępowania w przypadku wystąpienia incydentów lub naruszeń zasad ochrony informacji, w tym danych osobowych;
- realizacja praw jednostki;

c. cześć III:
- odpowiedzialność materialna i niematerialna związana z naruszeniem zasad ochrony informacji, w tym danych osobowych;

d. cześć IV:
   - pytania osób szkolonych;

e. cześć V:
   - *case study*;

f. cześć VI:
   - egzamin ustny.

ZAŁĄCZNIKI
Załącznik nr 32. Wzór Listy obecności ze szkolenia w Straży Gminnej (Miejskiej) w […].

XXIV. Zasady prowadzenia działań z wykorzystaniem urządzeń rejestrujących

1. Straż na mocy obowiązujących przepisów:
   a. posiada prawo do realizowania powierzonych jej zadań ustawowych z wykorzystaniem środków technicznych umożliwiających obserwację i rejestrację obrazu zdarzeń w miejscach publicznych bez możliwości nagrywania dźwięku wyłącznie:
      - za pośrednictwem urządzeń rejestrujących, takich jak:
        – monitoring wizyjny,
        – fotopułapki,
        – drony wyposażone w urządzenia rejestrujące dane;
      - w celu:
        – utrwalania dowodów popełnienia przestępstwa lub wykroczenia;
        – przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych;
        – ochrony obiektów komunalnych i urządzeń użyteczności publicznej, z tym że zadania muszą być dodatkowo dookreślone co do ich zakresu i czasu, a prowadzenie obserwacji prewencyjnych przy wykorzystaniu monitoringu wizyjnego nie może stanowić samoistnej przesłanki legitymizującej takie działania;
      - o ile komendant wykaże:
        – niezbędność wspomagania powyższych działań strażników środkami technicznymi;

– spełnienie wymagań określonych, w zależności od celu przetwarzania oraz planowanych operacji i użytego urządzenia, w następujących aktach prawnych:
  · RODO;
  · ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);
  · ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);
  · ustawie z dnia 3 lipca 2002 r. - Prawo lotnicze (Dz.U.2002.130.1112 ze zm.) i aktach powiązanych – drony;
  · rozporządzeniu wykonawczym Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz.U.UE.L.2019.152.45) w zakresie ochrony danych osobowych – drony,

b. straż nie może prowadzić obserwacji osób w miejscu zamieszkania, czy też wykonywania pracy podmiotu praw, których dane dotyczą;
c. straż nie może naruszać miru domowego;
d. straż nie może ingerować w prywatność osób;
e. administratorem danych osobowych uzyskanych za pośrednictwem urządzeń rejestrujących w celach, o których mowa w ppkt a jest komendant straży.

2. Przepisy ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) ograniczają strażom prawo do przetwarzania danych osobowych zebranych bez wiedzy i zgody osoby, której dane te dotyczą dla innych celów niż te, które zostały określone w tej ustawie.
3. Komendant obowiązany jest do:
a. sformalizowania relacji zachodzących pomiędzy współadministratorem oraz podmiotem przetwarzającym dane w jego imieniu;
b. wyznaczenia ról, zakresu zadań oraz obowiązków poszczególnym współadministratorom oraz podmiotom przetwarzającym dane w jego imieniu;
c. określenia celu przetwarzania danych;

d. wykazania niezbędności działań z wykorzystaniem urządzeń rejestrujących np. obraz, inne;
e. cyklicznego potwierdzania skuteczności prowadzonych działań;
f. niezbędności rejestrowania utrwalonych zdarzeń;
g. wykazania dopuszczenia do obsługi urządzeń rejestrujących oraz fotopułapek i dronów tylko osób spełniających stawiane im wymagania;
h. rozróżniania danych na:
   - dane osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;
   - dane osób skazanych za czyn zabroniony;
   - dane osób pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;
   - dane innych osób związanych z czynem zabronionym, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania, osoby, które mogą dostarczyć informacji o czynach zabronionych lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w dwóch pierwszych podpunktach;
i. rozróżniania danych na:
   - dane mające swoje źródło w faktach;
   - dane mające swoje źródło w indywidualnych ocenach;
   - dane osobowe, o ile będzie to możliwe lub nie będzie to dalece utrudnione;
j. ewidencjonowania operacji przetwarzania danych polegających w szczególności na:
   - zbieraniu danych;
   - modyfikowaniu danych;
   - przeglądaniu danych;
   - ujawnianiu wraz z przekazywaniem danych;
   - łączeniu danych;
   - usuwaniu danych;
k. ewidencjonowania operacji przetwarzania danych w oparciu o:
   - datę i godzinę operacji;

- tożsamość osoby, która przeglądała lub ujawniła dane osobowe – w miarę możliwości;
- tożsamość odbiorców danych osobowych – w miarę możliwości;
- zasadność operacji – dla ewidencji prowadzonych w sposób niezautomatyzowany;

z tym, że:

1) ewidencje winny być przeznaczone wyłącznie:
   a. do weryfikowania zgodności przetwarzania danych z prawem;
   b. do monitorowania własnej działalności;
   c. dla zapewnienia integralności i bezpieczeństwa danych osobowych;
   d. na potrzeby prowadzonych postępowań;
2) prowadzenie rozróżnienia oraz ewidencjonowania wymagane jest od 6 lutego 2020 r., chyba że straż wykaże, iż wprowadzenie takiego zautomatyzowanego systemu informatycznego, w celu dostosowania go do wdrożonych i funkcjonujących już w straży środków technicznych i organizacyjnych, wymaga niewspółmiernego wysiłku lub nakładów. Wówczas obowiązek wprowadzenia automatycznego rozróżnienia oraz ewidencjonowania wymagany będzie dopiero od 6 maja 2023 r. Wyjątek ten nie przekłada się na obowiązek prowadzenia od 6 lutego 2020 r. przez straż rozróżnienia oraz ewidencjonowania w wersji tradycyjnej (papierowej), o ile dokonanie takiego rozróżnienia będzie możliwe lub nie będzie dalece utrudnione;

l. respekt,owania godności ludzkiej;

m. przestrzegania zasad ochrony środowiska;

n. realizowania aktywnej ochrony praw osób fizycznych gwarantowanych przez Konstytucję Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U.1997.78.483 ze zm.);

o. wprowadzenia w porozumieniu ze współadministratorem regulaminu:
   - systemu monitoringu (zob. załącznik nr 33);
   - fotopułapek,
   - dronów;

p. oznaczenia rejestratorów danych, miejsc lub stref objętych zasięgiem urządzeń rejestrujących dane, w zależności od zastosowanego urządzenia i celu przetwarzania danych, po dokonaniu oraz udokumentowaniu

oceny i oszacowania ryzyka w związku z planowanymi operacjami przetwarzania informacji, w tym danych osobowych.

ZAŁĄCZNIKI
Załącznik nr 33. Wzór Regulaminu monitoringu wizyjnego wraz z załącznikami.

XXV. Zasady prowadzenia działań z wykorzystaniem bezzałogowych statków powietrznych – dronów

1. Drony wyposażone w urządzenia umożliwiające rejestrację danych osobowych mogą być wykorzystywane przez straże tylko i wyłącznie na terenie gmin, w których zostały one powołane, a także tylko i wyłącznie w miejscach ogólnodostępnych, czyli z wyłączeniem stref objętych zasięgiem miru domowego lub innych stref geograficznych ustawowo oznaczonych oraz w szczególności pod warunkiem, że:
   a. rejestrator zainstalowany na dronie nie ma możliwości utrwalania dźwięku oraz temperatury ciała;
   b. dron będzie zaliczony co najmniej do kategorii szczególnej;
   c. dane osobowe nie będą przetwarzane poza EOG, w tym na terenie USA;
   d. dane osobowe będą chronione adekwatnie do ustalonych zagrożeń;
   e. operator systemu posiadać będzie wymagane uprawnienia i ubezpieczenie;
   f. pilot systemu posiadać będzie wymagane kwalifikacje i uprawnienia, w szczególności szkolenia z zakresu:
      • ochrony danych;
      • zapewnienia prywatności;
   g. dokonano uprzedniej analizy zagrożeń mogących wystąpić podczas operacji;
   h. zgłoszono i uzgodniono z Polską Agencją Żeglugi Powietrznej planowaną operację;
   i. przeprowadzona analiza wskazała na niezbędność wspierania działań strażników z wykorzystaniem dronów.

1. Komendant, w zależności od rodzaju operacji z wykorzystaniem dronów bądź też realizowanych procesów w straży, zobowiązany jest do przestrzegania

przepisów regulujących bezpieczeństwo informacji, w tym ochronę danych osobowych, a także wymogów określonych w przepisach rozporządzenia wykonawczego Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz.U.UE.L.2019.152.45) w zakresie ochrony danych osobowych.

2. Każda realizowana przez straż operacja z wykorzystaniem dronów wyposażonych w rejestratory danych, w szczególności w ramach realizacji zadań związanych z ochroną środowiska, niesie ze sobą ryzyko bezprawnej ingerencji w obszary objęte mirem domowym. Stanu tego nie zmienia posiadanie upoważnienia wydanego przez wójta na mocy przepisu art. 379 ust. 2 ustawy z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz.U. 2001.62.627 ze zm.). Obszary objęte mirem domowym chronione są bowiem na mocy art. 50 Konstytucji RP, a także art. 193 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.) oraz art. 23 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. 1964.16.93 ze zm.).

3. Przepisy procesowe regulowane przez art. 220 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U.1997. 88.555 ze zm.) nie dają straży jakichkolwiek uprawnień do działania w ramach posiadanych kompetencji na terenie objętym mirem domowym w godzinach 22.00–6.00 (czas ciszy nocnej) nawet w ramach uprzednio już podjętej kontroli.

4. Do obszarów zastrzeżonych (z uwagi na ochronę miru domowego) zaliczyć należy każdy teren zamieszkałej nieruchomości oznaczonej choćby małym, nawet niewidzialnym z lotu drona, oznaczeniem, jak i inne pomieszczenie lub teren, w którym przebywa lub może przebywać osoba nieprzyzwalająca na ingerencję w strefę, w której się znajduje oraz czuje się bezpiecznie. Albowiem mir domowy chroni pewną określoną przestrzeń, strefę, co do której osoba w niej przebywająca ma prawo zakładać, że bez jej wyraźnej zgody lub wiedzy, nikt, w zgodzie z obowiązującym prawem, jej nie naruszy.

5. Do obszarów nieobjętych mirem domowym zaliczyć należy niezamieszkały teren nieruchomości, obiektu lub ich części, na których prowadzona jest działalność gospodarcza.

6. Przestrzeń objęta mirem domowym rozciąga się nie tylko horyzontalnie, ale również wertykalnie nad obszarem określonej, otwartej nieruchomości, na co komendant straży, jako administrator danych, zobowiązany jest

zwrócić uwagę w ramach projektowania każdej operacji z udziałem dronów wyposażonych w rejestrator danych.

7. Planując operacje z wykorzystaniem dronów, straże zobowiązane są uwzględnić w swoich analizach skuteczność respektowania zasady proporcjonalności osadzonej w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U.1997.78.483 ze zm.), odczytywanej w niniejszej Polityce jako norma gwarancyjna, której celem jest ochrona praw i wolności każdego podmiotu przed nadmierną ingerencją będącą skutkiem działań realizowanych przez straże, a także zminimalizować ryzyko ingerencji w prywatność, czyli zaplanować lot dronem w taki sposób, aby działania prowadzone z jego wykorzystaniem nie przynosiły szkody podmiotowi danych, a możliwość gromadzenia danych o osobach wynikała bezpośrednio z ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.), czego wymaga art. 51 Konstytucji RP.

8. Każda osoba fizyczna ma prawo zakładać, że jej prywatność nie jest naruszana, a jej dane osobowe nie są przetwarzane z naruszeniem prawa. Dlatego też w przypadku podejrzenia wystąpienia naruszenia jej praw dysponuje ona uprawnieniem skutkującym możliwością:

a. uzyskania w każdym czasie informacji w zakresie określonym przez:
   - art. 15–22 i 33 RODO;
   - art. 22–30 DODO;
   - art. 6 ustawy z 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2001.112.1198 ze zm.);

b. zgłoszenia naruszenia do Prezesa UODO;

c. wniesienia wobec komendanta roszczenia o naruszenie dóbr osobistych, o których mowa w art. 23 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. 1964.16.93 ze zm.);

d. zgłoszenia przekroczenia lub niedopełnienia obowiązków do Prokuratury – w tym przypadku istotne jest to, że do zaistnienia znamion przestępstwa nie jest konieczne, aby wystąpił jakikolwiek uszczerbek w dobrach chronionych prawem, gdyż przedmiotem ochrony jest prawidłowe funkcjonowanie instytucji państwowych i samorządu terytorialnego, a także wynikający z tego ich autorytet. Stąd też źródłem naruszeń mogą być zarówno normy prawne regulujące obowiązki komendanta, jak i polecenia organów kontrolnych bądź nadzorczych lub polecenia służbowe

wydane przez wójta, o ile ich zakres mieści się w granicach posiadanych uprawnień, a niebezpieczeństwo będzie rzeczywiste i skonkretyzowane.

9. W przypadku wykazania przez komendanta, że przetwarzane przez straż dane osobowe znajdują się wyłącznie w aktach spraw lub czynności bądź urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, które prowadzone są na podstawie m.in. ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. 2001.106.1148 ze zm.), nie jest możliwe uznanie, iż zwolniony jest on z obowiązku ochrony przetwarzanych przez straż danych osobowych.

10. Wyłączenie, o którym mowa w art. 3 ust.1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) należy odnosić i odczytywać wyłącznie przez pryzmat art. 26 tej ustawy – artykuł ten ogranicza zakres dostępu do danych osobowych podmiotu praw, ale nie znosi obowiązku ich ochrony. W takich okolicznościach uprawnienia dostępowe podmiotu praw, których dane przetwarza straż regulują przepisy prawa procesowego – właściwego, z uwagi na postępowanie, w ramach którego tworzone są akta lub wykorzystane przy użyciu urządzeń ewidencyjnych. W takim przypadku podmiotom danych przysługiwać będą prawa zależnie od roli, w jakiej będą w takim postępowaniu występować.

11. Straże posiadając prawo do przetwarzania danych osobowych bez wiedzy i zgody osoby, której one dotyczą, mogą realizować je wyłącznie:

- w przypadku przetwarzania danych uzyskanych w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia;
- w przypadku przetwarzania danych z rejestrów, ewidencji i zbiorów, do których straże posiadają dostęp na podstawie odrębnych przepisów;
- w celu zidentyfikowania sprawcy naruszenia obowiązujących przepisów, czyli wyłącznie po wykazaniu podjęcia przez straż czynności dających podstawę do tego, aby określony czyn, a tym samym określone zachowanie podmiotu danych można było uznać za wykroczenie, o którym mowa w art. 1 ustawy z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U.1971.12.114 ze zm.), dlatego też przywołane prawo nie przekłada się na:

– swobodę wyznaczania celów i zakresu przetwarzania danych osobowych;

– możliwość działania straży z niejawnym wykorzystaniem dronów.

Celem działań straży z wykorzystaniem dronów nie może być bowiem przetwarzanie danych wrażliwych w zakresie:

– pochodzenia rasowego lub etnicznego;

– poglądów politycznych;

– przekonań religijnych lub filozoficznych;

– przynależności wyznaniowej;

– przynależności partyjnej lub związkowej;

– stanu zdrowia;

– kodu genetycznego;

– nałogów lub życia seksualnego,

nawet w przypadku formalnego odebrania zgody od podmiotu danych, chyba, że dane takie zostały upublicznione lub straż uzyskała do nich dostęp bez intencji przetwarzania tego rodzaju danych (np. dane zostały zarejestrowane w związku z realizacją innego celu i stanowią integralną część nagrania – a informacje objęte zakazem ujawniają kontekstowo). Jednak nawet w takich okolicznościach straż jest obwiązana wykazać niezbędność przetwarzania danych wrażliwych (oraz/lub brak możliwości natychmiastowego usunięcia).

13. Możliwość przetwarzania danych wrażliwych, pojawiającą się w sytuacji współdziałania z właściwymi podmiotami, w celu:

- ochrony życia lub zdrowia;
- interesów osoby, której dane dotyczą lub innej osoby,

należy traktować jako wyjątek od zasady zakazu ich przetwarzania i taka okoliczność nie zwalnia od wykazania niezbędności ich przetwarzania.

W ten sam sposób należy traktować wszystkie inne sytuacje, wskazane w art. 11 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.), których zaistnienie będzie potencjalnie generować możliwość pozyskania danych wrażliwych. Każdorazowo wymaga to przeprowadzenia oceny niezbędności ich przetwarzania.

14. Przetwarzanie danych osobowych zebranych z wykorzystaniem dronów po ustaniu celu głównego, określonego w ramach planowanej operacji dronem, wymusza na strażach konieczność wykazania wystąpienia

niezbędności ich dalszego przetwarzania lub realizacji obowiązku prawnego ich dalszego przetwarzania z uwzględnieniem możliwych zmiennych klasyfikujących utrwalony czyn jako czyn zabroniony, do których to zmiennych zalicza się:

a. społeczną szkodliwość czynu, której stopień uzależniony jest od uzewnętrznionego zachowania człowieka (działania lub zaniechania) będącego przejawem jego woli – stąd też brak wykazania szkodliwości czynu przekreśla byt wykroczenia;
b. bezprawność, która wiąże się z tym, że określony czyn musi być zabroniony przez ustawę obowiązującą w czasie jego popełnienia pod groźbą kary aresztu, ograniczenia wolności, grzywny do 5000 złotych lub nagany;
c. zawinienie, które wymusza niezbędność przypisania dokonania czynu zabronionego konkretnemu podmiotowi danych w określonym czasie bądź dokonania ustaleń, że możliwość braku przypisania winy konkretnemu człowiekowi w określonym czasie jest wykluczona z punktu widzenia przeciętnie roztropnego człowieka. Stąd też do katalogu tego zaliczyć należy zachowanie podmiotu danych w określonym stadium popełniania czynu z uwzględnieniem:
   - zamiaru popełnienia czynu,
   - przygotowania do popełnienia czynu,
   - usiłowania popełnienia czynu,
   - dokonania czynu,

   przy czym każda postać stadialna objęta jest karalnością tylko wówczas, gdy ustawa tak stanowi.

15. Możliwość wykonania operacji w przestrzeni powietrznej zależna jest m.in. od:

a. wykazania zgodności z celami ustawowo wskazanymi;
b. wykazania niezbędności zastosowania dronów;
c. ustalonego poziomu i zakresu występujących ryzyk w obszarze ochrony danych osobowych i zapewnienia prywatności.

16. Wykonanie operacji w przestrzeni powietrznej nie będzie dopuszczalne, gdy:

a. ujawniony zostanie zbyt wysoki poziom zagrożeń występujących w obszarze niezbędności zapewnienia ochrony danych osobowych

i prywatności, których zakresu straż nie będzie mogła skutecznie zminimalizować w ramach posiadanych aktywów i zasobów;

b. brak możliwości wykazania zgodności z celami ustawowo wskazanymi;

c. brak możliwości wykazania niezbędności zastosowania dronów w celu wspomożenia działań straży.

17. Komendant zobowiązany jest do spełnienia wszystkich wymagań prawnych z zakresu ochrony danych przetwarzanych z użyciem drona z chwilą jego wykorzystania.

18. Wartym podkreślenia jest również to, że każdy komunikat kierowany w szczególności do podmiotu praw może być kierowany także za pośrednictwem strony WWW, o ile dane medium spełniać będzie wymogi stawiane przez ustawę z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019.848).

XXVI. Zasady ochrony sygnalistów

1. Sygnalistą może zostać:

a. strażnik,

b. pracownik urzędu,

c. inna osoba, w tym świadek zdarzenia, pokrzywdzony, podejrzany, a nawet były pracownik lub kandydat na określone stanowisko pracy.

Sygnalistą może zatem zostać każda osoba, która może i chce dokonać zgłoszenia o naruszeniu prawa, i każdej z tych osób należy zapewnić szczególną ochronę jej danych osobowych w związku z dokonanym zgłoszeniem.

2. Pracodawca obowiązany jest zapewnić trzy kanały dystrybucji zgłoszeń, mając na uwadze:

a. możliwość zgłoszenia wewnętrznego, czyli dokonywanego w ramach organizacji, z którą sygnalista jest związany;

b. możliwość zgłoszenia zewnętrznego, czyli dokonywanego bezpośrednio do odpowiednich organów państwowych, przy czym sygnalista może albo najpierw dokonać zgłoszenia wewnętrznego (modelowo), albo od razu dokonać zgłoszenia zewnętrznego (i w tym przypadku nie powinien on stracić swojego statusu ani ochrony);

c. możliwość ujawnienia publicznego, czyli podania informacji na temat naruszeń prawa do wiadomości publicznej (wyjątkowo, np. wtedy, gdy sygnalista dokonał uprzednio zgłoszenia wewnętrznego i zewnętrznego albo samego zgłoszenia zewnętrznego, ale nie doczekał się odpowiedniej reakcji).

3. Pracodawca obowiązany będzie umożliwić sygnalistom dokonanie zgłoszeń i ujawnianie nieprawidłowości w bezpieczny dla nich sposób, a wśród wprowadzanych środków ochrony muszą się znaleźć m.in:

a. efektywne sposoby ochrony tożsamości sygnalisty, w tym zapewnienia jego anonimowości;

b. środki ochrony przed odwetem w ramach stosunków pracy (np. ochrona przed zwolnieniem, zawieszeniem, degradacją lub wstrzymaniem awansu, negatywną oceną wyników pracy, dyskryminacją, stosowaniem środków dyscyplinujących lub podobnych);

c. inne środki ochrony przed odwetem (np. ochrona przed szkodą, nadszarpnięciem reputacji danej osoby, zwłaszcza w mediach społecznościowych, ochrona przed utratą dochodów, ochrona przed wcześniejszym rozwiązaniem lub wypowiedzeniem umowy dotyczącej dostawy towarów lub umowy o świadczenie usług);

d. efektywne sposoby ochrony w razie naruszenia przez sygnalistę tajemnicy przedsiębiorstwa,

e. objęcie ochroną nie tylko samego sygnalisty, ale również osób mu pomagających (np. rodzina, koledzy z pracy).

f. zapewnienie skutecznych, proporcjonalnych i odstraszających sankcji wobec osób fizycznych lub prawnych utrudniających dokonywanie zgłoszeń lub dokonujących działań odwetowych wobec sygnalisty.

4. Administrator obowiązany jest nadzorować proces legislacyjny związany z implementacją dyrektywy o ochronie sygnalistów przyjętej 7 października 2019 r. przez Radę Europy, w celu opracowania i wdrożenia w wyznaczonym przez ustawodawcę czasie wymaganych procedur, gdy w następstwie implementacji zostanie wskazany jako podmiot zobowiązany do podjęcia takich działań.

5. Na dzień wydania niniejszej publikacji w zakresie postępu prac legislacyjnych w przedmiocie zagadnienia wiadomo jest jedynie to, że w:

a. zarządzeniu nr 229 Prezesa Rady Ministrów z dnia 1 grudnia 2020 r. w sprawie wyznaczenia ministra właściwego do przeprowadzenia prac legislacyjnych mający na celu implementację dyrektywy Parlamentu

Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie osób zgłaszających naruszenia prawa Unii(M.P.2020.1112) wskazano jedynie ministra właściwego do przeprowadzenia prac legislacyjnych;
natomiast w:

b. zarządzeniu nr 6 Ministra Rozwoju, Pracy i Technologii z dnia 10 grudnia 2020 r. w sprawie powołania Zespołu do spraw przygotowania regulacji w związku z implementacją dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie osób zgłaszających naruszenia prawa Unii (Urz.MRPiT.2020) wskazano jedynie członków zespołu, który składa się z przedstawicieli poszczególnych departamentów.

XXVII. Odpowiedzialność karna

Zwiększenie świadomości strażników o zakresie odpowiedzialności karnej za naruszenia prawa ma na celu zminimalizowanie ryzyka podejmowania działań z premedytacją przez strażników.

1. Obowiązek zawiadomienia o podejrzeniu popełnienia przestępstwa.

Jak stanowi art. 304 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.):

„§1. Każdy, dowiedziawszy się o popełnieniu przestępstwa ściganego z urzędu, ma społeczny obowiązek zawiadomić o tym prokuratora lub Policję.

§2. Instytucje państwowe i samorządowe, które w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten organ stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa".

Zawiadomienie może zostać dokonane zarówno bezpośrednio, jak i pośrednio przy wykorzystaniu dowolnych nośników informacji, w tym również anonimowo.

2. Niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych.

Jak stanowi art. 54 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125):

„§1. Kto przetwarza dane osobowe, o których mowa w przepisach o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
§2. Jeżeli czyn określony w ust. 1 dotyczy danych wrażliwych, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech".

3. Udaremnianie lub utrudnianie przeprowadzenia kontroli.

Jak stanowi art. 55 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125):

Kto udaremnia lub istotnie utrudnia kontrolującemu przeprowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat dwóch.

Przestępstwa z art. 54 i art. 55 cytowanej ustawy mogą zostać popełnione przez każdą świadomą i zdolną do poniesienia odpowiedzialności osobę.

4. Odpowiedzialność cywilna na podstawie RODO.

Jak stanowi art. 79 RODO:

Każda osoba ma prawo do ochrony prawnej przed sądem przeciwko administratorowi danych lub podmiotowi przetwarzającemu.

Jak stanowi art. 82 RODO:

Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO ma prawo uzyskać od administratora danych lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

5. Odpowiedzialność karna na kanwie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.)

Jak stanowi art. 107 cytowanej ustawy:

Kto przetwarza dane osobowe choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony podlega grzywnie, karze ograniczenia wolności, albo pozbawienia wolności do lat 2 (jeżeli czyn dotyczy szczególnych kategorii danych zagrożenie karą pozbawienia wolności wzrasta do lat 3).

Jak stanowi art. 108 cytowanej ustawy:

Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

6. Odpowiedzialność pracownika (dyscyplinarna) na kanwie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.).

Jak stanowi art. 58 cytowanej ustawy:

Jeżeli Prezes Urzędu, na podstawie posiadanych informacji, uzna, że doszło do naruszenia przepisów dotyczących przetwarzania danych osobowych, może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom, które dopuściły się naruszeń, i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

7. Odpowiedzialność IOD.

W zakres odpowiedzialności prawnej IOD wchodzi:

a. odpowiedzialność pracownicza za niewłaściwe wykonywanie obowiązków;
b. odpowiedzialność cywilna w związku z naruszeniem dóbr osobistych na mocy art. 24 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U.1964.16.93 ze zm.);
c. odpowiedzialność karna – sankcje.

8. Sprzedajność pełniącego funkcję publiczną.

Jak stanowi art. 228 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.555 ze zm.):

„§1. Kto, w związku z pełnieniem funkcji publicznej, przyjmuje korzyść majątkową lub osobistą albo jej obietnicę podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§3. Kto, w związku z pełnieniem funkcji publicznej, przyjmuje korzyść majątkową lub osobistą albo jej obietnicę za zachowanie stanowiące naruszenie przepisów prawa, podlega karze pozbawienia wolności od roku do lat 10.

§4. Karze określonej w §3 podlega także ten, kto, w związku z pełnieniem funkcji publicznej, uzależnia wykonanie czynności służbowej od otrzymania korzyści majątkowej lub osobistej albo jej obietnicy lub takiej korzyści żąda.

§5. Kto, w związku z pełnieniem funkcji publicznej, przyjmuje korzyść majątkową znacznej wartości albo jej obietnicę podlega karze pozbawienia wolności od lat 2 do 12.
§6. Karom określonym w §1–5 podlega odpowiednio także ten, kto, w związku z pełnieniem funkcji publicznej w państwie obcym lub w organizacji międzynarodowej, przyjmuje korzyść majątkową lub osobistą albo jej obietnicę lub takiej korzyści żąda, albo uzależnia wykonanie czynności służbowej od jej otrzymania".

9. Nadużycie uprawnień przez funkcjonariusza.

Jak stanowi art. 231 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz.U.1997.88.553 ze zm.):
„§ 1. Funkcjonariusz publiczny, który, przekraczając swoje uprawnienia lub nie dopełniając obowiązków, działa na szkodę interesu publicznego lub prywatnego, podlega karze pozbawienia wolności do lat 3.
§2. Jeżeli sprawca dopuszcza się czynu określonego w §1 w celu osiągnięcia korzyści majątkowej lub osobistej, podlega karze pozbawienia wolności od roku do lat 10.
§3. Jeżeli sprawca czynu określonego w §1 działa nieumyślnie i wyrządza istotną szkodę, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§4. Przepisu §2 nie stosuje się, jeżeli czyn wyczerpuje znamiona czynu zabronionego określonego w art. 228.

10. Ujawnianie informacji w związku z wykonywaną funkcją.

Jak stanowi art. 266 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.):
„§1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

Przestępstwa z art. 228 i art. 231 Kodeksu karnego mogą zostać popełnione przez funkcjonariusza publicznego. Natomiast przestępstwo z art. 266 Kodeksu karnego może zostać popełnione przez każdą świadomą i zdolną do poniesienia odpowiedzialności osobę, o ile przestępstwo jest powiązane z realizowanymi przez nią działaniami zawodowymi, gdzie korzyścią

majątkową lub osobistą jest korzyść zarówno dla siebie, jak i dla kogoś innego.

11. Bezprawne uzyskanie informacji.

Jak stanowi art. 267 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.):

„Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego".

Tej samej karze podlega również ten, kto informację uzyskaną w sposób określony w §1–2 ujawnia innej osobie.

12. Utrudnianie zapoznania się z informacją.

Jak stanowi art. 268 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.):

„§1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Jeżeli czyn określony w §1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§3. Kto, dopuszczając się czynu określonego w §1 lub §2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

13. Niszczenie danych informatycznych.

Jak stanowi art. 268a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.):

„§1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§2. Kto, dopuszczając się czynu określonego w §1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

14. Uszkodzenie danych informatycznych.

Jak stanowi art. 269 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.):

„§1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§2. Tej samej karze podlega, kto dopuszcza się czynu określonego w §1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych".

15. Zakłócenie systemu komputerowego.

Jak stanowi art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.):

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Przestępstwa mogą zostać popełnione przez każdą świadomą i zdolną do poniesienia odpowiedzialności osobę, gdy korzyścią majątkową lub osobistą jest korzyść zarówno dla siebie, jak i dla kogoś innego.

XXVIII. Zasady prowadzenia i uaktualniania dokumentacji

1. Za aktualność i poprawność Polityki odpowiada administrator.

2. Przeglądu Polityki pod kątem jej aktualności oraz poprawności dokonuje komendant nie rzadziej niż dwa razy w roku, z tym że pierwszy przegląd Polityki należy przeprowadzić nie później niż w 2021roku.

3. Każda zmiana Polityki lub treści w niej zawartych powinna zostać odnotowana w rejestrze (zob. Załącznik nr 34).

ZAŁĄCZNIKI
Załącznik nr 34. Wzór Rejestru zmian w Polityce ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

Zatwierdził
Komendant Straży Gminnej (Miejskiej) w [...]

Zapoznał się:
Wójt [...]

XXIX. Lista załączników

1. Załącznik nr 1. Wzór strony tytułowej Polityki ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].
2. Załącznik nr 1.1. Wzór Zarządzenia wdrożenia Polityki ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].
3. Załącznik nr 2. Wzór Mapy procesów w Straży Gminnej (Miejskiej) w [...].
4. Załącznik nr 3. Wzór Protokołu przeglądu zasobów informacyjnych w Straży Gminnej (Miejskiej) w [...].
5. Załącznik nr 4. Wzór Rejestru przeglądów zasobów informacyjnych w Straży Gminnej (Miejskiej) w [...].
6. Załącznik nr 5. Wzór wykazu przykładowych zaleceń w zakresie wymaganych środków technicznych i organizacyjnych w Straży Gminnej (Miejskiej) w [...].
7. Załącznik nr 6. Wzór Rejestru ewidencji zmian, wdrożeń, przeglądów i zaleceń w Straży Gminnej (Miejskiej) w [...].
8. Załącznik nr 7. Wzór Rejestru nośników informatycznych w Straży Gminnej (Miejskiej) w [...].
9. Załącznik nr 8. Wzór Ewidencji rejestrów, ewidencji i wykazów w Straży Gminnej (Miejskiej) w [...].

10. Załącznik nr 9. Wzór Rejestru systemów i aplikacji w Straży Gminnej (Miejskiej) w [...].
11. Załącznik nr 10. Wzór Rejestru naruszeń/ podejrzeń naruszeń ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].
12. Załącznik nr 11. Wzór Raportu IOD z oceny naruszeń/ podejrzeń naruszeń ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].
13. Załącznik nr 12. Wzór Formularza zgłoszenia naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].
14. Załącznik nr 13. Wzór przykładowej Klauzuli informacyjnej dla Straży Gminnej (Miejskiej) w [...].
15. Załącznik nr 14. Wzór Rejestru udostępnień danych i informacji w Straży Gminnej (Miejskiej) w [...].
16. Załącznik nr 15. Wzór Raportu z oceny ryzyka stopnia (wagi) naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].
17. Załącznik nr 16. Wzór Raportu z oceny ryzyka naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].
18. Załącznik nr 17. Wzór Rejestru zasobów krytycznych w Straży Gminnej (Miejskiej) w [...].
19. Załącznik nr 17.1. Wzór Raportu z przeglądu planów ciągłości działania w Straży Gminnej (Miejskiej) w [...].
20. Załącznik nr 18. Wzór Rejestru przeglądów planów ciągłości działania w Straży Gminnej (Miejskiej) w [...].
21. Załącznik nr 19. Wzór Umowy o współadministrowaniu danymi w Straży Gminnej (Miejskiej) w [...].
22. Załącznik nr 20. Wzór Umowy powierzenia przetwarzania danych w Straży Gminnej (Miejskiej) w [...].
23. Załącznik nr 21. Wzór Wykazu kategorii czynności przetwarzania danych osobowych, za które odpowiada komendant Straży Gminnej (Miejskiej) w [...].
24. Załącznik nr 22. Wzór Wykazu kategorii przetwarzania danych w imieniu komendanta Straży Gminnej (Miejskiej) w [...].
25. Załącznik nr 23. Wzór Protokołu zniszczenia informatycznych nośników danych w Straży Gminnej (Miejskiej) w [...].
26. Załącznik nr 24. Wzór Wniosku o nadanie/ odebranie upoważnienia do przetwarzania danych przetwarzanych w Straży Gminnej (Miejskiej) w [...].

27. Załącznik nr 25. Wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych w Straży Gminnej (Miejskiej) w [...].
28. Załącznik nr 26. Wzór Rejestru wniosków o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w Straży Gminnej (Miejskiej) w [...].
29. Załącznik nr 27. Wzór Miesięcznego Sprawozdania z działań IOD w Straży Gminnej (Miejskiej) w [...].
30. Załącznik nr 28. Wzór Rocznego sprawozdania z działań IOD w Straży Gminnej (Miejskiej) w [...].
31. Załącznik nr 29. Wzór Rejestru sprawozdań z działań IOD w Straży Gminnej (Miejskiej) w [...].
32. Załącznik nr 30. Wzór Arkusza oceny ryzyka procesów przetwarzania w zakresie wydanych rekomendacji przez IOD w Straży Gminnej (Miejskiej) w [...].
33. Załącznik nr 31. Wzór Rejestru przeprowadzonych ocen ryzyka procesów przetwarzania w zakresie wydanych rekomendacji przez IOD w Straży Gminnej (Miejskiej) w [...].
34. Załącznik nr 32. Wzór listy obecności ze szkolenia w Straży Gminnej (Miejskiej) w [...].
35. Załącznik nr 33. Wzór Regulaminu monitoringu wizyjnego wraz z załącznikami.
36. Załącznik nr 34. Wzór Rejestru zmian w Polityce ochrony danych osobowych w Straży Gminnej (Miejskiej) w [...].

XXX. Biogramy autorów

1. dr Dariusz Wasiak https://orcid.org/0000-0001-6057-7475
   Adiunkt w WSB we Wrocławiu. Specjalizuje się w bezpieczeństwie informacji, w tym ochronie danych osobowych oraz dostępie do informacji publicznej i prawie do prywatności. Autor publikacji naukowych z zakresu prawa, w tym wykorzystywania klauzul limitacyjnych oraz bezpieczeństwa informacji i ochrony danych osobowych. Absolwent studiów na kierunkach: prawo, zarządzanie bezpieczeństwem, ekonomia menadżerska, zarządzanie kadrami oraz ochrona danych osobowych, a także cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji.

Audytor zintegrowanego systemu zarządzania według norm ISO 14001, ISO 27001, ISO 45001, ISO 9001, OHSAS1800. Pełnomocnik wg ISO 9001. Compliance Officer wg normy ISO 19600 oraz ISO 37001. Audytor wiodący dla systemów zarządzania bezpieczeństwem informacji według normy ISO 27001 oraz zarządzania ciągłością działania według normy ISO 22301. Audytor wewnętrzny m.in. dla systemów zarządzania prywatnością wg normy ISO 27701

Praktyk z zakresu efektywnego realizowania ochrony danych i innych informacji prawnie chronionych. Doświadczenie oparte na współpracy z administracją samorządową, służbami mundurowymi jako komendant straży, konsultant i IOD, a także w spółkach kapitałowych jako doradca, ABI i IOD oraz audytor dla podmiotów certyfikujących i wdrożeniowych.

Uczestnik licznych szkoleń tematycznych oraz realizator kilku projektów wdrożeniowych z zakresu RODO, bezpieczeństwa informacji, w tym obsługi zgłoszeń i zapewnienia poufności sygnalistom. Prelegent na konferencjach organizowanych przez GIODO i PREZESA UODO.

Mediator sądowy w sprawach karnych i cywilnych oraz biegły sądowy przy Sądzie Okręgowym we Wrocławiu z dziedziny bezpieczeństwo informacji.

Wspólnik w Leximum Jabłoński i Wspólnicy sp. z o.o. sp. k.

2. Tomasz Soczyński https://orcid.org/0000-0002-0795-5067
Doktorant na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego oraz absolwent Uniwersytetu Śląskiego. Prelegent i panelista licznych konferencji naukowych, a także wieloletni praktyk w prowadzeniu efektywnych szkoleń w zakresie bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.

Zawodowo specjalizuje się w bezpieczeństwie przetwarzania informacji i danych oraz zabezpieczeń systemów informatycznych. W jego obszarze zainteresowań zawodowych i naukowych znajdują się również

zagadnienia związane z prywatnością w prawie telekomunikacyjnym oraz naruszeniami danych osobowych w kontekście rozwijających się rozwiązań technologicznych.

Autor licznych publikacji naukowych z obszaru bezpieczeństwa informacji oraz cyberbezpieczeństwa

3. dr Krzysztof Wygoda https://orcid.org/0000-0002-0997-5512
Adiunkt na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Członek PTPK i Członek Komitetu Redakcyjnego dwumiesięcznika PPK. Autor i współautor ponad 100 publikacji, w tym kilkudziesięciu monografii i artykułów poświęconych problematyce ochrony danych osobowych, a także współautor komentarza do rozporządzenia ogólnego o ochronie danych oraz do ustawy o dostępie do informacji publicznej. Współtwórca opinii i ekspertyz dla GIODO i Prezesa UODO.

Specjalista z zakresu ochrony danych osobowych i dostępu do informacji publicznej zajmujący się kompleksowym doradztwem i obsługą prawną administratorów danych osobowych. Prelegent i panelista kilkudziesięciu konferencji i kongresów poświęconych ochronie danych osobowych.

Posiada ponad 25-letnie doświadczenie w obszarze szkoleń, doradztwa i audytów w zakresie ochrony danych osobowych, ochrony informacji i dostępu do informacji publicznej. Współtwórca i wieloletni wykładowca na studiach podyplomowych z tego obszaru. Realizator i współrealizator kilku projektów wdrożeniowych z zakresu RODO.

Wspólnik w Leximum Jabłoński i Wspólnicy sp. z o.o. sp. k.

XXXI. Wybrana literatura

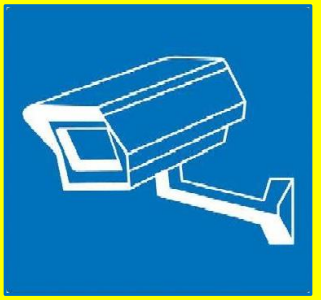
1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U.1997.78.483 ze zm.);
2. Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U. 1971.12.114 ze zm.);

3. Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz.U.1982.35.228 ze zm.);
4. Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.);
5. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz.U.1997.90.557 ze zm.);
6. Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U.1997. 88.555 ze zm.);
7. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U.1997.88.553 ze zm.);
8. Ustawa z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz.U.1999.83.930 ze zm.);
9. Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz.U. 2001.62.627 ze zm.);
10. Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. 2001. 106.1148 ze zm.);
11. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001.112.1198 ze zm.);
12. Ustawa z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz.U.2002.130.1112 ze zm.);
13. Ustawa z dnia 14 grudnia 2012 r. o odpadach (Dz.U. 2013.21 ze zm.);
14. Ustawa z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz.U.2014.24 ze zm.).;
15. Ustawa z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz.U.2016.177 ze zm.);
16. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);
17. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125);
18. Rozporządzenie (WE) NR 785/2004 Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie wymogów ubezpieczeniowych przewoźników lotniczych i operatorów statków powietrznych (Dz.U.U-E.L.2004.138.1);

19. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1);
20. Rozporządzenie Wykonawcze Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich (Dz.U.UE.L.2019.152.1);
21. Rozporządzenie Wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz.U.UE.L.2019.152.45);
22. Rozporządzenie delegowane Komisji (UE) 2020/1058 z dnia 27 kwietnia 2020 r. zmieniające rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych (Dz.U.UE.L.2020.232.1);
23. Rozporządzenie wykonawcze Komisji (UE) 2020/639 z dnia 12 maja 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do standardowych scenariuszy operacji wykonywanych w zasięgu wzroku lub poza nią (Tekst mający znaczenie dla EOG) (Dz.U.UE.L.2020.150.1);
24. Rozporządzenie wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19 (Dz.U.UE.L.2020.176.13);
25. Dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z dnia 18 czerwca 2009 r. w sprawie bezpieczeństwa zabawek (Dz.U.UE.L.2009.170.1);
26. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE.L.2016.119.89);
27. Gawroński M. i inni, *RODO ze wzorami*, (red.) M. Gawroński, Warszawa 2018, w tym przywołana tam literatura;

28. Grzelak A. i inni, *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, (red.) A. Grzelak, Warszawa 2019, w tym przywołana tam literatura;
29. Liwszic P, T. Ochocki, Łukasz Pociecha, *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, Warszawa 2019, w tym przywołana tam literatura;
30. Stanik J., Kiedrowicz M., Protasowicki T., *Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2014, vol. 113/2, w tym przywołana tam literatura.

UWAGA !!! OBSZAR MONITOROWANY



ADMINISTRATOR DANYCH

Administratorem danych osobowych przetwarzanych w związku z prowadzonym monitoringiem wizyjnym na terenie ..... jest ..... z siedzibą przy ..... , tel. ..... e-mail:.....

INSPEKTOR OCHRONY DANYCH

Z Inspektorem Ochrony Danych można się skontaktować za pośrednictwem poczty elektronicznej: ..... lub kierując korespondencje na adres: Inspektor Ochrony Danych ..... , bądź .....

WSPÓŁADMNISTRATOR

Współadministratorem danych osobowych przetwarzanych w związku z prowadzonym monitoringiem wizyjnym na terenie ..... jest komendant straży gminnej (miejskiej) w [...] z siedzibą przy , tel. ..... e-mail:.....

CEL PRZETWARZANIA

- **Utrwalanie dowodów popełnienia przestępstwa lub wykroczenia**
- **Przeciwdziałanie przypadkom naruszania spokoju i porządku w miejscach publicznych**
- **Ochrona obiektów komunalnych i urządzeń użyteczności publicznej**
- **Ochrona przeciwpożarowa i przeciwpowodziowa**

PODSTAWA PRAWNA PRZETWARZANIA

- **Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.1990.16.95 zm.)**
- **Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. 1997.123.779 ze zm.)**

POSTANOWIENIA SPECJALNE I PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

- **Zasięgiem monitoringu wizyjnego objęte są obszary w polu widzenia kamer**
- **Administrator przechowuje nagrania przez okres 30 dni od dnia nagrania. Okres przechowywania nagrań może jednak zostać przedłużony, w szczególność w przypadku uznania nagrania za materiał dowodowy.**
- **Z miejscami usytuowania kamer, procesem przetwarzania danych oraz przysługującymi prawami można zapoznać się w sposób określony po lewej stronie.**

WIĘCEJ INFORMACJI

- **w siedzibie**
  - **urzędu gminy [...]**
  - **straży gminnej (miejskiej) w [...]**
- **na stronie: https://.....**
- **poprzez kod QR.**

Załącznik nr 1 do uchwały / zarządzenia z dnia 01. […] 20[…] r.
w sprawie przyjęcia i wdrożenia w Straży Gminnej (Miejskiej) w […]
Polityki ochrony danych osobowych w Straży Gminnej (Miejskiej) w […]

Polityka ochrony danych osobowych
w
Straży Gminnej (Miejskiej) w […]
(Polityka lub Polityka ODO)

Uwaga:

1. Niniejsza Polityka wraz z załącznikami jest dokumentem wewnętrznym.
2. Nadzór nad realizacją Polityki oraz dokumentacją sprawuje komendant.
3. Udostępnienie Polityki następuje wyłącznie za wiedzą Komendanta.
4. Udostępnienie Polityki wraz z załącznikami następuje wyłącznie za wiedzą i zgodą Komendanta.

Siedziba
ul. […]
kod […]
tel. […]
@: […]
https:// […]

[…], 2021

Formularz dokumentu

Wersja	1.0
Liczba stron	
Data przyjęcia	
Data udostępnienia	
Liczba kopii	1
Planowany termin przeglądu	
Dystrybucja i kopiowanie dokumentu	ograniczone
Udostępnienie załączników dokumentu	ograniczone – komendant straży

Historia przeglądów i zmian

Wersja	1.1
Liczba stron	
Data utworzenia	
Data ostatniego przeglądu	
Data ostatniej modyfikacji	
Zakres modyfikacji	
Data przyjęcia	
Data udostępnienia	
Liczba kopii	1
Planowany termin przeglądu	
Dystrybucja i kopiowanie dokumentu	ograniczone
Udostępnienie załączników dokumentu	komendant straży

Wersja	1.2
Liczba stron	
Data utworzenia	
Data ostatniego przeglądu	
Data ostatniej modyfikacji	
Zakres modyfikacji	
Data przyjęcia	
Data udostępnienia	
Liczba kopii	1
Planowany termin przeglądu	
Dystrybucja i kopiowanie dokumentu	ograniczone
Udostępnienie załączników dokumentu	komendant straży

Zarządzenie Nr […]/[…]
Komendanta Straży Gminnej (Miejskiej) w […]
z dnia […]
w sprawie przyjęcia i wdrożenia Polityki ochrony danych osobowych w Straży Gminnej (Miejskiej) w […]

Na podstawie art. 31 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125), przy uwzględnieniu przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 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.U.UE.L.2016.119.1) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018.1000 ze zm.), w celu wykonywania ustawowych zadań Straży Gminnej (Miejskiej) w […] ustalonych w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) wraz z aktami wykonawczymi w zakresie ochrony danych osobowych osób fizycznych przetwarzanych w Straży Gminnej (Miejskiej) w […],

zarządzam co następuje:

§1.

Wprowadzam do stosowania Politykę ochrony danych osobowych w Straży Gminnej (Miejskiej) w […], w brzmieniu określonym w Załączniku nr 1 do Zarządzenia – w dalszej treści występującej, jako Polityka lub Polityka ODO.

§2.

Zobowiązuję wszystkich strażników Straży Gminnej (Miejskiej) w […] do zapoznania się z Polityką oraz bezwzględnego stosowania opisanych w niej procedur.

§3.

Zobowiązuję Inspektora ochrony danych w Straży Gminnej (Miejskiej) w [...] do nadzoru, monitorowania wdrażania i stosowania Polityki oraz do niezwłocznego informowania Komendanta – administratora danych osobowych, o wszystkich stwierdzonych incydentach, naruszeniach zasad ochrony danych osobowych lub praw i wolości podmiotu danych, a także o innych ujawnionych nieprawidłowościach w stosowaniu ustalonych procedur Polityki.

§4.

Zarządzenie wchodzi w życie z dniem podpisania

.....

Data, pieczęć i czytelny podpis

Mapa procesów w Straży Gminnej (Miejskiej) w [...]

Lp.	Nazwa procesu / czynności (zadanie)	Zakres czynności	Cel wspierający	Zastosowane środki i urządzenia	Współadministrator	Podmiot przetwarzający	Forma uregulowania współadministrowania/ powierzenia przetwarzania	Dokonano uprzedniej weryfikacji podmiotu przetwarzającego	Proces zautomatyzowany / częściowo zautomatyzowany	Kategorie i zakres danych osobowych	Model pozyskania danych	Źródło danych	Miejsce, w którym następuje pierwsze przetworzenie danych	Miejsce przetwarzania nośników danych	Miejsce przechowywania danych	Nośnik danych	Sposób zabezpieczenia nośnika	Osoby upoważnione do przetwarzania danych	Rola osób upoważnionych w tym procesie	Podmioty i osoby, którym udostępniane są dane oraz inne informacje	Zakres udostępnianych danych i informacji	Zadanie powiązane	Niezbędność powiązania z innym zadaniem	DODO	Dane osobowe znajdującą się w aktach sprawy etc.	RODO	KPA	KPK	KPW	Pozostałe akty normatywne regulujące proces	Systemy i oprogramowanie	Nazwa zbioru
1																																

Przegląd mapy procesów

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

[…], […].[…].20[…] r.

Numer protokołu: […].20[…]

Skład zespołu:

1. ..... - imię i nazwisko / organizacja / funkcja
2. ..... - imię i nazwisko / organizacja / funkcja

Protokół

z przeglądu zasobów informacyjnych w Straży Gminnej (Miejskiej) w […]

1. Proces / czynności poddane przeglądowi:
   a. .....
2. Oznaczenie procesu / czynności:
   a. .....
3. Oznaczenie zasobu informacyjnego:
   a. .....
4. Data utworzenia zasobu informacyjnego oraz podstawa prawna jego utworzenia:
   a. .....
   b. .....
5. Forma gromadzenia zasobu informacyjnego:
   a. .....
6. Miejsca przechowywania zasobu informacyjnego:
   a. .....
7. Systemy i oprogramowanie biorące udział w gromadzeniu i przechowywaniu zasobu informacyjnego:
   a. .....
8. Nośniki, na których gromadzony jest zasób informacyjny:
   a. .....
9. Podmiot odpowiedzialny za ochronę zasobu informacyjnego:
   a. .....
10. Osoba odpowiedzialna za bezpieczeństwo zasobu informacyjnego:
    a. .....
11. Kategoria podmiotów i organizacji posiadających dostęp do zasobów informacyjnych oraz podstawa prawna umożliwiająca dostęp do zasobu informacyjnego:
    a. .....
    b. .....

12. Kategoria osób posiadających dostęp do zasobów informacyjnych oraz podstawa prawna umożliwiająca dostęp do zasobu informacyjnego:
    a. .....
    b. .....
13. Procesy powiązane:
    a. .....
14. Cel przeglądu:
    a. .....

Ustalenia w zakresie ochrony danych osobowych:

1. W ramach realizacji procesu dochodzi / nie dochodzi do przetwarzania danych osobowych:
    a. .....
2. Cel przetwarzania danych osobowych:
    a. .....
3. Podstawy prawne przetwarzania danych osobowych:
    a. .....
4. Kategorie danych przetwarzana w ramach realizacji procesu:
    a. zwykłe
    b. wrażliwe
    c. o naruszeniach prawa
5. Zakres danych przetwarzanych w ramach realizacji procesu:
    a. .....
    b. .....
6. Miejsca przetwarzania danych osobowych:
    a. .....
7. Systemy, oprogramowanie i nośniki biorące udział w przetwarzaniu danych osobowych:
    a. .....
8. Istniejące zabezpieczenia organizacyjne:
    a. .....
9. Istniejące zabezpieczenie techniczne:
    a. .....

Na tym protokół w dniu [...] o godz. [...] zakończono.

Data i podpisy członków zespołu:
1. .....
2. .....

Data przekazania protokołu IOD: .....
Forma przekazania protokołu IOD: .....
Data i podpis osoby, która dokonała przekazania:
.....

Rekomendacje IOD:
1. .....
Data przekazania protokołu komendantowi: .....
Forma przekazania protokołu komendantowi: .....

Data i podpis IOD
.....

Data i podpis komendanta
.....

Polecenie komendanta:
1. .....

Data i podpis komendanta
.....

Rejestr przeglądów zasobów informacyjnych w Straży Gminnej (Miejskiej) w […]

Lp.	Proces / czynność poddana przeglądowi	Numer z Mapy procesów	Numer protokołu	Data przeglądu	Podstawa dokonania przeglądu	Skład zespołu dokonującego przeglądu	Wynik przeglądu			Dane osobowe przetwarzane na mocy			Podjęte działania		Planowany termin przeglądu	Uwagi
							Zakres nieprawidłowości	Przetwarzane kategorie danych osobowych	Procesy powiązane	RODO	DODO	Przepisów procesowych	zaradcze	naprawcze		
1																
2																
3																
4																
5																

Przegląd rejestru

Uwagi

Data i czytelny podpis osoby dokonującej przeglądu

Strona 1 z 10

Wykaz przykładowych zaleceń w zakresie wymaganych środków technicznych i organizacyjnych w Straży Gminnej (Miejskiej) w [...]			
Lp.	Cel stosowania technicznych i organizacyjnych środków ochrony danych	Wymagane zabezpieczenia	
1.	Kontrola dostępu	1.	Umiejscowienie pomieszczeń stanowiących obszary przetwarzania danych tak, aby ograniczony był do nich dostęp przez osoby postronne
		2.	Zastosowanie środków kontroli dostępu, np. drzwi o podwyższonej odporności na włamania z zamkami elektromagnetycznymi o podwyższonej odporności na pokonanie zabezpieczeń. Dotyczy to zarówno wejścia na teren obiektu, jak i całego budynku
		3.	Zastosowanie monitoringu wizyjnego bez dźwięku wewnątrz pomieszczeń
		4.	System alarmowy podłączony do grupy interwencyjnej firmy ochrony z ustalonym czasem reakcji pozwalającym na skuteczna działania zapobiegawcze
		5.	Zakaz używania urządzeń utrwalających obraz i dźwięk
		6.	Ulokowanie sprzętu w taki sposób, aby zminimalizować ryzyko dostępu do sprzętu
		7.	Ulokowanie sprzętu w taki sposób, aby zminimalizować ryzyko podglądu treści wyświetlanych na monitorze
2.	Kontrola nośników danych	1.	Wykorzystanie technik kryptograficznych do ochrony danych na nośnikach wymiennych
		2.	Określenie liczby nośników, ich użytkowników oraz ich zarejestrowanie
		3.	Przypisanie nośników wymiennych do urządzeń
		4.	Przechowywanie nośników informacji w warunkach gwarantujących ich bezpieczeństwo oraz poufność informacji
		5.	Przechowywanie na oddzielnych nośnikach kopii danych
		6.	Monitorowanie kopiowania i usuwania informacji
		7.	Stała kontrola posiadania notatników służbowych oraz zasobów służbowych aparatów telefonicznych
		8.	Usuwanie informacji w sposób uniemożliwiający ich odtworzenie przy uwzględnieniu normy DIN 6639

3.	Kontrola przechowywania danych	1.	Zapewnienie mechanizmu automatycznego blokowania ekranu w przypadku czasowej nieaktywności użytkownika – od 2 do 5 minut nieaktywności
		2.	Zobowiązanie użytkownika do blokowania ekranu po odejściu od stanowiska lub wymuszenie tego systemowo
		3.	Zobowiązanie użytkownika do stosowania się do zasady czystego biurka, czystego kosza, czystego ekranu
		4.	Zobowiązanie użytkownika do wyłączania stacji roboczej po zakończeniu pracy lub systemowe wymuszenie wyłączenia po 15 minutach nieaktywności użytkownika
		5.	Stosowanie filtrów prywatyzujących na ekranach komputerów
4.	Kontrola użytkowników	1.	Zobowiązanie użytkowników do zachowania w poufności danych uwierzytelniających
		2.	Zapewnienie wymuszenia, przy pierwszym użyciu, tymczasowych danych uwierzytelniających
		3.	Zakaz współdzielenia danych uwierzytelniających
		4.	Zakaz korzystania z tych samych danych uwierzytelniających dla celów prywatnych i służbowych
		5.	Bezzwłoczne blokowanie kont osób, które odeszły od straży lub znajdują się na urlopie lub chorobowym
		6.	Cykliczne przeglądy uprawnień systemowych użytkowników
5.	Kontrola dostępu do danych	1.	Rozdzielenie ról związanych z kontrolą dostępów: wnioskowanie, autoryzacja, zarządzanie dostępami, użytkownik konta
		2.	Stosowanie formalnego procesu przydzielania oraz odbierania dostępów użytkownikom
		3.	Stosowanie zasad zawartych w Polityce ochrony danych osobowych
		4.	Prowadzenie spisu praw dostępowych do systemów i usług przydzielonych użytkownikom
		5.	Zarządzanie prawami uprzywilejowanego dostępu
		6.	Cykliczne testyy praw dostępowych
		7.	Cykliczne przeglądy uprawnień użytkowników

6.	Kontrola przesyłu danych	1.	Wykrywanie i ochrona przed szkodliwym kodem, który może być przesyłany za pomocą środków komunikacji elektronicznej
		2.	Określenie akceptowalnego sposobu korzystania z elektronicznych urządzeń komunikacji na odległość
		3.	Korzystanie z technik kryptograficznych
		4.	Automatyczne i manualne odnotowywanie odbiorców danych
		5.	Zakaz wykorzystywania prywatnej poczty elektronicznej do celów służbowych oraz prywatnej do celów służbowych
7.	Kontrola wprowadzania danych	1.	Wdrożenie mechanizmów pozwalających odnotować informacje w zakresie ewidencjonowania operacji przetwarzania danych
		2.	Wdrożenie mechanizmów informujących o stwierdzonych anomaliach systemowych oraz w innych rejestrach
		3.	Wdrożenie procedur cyklicznego analizowania informacji w zakresie ewidencjonowania operacji przetwarzania danych
		4.	Stosowanie wyłącznie indywidualnych danych uwierzytelniających
		5.	Weryfikowanie współdzielenia danych uwierzytelniających
8.	Kontrola transportu	1.	Sprawdzenie nośników danych i materiałów pod kątem ich naruszenia lub zniszczenia w czasie transportu
		2.	Korzystanie z wiarygodnych środków komunikacji, w tym z podmiotów, z którymi zawarto indywidualne umowy na transport nośników danych
		3.	Wdrożenie procedur weryfikacji kurierów, którym przekazuje się nośniki danych
		4.	Korzystanie z tzw. bezpiecznych kopert
		5.	Wdrożenie procedur opisywania, zabezpieczenia i weryfikacji nośników zawierających dane
		6.	Prowadzenie ewidencji przesyłanych nośników zawierających dane

9.	Odzyskiwanie danych	1.	Określenie zakresu i częstotliwości wykonywania kopii zapasowych
		2.	Przechowywanie kopii zapasowych w innej lokalizacji niż źródłowe nośniki informacji w sposób zapewniający bezpieczeństwo danych
		3.	Ustalenie i wprowadzenie adekwatnych zabezpieczeń technicznych, fizycznych i organizacyjnych kopii zapasowych
		4.	Regularne, nie rzadziej niż raz w miesiącu, testowanie poprawności kopii zapasowych
		5.	Kryptograficzne zabezpieczenie kopii zapasowych
		6.	Ustanowienie i wdrożenie procedur ciągłości działania
10.	Integralność	1.	Systematyczna kontrola i analiza przez WPO oraz Komendanta dzienników zdarzeń rejestrujących działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji
		2.	Uniemożliwienie ASI i ABI usuwanie lub dezaktywację dzienników systemowych
		3.	Synchronizacja zegarów wszystkich systemów przetwarzających informacje z jednym wzorcowym czasem i ich stałe monitorowanie
		4.	Wdrażanie aplikacji i oprogramowań systemów wyłącznie po ich testowym sprawdzeniu pod kątem ich bezpieczeństwa i funkcjonalności
		5.	Aktualizacja oprogramowań, bibliotek i aplikacji wyłącznie przez lub przy udziale ASI i ABI

Przegląd wykazu	
Data i czytelny podpis osoby dokonującej przeglądu	Uwagi
Strona 1 z 10	

Rejestr zmian, wdrożeń, przeglądów i zaleceń w Straży Gminnej (Miejskiej) w […]															
Lp.	Nazwa		Zakres				Data				Imię i nazwisko osoby dokonującej				Uwagi
	procesu	czynności	przeglądu	zmian	wdrożeń	zaleceń	wdrożenia	przeglądu	zalecenia	zmiany	wdrożenia	przeglądu	zalecenia	zmiany	
1.															
2.															
3.															

Przegląd rejestru	
Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

Rejestr nośników informatycznych w Straży Gminnej (Miejskiej) w […]

Lp.	Nośnik				Forma i rodzaj zabezpieczenia	Cel wykorzystywania	Data				Uwagi
	Numer seryjny	Typ	Właściciel	Użytkownik			Przekazania	Zagubienia	Zniszczenia	Przeszkolenia użytkownika z obsługi nośnika	
1.											
2.											
3.											

Przegląd rejestru

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

Strona 1 z 10

Ewidencja rejestrów, ewidencji i wykazów w Straży Gminnej (Miejskiej) w […]

Lp.	Nazwa		Liczba stron	Cel prowadzenia	Data utworzenia	Data zakończenia	Numer wersji	Uwagi
	Rejestru	Ewidencji	Wykazu					
1.								
2.								
3.								

Przegląd ewidencji

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

Strona 1 z 10

Rejestr systemów i aplikacji w straży gminnej (miejskiej) w […]											
Lp.	Nazwa		Licencja/ data ważności	Producent		Dane osobowe są przetwarzane		Sygnatura umowy, w tym uchwały lub zarządzenia,			Uwagi
	aplikacji	systemu		Nazwa	Siedziba	[oza EOG	na terenie USA	o współadministrowanie	powierzenia przetwarzania danych	głównej	
1.											
2.											
3.											
Przegląd rejestru											
Data i czytelny podpis osoby dokonującej przeglądu				Uwagi							
Strona 1 z 10											

Rejestr naruszeń / podejrzeń naruszeń ochrony danych osobowych w Straży Gminnej (Miejskiej) w […]

Dane dot. zgłoszenia	L.p.		1
	Incydent/ naruszenie		
	Data i godzina incydentu/ zgłoszenia naruszenia		
	Data i godzina stwierdzenia naruszenia		
	Zgłaszający	Nazwisko i imię	
		Dane kontaktowe	
Dane dot. naruszenia/ podejrzenia naruszenia ochrony danych osobowych, jego skutków	Nazwa procesu związanego z naruszeniem		
	Właściciel procesu związanego z naruszeniem		
	Opis naruszenia/ podejrzenia naruszenia		
	Kategoria i liczba osób, których dotyczy naruszenie		
	Zakres danych lub kategorie danych, których dotyczy naruszenie		
	Możliwe konsekwencje naruszenia/ podejrzenia naruszenia ochrony danych osobowych		
	Ustalenia: doszło / nie doszło do naruszenia ochrony danych osobowych		
Zgłoszenie / zawiadomienie o wystąpieniu naruszenia	Organu Nadzorczego (UODO)	Podjęte działania	
		Data zgłoszenia	
		Godzina zgłoszenia	
		Treść zgłoszenia	
	Osób, których danych dot. naruszenie	Podjęte działania	
		Data zawiadomienia	
		Treść zawiadomienia	
		Powód braku zawiadomienia	
Istniejące środki bezpieczeństwa		Opis obowiązujących środków bezpieczeństwa w dniu ujawnienia naruszenia	
Raporty		Raport IOD	
		Raport z ceny stopnia ważności naruszenia	
Ocena stopnia ważności naruszenia			
Podjęte działania	Naprawcze		
	Zaradcze		
Data zakończenia postępowania			

Przegląd rejestru

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

Strona 1 z 10

[…], […].[…].20[…] r.

Numer raportu: […].20[…]
Inspektor Ochrony Danych

Komendant
[…]

RAPORT IOD
z oceny
naruszenia / podejrzenia naruszenia ochrony danych osobowych
w Straży Gminnej (Miejskiej) w […]

Informacje ogólne:

1. Data i godzina zgłoszenia naruszenia / podejrzenia naruszenia ochrony danych osobowych

.....

2. Data i godzina przyjęcia zgłoszenia przez IOD

.....

3. Osoby skutecznie poinformowane o zgłoszeniu:
   a. .....(imię i nazwisko, stanowisko, sposób poinformowania)
4. Osoby skutecznie poinformowane o naruszeniu:
   a. .....(imię i nazwisko, stanowisko, sposób poinformowania)
5. Osoby uczestniczące w obsłudze zgłoszenia:
   a. .....(imię i nazwisko, stanowisko)
6. Osoby uczestniczące w obsłudze naruszenia:
   a. .....(imię i nazwisko, stanowisko)
7. Data i godzina zakończenia obsługi zgłoszenia

.....

8. Data i godzina zakończenia obsługi naruszenia

.....

Klasyfikacja zgłoszenia:

Doszło do naruszenia ochrony danych osobowych / Nie doszło do naruszenia ochrony danych osobowych

Kwalifikacja obowiązku:

1. Występuje obwiązek zgłoszenia naruszenia ochrony danych osobowych do Prezesa UODO / Nie występuje obwiązek zgłoszenia naruszenia ochrony danych osobowych do Prezesa UODO
2. Występuje obwiązek poinformowania osób o naruszeniu ochrony danych osobowych / Nie występuje obwiązek poinformowania osób o naruszeniu ochrony danych osobowych

Ustalenia:

1. Charakter naruszenia ochrony danych osobowych

.....

2. Przybliżona liczba osób, których dane dotyczą

.....

3. Kategoria i zakres danych osobowych:
   a. .....
4. Podmioty współuczestniczące
   a. .....(współadministrator/ podmiot przetwarzający)
5. Przetwarzanie transgraniczne:
   a. ..... (poza EOG/ USA)
6. Zidentyfikowane podatności:
   a. .....
7. Zidentyfikowane ryzyka dla praw i wolności:
   a. .....
8. Działania i środki zaradcze:
   a. .....
9. Działania i środki naprawcze:
   a. .....
10. Działania na przyszłość:
    a. .....

Rekomendacje:

1. .....

Inne zalecenia i uwagi:

1. .....

Data i podpis IOD

.....

Data przekazania protokołu komendantowi .....

Forma przekazania protokołu komendantowi .....

Data i podpis IOD

.....

Data i podpis komendanta

.....

Polecenie komendanta:

1. .....

Data i podpis komendanta

.....

Formularz dostępny na stronie WWW https://www.biznes.gov.pl/pl/usluga/889 lub https://uodo.gov.pl/pl/134/233

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) Kliknij tutaj, aby wprowadzić tekst.

☐ Zgłoszenie kompletne/jednorazowe	☐ Zgłoszenie wstępne	☐ Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić tekst.

☐ Naruszenie zostało lub zostanie zgłoszone organowi ochrony danych osobowych w innym państwie Jeśli tak, podaj w jakim.

☐ Naruszenie zostało lub zostanie zgłoszone innym organom np. Policja, CSIRT NASK, CSIRT GOV, CSIRT MON (najedź myszką na nazwę organu, by dowiedzieć się więcej)

Podaj nazwy tych organów
Kliknij tutaj, aby wprowadzić tekst.

Podaj numer/sygnaturę zgłoszenia do innego organu
Kliknij tutaj, aby wprowadzić tekst.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.

REGON (opcjonalnie) Podaj numer. NIP (opcjonalnie) Podaj numer. KRS (opcjonalnie) Podaj numer.

Sektor (opcjonalnie) *Dla sektora publicznego:* Wybierz element. *Dla sektora prywatnego:* Wybierz element.

2B. Adres siedziby administratora danych

Ulica Kliknij tutaj, aby wprowadzić tekst. Numer domu Podaj numer Numer lokalu Podaj numer

Miejscowość Kliknij tutaj, aby wprowadzić tekst. Kod pocztowy Kliknij tutaj, aby wprowadzić tekst.

Gmina Kliknij tutaj, aby wprowadzić tekst. Powiat Kliknij tutaj, aby wprowadzić tekst.

Województwo Kliknij tutaj, aby wprowadzić tekst. Państwo Kliknij tutaj, aby wprowadzić tekst.

2C. Osoby uprawnione do reprezentowania administratora

1. Imię i nazwisko Kliknij tutaj, aby wprowadzić tekst. Stanowisko Kliknij tutaj, aby wprowadzić tekst.

(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk ✚, który pojawi się po prawej stronie.)

2D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** oraz dowód uiszczenia opłaty skarbowej.

2E. Inspektor ochrony danych

Imię i nazwisko imię i nazwisko. Numer telefonu Numer telefonu. Adres e-mail E-mail.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.
Kliknij tutaj, aby wprowadzić tekst.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

(Aby dopisać kolejne podmioty, należy po kliknięciu na powyższe pole kliknąć przycisk , który pojawi się po prawej stronie.)

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałaś/eś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa,
Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe, jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h.
Kliknij tutaj, aby wprowadzić tekst.

3B. Czas naruszenia

Data i czas zaistnienia/ rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

- ☐ a) Zgubienie lub kradzież nośnika/ urządzenia
- ☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
- ☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy
- ☐ d) Nieuprawnione uzyskanie dostępu do informacji
- ☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
- ☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych
- ☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)
- ☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie
- ☐ i) Nieprawidłowe usunięcie/ zniszczenie danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora
- ☐ j) Niezamierzona publikacja
- ☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy
- ☐ l) Ujawnienie danych niewłaściwej osoby
- ☐ m) Ustne ujawnienie danych osobowych

4C. Działanie złośliwego oprogramowania (Odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczone zostało pole f.)

a) Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności?
(W sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu.)
Kliknij tutaj, aby wprowadzić tekst.

b) Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (Podaj nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin.).

Kliknij tutaj, aby wprowadzić tekst.

c) Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak, to w jakim czasie ją przywrócił?

Kliknij tutaj, aby wprowadzić tekst.

UWAGA: *Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem https://incydent.cert.pl/. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe.*
O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza), podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska.

4D. Przyczyna naruszenia

- ☐ Wewnętrzne działanie niezamierzone
- ☐ Wewnętrzne działanie zamierzone
- ☐ Zewnętrzne działanie niezamierzone
- ☐ Zewnętrzne działanie zamierzone

4E. Charakter

- ☐ Naruszenie poufności danych
  Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych.
- ☐ Naruszenie integralności danych
  Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania.
- ☐ Naruszenie dostępności danych
  Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną.

4F. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji).

Kliknij tutaj, aby wprowadzić tekst.

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- ☐ Nazwiska i imiona
- ☐ Imiona rodziców
- ☐ Data urodzenia
- ☐ Numer rachunku bankowego
- ☐ Adres zamieszkania lub pobytu
- ☐ Numer ewidencyjny PESEL
- ☐ Adres e-mail
- ☐ Nazwa użytkownika i/lub hasło
- ☐ Dane dotyczące zarobków i/lub posiadanego majątku
- ☐ Nazwisko rodowe matki
- ☐ Seria i numer dowodu osobistego
- ☐ Numer telefonu
- ☐ Wizerunek
- ☐ Inne, wskaż jakie

  Kliknij tutaj, aby wprowadzić tekst.

6B. Dane szczególnej kategorii

- ☐ 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

6C. Dane, o których mowa w art. 10 RODO

☐ Dane dotyczące wyroków skazujących ☐ Dane dotyczące czynów zabronionych ☐ Inne

Kliknij tutaj, aby wprowadzić tekst.

7. Kategorie osób

☐ Pracownicy
☐ Użytkownicy
☐ Subskrybenci
☐ Studenci
☐ Uczniowie
☐ Służby mundurowe (np. wojsko, policja)
☐ Klienci (obecni i potencjalni)
☐ Klienci podmiotów publicznych
☐ Pacjenci
☐ Dzieci
☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie.
W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

☐ Utrata kontroli nad własnymi danymi osobowymi
☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
☐ Ograniczenie możliwości realizowania praw
☐ Dyskryminacja
☐ Kradzież lub sfałszowanie tożsamości
☐ Strata finansowa
☐ Naruszenie dobrego imienia
☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
☐ Nieuprawnione odwrócenie pseudonimizacji
☐ Inne
Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą.

Kliknij tutaj, aby wprowadzić tekst.

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

○ Tak ◉ Nie

Uzasadnienie

Kliknij tutaj, aby wprowadzić tekst.

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Zgodnie z treścią art. 22 ust. 1 i 2 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125) w zw. z art. 10a ust. 2 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. z 1997.123.779 ze zm.) – zwaną dalej **Ustawą**, informuję że:

I. ADMINISTRATOR DANYCH

Administratorem Pani/Pana danych osobowych jest Komendant Straży Gminnej (Miejskiej) w […], z którym można się skontaktować w następujący sposób:

1. listownie:
   Komendant Straży Gminnej (Miejskiej) w […]
   ul. […]
   kod i miejscowość […];
2. za pośrednictwem poczty elektronicznej:
   […]@[…];
3. telefonicznie:
   +48 […].

II. INSPEKTOR OCHRONY DANYCH

Inspektorem Ochrony Danych w Straży Gminnej (Miejskiej) w […] jest Pani/Pan […], z którym/ą można się skontaktować w następujący sposób:

1. listownie:
   Inspektor Ochrony Danych
   Straż Gminna (Miejska) w […]
   ul. […]
   kod i miejscowość […];
2. za pośrednictwem poczty elektronicznej:
   […]@[…].

III. CEL PRZETWARZANIA DANYCH OSOBOWYCH

Państwa dane osobowe będą przetwarzane w celu realizacji zadań związanych z ochroną porządku publicznego na terenie Gminy […], o których mowa w art. 11 Ustawy, przy wykorzystaniu podstawowych instrumentów prawnych regulowanych w szczególności przez przepisy:

1. ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125);
2. art. 10a ust. 1 oraz 10b i art. 12–12a Ustawy;
3. ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia (Dz.U. 2001.106.1148 ze zm.);
4. ustawy z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U. 1971.12.114 ze zm.).

IV. PRZETWARZANIE DANYCH POZA EOG

Pani/ Pana dane osobowe nie są przekazywane poza Europejski Obszar Gospodarczy.

V. PRAWO DO WNIESIENIA SKARGI

Każdej osobie, której dane dotyczą przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie przy ul. Stawki 2, 00–193 Warszawa, gdy uzna ona, że jej prawa zostały naruszone w wyniku przetwarzania danych osobowych przez Straż Gminną (Miejską) w [...].

Skargę można składać w następujący sposób:

1. listownie:
   Prezes Urzędu Ochrony Danych Osobowych
   ul. Stawki 2
   00-193 Warszawa;
2. za pośrednictwem elektronicznej skrzynki podawczej dostępnej na stronie WWW:
   https://www.uodo.gov.pl/pl/p/kontakt;
   a także:
3. kierując skargę na adres Inspektora Ochrony Danych w Straży Gminnej (Miejskiej) w [...] wskazany w pkt II;
4. kierując skargę do Wójta [...], jako organu sprawującego na mocy art. 7 ust. 2 Ustawy nadzór nad działaniami Komendanta Straży Gminnej (Miejskiej) w [...], za pośrednictwem:
   a. skrzynki podawczej dostępnej na stronie WWW:
      https://epuap.gov.pl/[....];

b. poczty elektronicznej
[…]@[…];
lub
c. listownie:
Wójt […]
ul. […]
kod i miejscowość […];
d. telefonicznie:
+48 […];
e. osobiście pod adresem wskazanym w pkt V ust. 4 lit c powyżej, w każdy:
- […], w godz. […]–[…];
- […], w godz. […]–[…].

VI. PRAWO DO ŻĄDANIA

Osoba, której dane dotyczą, posiada prawo żądania od administratora danych:

1. dostępu do danych osobowych,
2. sprostowania,
3. usunięcia danych osobowych,
4. ograniczenia przetwarzania danych osobowych.

VII. Klauzula informacyjna jest dostępna:

1. na stronie WWW BIP:
https://[….];
2. w siedzibie Straży Gminnej (Miejskiej) w […] pod adresem wskazanym w pkt I.

Rejestr udostępnień danych i informacji w Straży Gminnej (Miejskiej) w [...]

Lp.	Dane wnioskującego	Kanał wpływu wniosku	Data wpływu	Sygnatura wniosku	Podstawa złożenia wniosku	Zakres żądania	Osoba zobowiązana do analizy wniosku	Zakres udostępnionych danych / informacji	Odmowa udostępnienia/ Zakres odmowy udostępnienia	Podstawa prawna odmowy udostępnienia	Forma / Sposób udostępnienia	Data udostępnienia	Osoba udostępniająca informacje	Uwagi
1.														
2.														
3.														

Przegląd rejestru

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

[…], […].[…].20[…] r.

Numer raportu: […].20[…]

Inspektor Ochrony Danych

Komendant
[…]

RAPORT
z oceny ryzyka stopnia (wagi) naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w […]

Dotyczy: …… (numer naruszenia z rejestru)

1. Opis naruszenia:

……

2. Środki techniczne i organizacyjne przed naruszeniem:
   a. ……
3. Kategoria danych:
   a. ……
4. Zakres danych:
   a. ……
5. Cel przetwarzania danych:
   a. ……
6. Podstawa prawna przetwarzania danych:
   a. ……
7. Podjęte czynności po wystąpieniu naruszenia:
   a. ……
8. Poziom kontekstu przetwarzania danych:

……

Uzasadnienie:

……

9. Prawdopodobieństwo identyfikacji:

.....

Uzasadnienie:

.....

10. Okoliczności naruszenia:

.....

Uzasadnienie:

.....

11. Ocena ryzyka:

.....

Uzasadnienie:

.....

12. Powiadomienie PUODO:

.....

Uzasadnienie:

.....

13. Wnioski:

.....

Data i podpis IOD

.....

Data przekazania protokołu komendantowi: .....

Forma przekazania protokołu komendantowi: .....

Data i podpis IOD

.....

Data i podpis komendanta

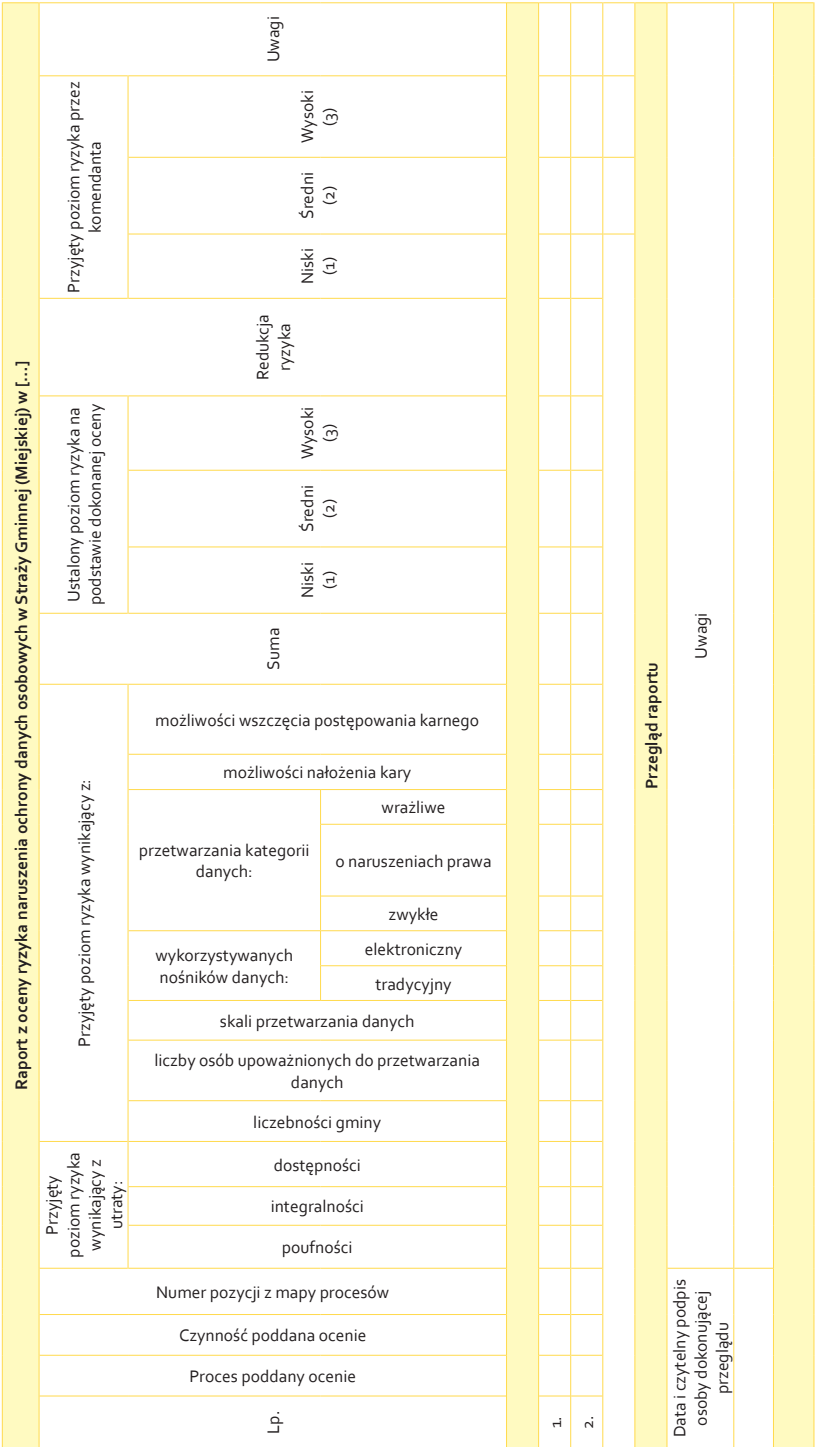
.....

Polecenie komendanta:

1. .....

Data i podpis komendanta

.....


Raport z oceny ryzyka naruszenia ochrony danych osobowych w Straży Gminnej (Miejskiej) w […]
Lp.
Proces poddany ocenie
Czynność poddana ocenie
Numer pozycji z mapy procesów
Przyjęty poziom ryzyka wynikający z utraty:
poufności
integralności
dostępności
Przyjęty poziom ryzyka wynikający z:
liczebności gminy
liczby osób upoważnionych do przetwarzania danych
skali przetwarzania danych
wykorzystywanych nośników danych:
tradycyjny
elektroniczny
przetwarzania kategorii danych:
zwykłe
o naruszeniach prawa
wrażliwe
możliwości nałożenia kary
możliwości wszczęcia postępowania karnego
Suma
Ustalony poziom ryzyka na podstawie dokonanej oceny
Niski (1)
Średni (2)
Wysoki (3)
Redukcja ryzyka
Przyjęty poziom ryzyka przez komendanta
Niski (1)
Średni (2)
Wysoki (3)
Uwagi
1.
2.
Przegląd raportu
Uwagi
Data i czytelny podpis osoby dokonującej przeglądu

Wzór Rejestru zasobów krytycznych w Straży Gminnej (Miejskiej) w […]										
Lp.	Nazwa krytycznego zasobu	Stopień krytyczności zasobu	Lokalizacja zasobu	Właściciel usługi/zasobu	Sposób postępowania w przypadku awarii	Sposób postępowania w przypadku całkowitej utraty zasobu	Osoba odpowiedzialna	Numer umowy SLA	Zaplanowane środki finansowe w celu realizacji zadania	Zastępstwo osoby odpowiedzialneje
				Dane kontaktowe			Dane kontaktowe	Czas reakcji		Dane kontaktowe
1.										
2.										
Przegląd rejestru										
Data i czytelny podpis osoby dokonującej przeglądu				Uwagi						
Strona 1 z 10										

[…], […].[…].20[…] r.

Numer raportu: […].20[…]

Skład zespołu:

1. ..... – imię i nazwisko/ organizacja/ funkcja
2. ..... – imię i nazwisko/ organizacja/ funkcja

RAPORT
z przeglądu planów ciągłości działania w Straży Gminnej (Miejskiej) w […]

Proces objęty przeglądem : .....
Oznaczenie procesu (zgodnie z mapą procesów) .....

1. Sprawdzeniu poddano:
   a. uprawnienia nadzorującego ciągłość działania:
      • ..... ;
   b. dokumentacje:
      • ..... ;
   c. model oceny ryzyka:
      • ..... ;
   d. metodykę planu odtworzeniowego:
      • ..... ;
   e. środki zabezpieczenia technicznego:
      • ..... ;
   f. środki zabezpieczenia organizacyjnego:
      • ..... ;
   g. terminowość przeglądów i napraw:
      • ..... ;
   h. stan zabezpieczeń:
      • ..... ;
   i. kompletność zaplanowanych działań:
      • ..... ;

j. adekwatność zaplanowanych działań i metod odtworzeniowych:
   • ..... ;
k. skuteczność działań i metod odtworzeniowych:
   • ..... ;
l. czasy odtworzeniowe:
   • ..... ;

Ujawnione nieprawidłowości:
1. ..... ;
Osoba odpowiedzialna za nieprawidłowości:
1. ..... ;
Podjęte działania doraźne w ramach przeglądu:
1. ..... ;
Rekomendowane działania naprawcze:
1. ..... ;

Na tym raport w dniu [...] o godz. [...] zakończono.
Data i podpisy członków zespołu:
1. .....
2. .....

Data przekazania protokołu komendantowi: .....
Forma przekazania protokołu komendantowi: .....
Data i podpis osoby, która dokonała przekazania:
.....

Polecenie komendanta:
1. .....
Data i podpis komendanta
.....

Rejestr przeglądów planów ciągłości działania w Straży Gminnej (Miejskiej) w […]

Lp.	Proces poddany przeglądowi	Oznaczenie procesu zgodnie z mapą procesów	Data przeglądu	Uczestnicy przeglądu	Ocena dokumentacji	Ocena wdrożonych procedur	Ujawnione nieprawidłowości	Osoba odpowiedzialna na nieprawidłowości	Podjęte działania zaradcze	Rekomendowane działania naprawcze	Planowany termin przeglądu	Uwagi
1.												
2.												
3.												

Przegląd rejestru

Data i czytelny podpis osoby dokonującej przeglądu

Uwagi

UMOWA O WSPÓŁADMINISTROWANIE
NR […].20[…]
(UMOWA)

zawarta dnia ..... w ..... , pomiędzy:

..... z siedzibą w ..... ,
adres ....., NIP ....., REGON ....., ,
reprezentowanego przez: .....
(Współadministrator wiodący)
a
..... z siedzibą w ..... ,
adres ..... , NIP ..... , REGON ....., ,
reprezentowanego przez: .....
(Współadministrator)

każda zwana także Stroną oraz łącznie zwanymi Współadministratorami lub Stronami,

Mając na uwadze, że:

1. Strony wspólnie ustalają cele oraz sposoby przetwarzania danych osobowych, których zakres określiły w:
   a. umowie .....
      zawartej na potrzeby realizacji zadań ok,reślonych w:
   b. art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 1990 r.16.95 ze zm.);
   c. art. 50a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 1990 r.16.95 ze zm.);
      oraz
   d. art. 11 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) w zw. z ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125) (USTAWA);
      na zasadzie współadministrowania w rozumieniu:

e. art. 33 USTAWY oraz art. 26 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 (RODO).

2. Współadministratorzy mają świadomość niezbędności wypełnienia obowiązków prawnych ciążących na nich na mocy RODO oraz USTAWY.

3. Celem niniejszej UMOWY jest określenie odpowiedniego zakresu obowiązków Współadministratorów oraz relacji pomiędzy Współadministratorami oraz Współadministratorami a podmiotami, których dane dotyczą, w tym określenie zakresu i sposobu obsługi przez Współadministratorów żądań osób, których dane dotyczą oraz realizacji obowiązków, o których mowa w art. 13 i art. 14 RODO oraz art. 22 USTAWY.

Strony postanowiły zawrzeć Umowę o następującej treści:

§ 1 Opis współadministrowania

1. Na warunkach określonych niniejszą Umową Strony określają odpowiedni zakres swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO i USTAWY.

2. Cel i sposób przetwarzania przez Współadministratorów danych osobowych wynika z niniejszej Umowy oraz Umowy o sygnaturze ..... zawartej w dniu ..... na ..... .

3. Strony ustaliły, że:

a. wspólnym celem przetwarzania danych osobowych jest:

• ..... ;

b. dane osobowe przetwarzane są w następujący sposób:

• ..... .

4. Rodzaje danych osobowych przetwarzanych przez Współadministratorów określa **Załącznik nr 1**. Rodzaj przetwarzanych danych osobowych.

5. Kategorię osób przetwarzanych przez Współadministratorów określa **Załącznik nr 2**. Kategoria osób.

§ 2 Obowiązki Współadministratorów

1. Obowiązki względem osób, których dane dotyczą, obejmujące obowiązek informacyjny i realizacje praw jednostki (Prawa jednostki), wykonywane będą przez Współadministratora wiodącego. Jeśli osoba objęta współadministrowaniem skieruje swoje żądanie do Współadministratora, ten przekaże je niezwłocznie, lecz nie później niż w ciągu 24 godzin Współadministratorowi wiodącemu, a także niezależnie rozpocznie czynności w celu realizacji żądania, jeżeli taka potrzeba wynika z treści wniesionego żądania.
2. Strony ustalają rolę i zakres w realizowaniu obowiązków wynikających z RODO i USTAWY w niniejszy sposób:
   a. Współadministratorzy oświadczają, że przetwarzają dane osobowe zgodnie z zasadami określonymi w art. 5 RODO oraz art. 31 USTAWY.
   b. Współadministrator wiodący przechowuje wszelką dokumentację dotyczącą współadministrowania, dla potrzeb spełnienia wymogu rozliczalności.
   c. Współadministratorzy oświadczają, że przetwarzają dane osobowe wyłącznie w przypadkach i zakresie, w jakim zachodzi jedna z podstaw przetwarzania wskazana w art. 6 lub 9 RODO bądź 13–14 USTAWY.
   d. Współadministratorzy nie przekazują danych osobowych poza EOG.
   e. Planując dokonanie zmian w sposobie przetwarzania danych osobowych, Strony mają obowiązek:
      - zastosować się do wymogu projektowania ochrony danych, o którym mowa w art. 25 RODO;
      - informować z wyprzedzeniem Strony o planowanych zmianach w taki sposób i w takich terminach, z zastrzeżeniem art. 3 i art. 26 USTAWY, aby zapewnić Stronom realną możliwość reagowania, jeżeli planowane przez Stronę zmiany w opinii przynajmniej jednej ze Stron grożą uzgodnionemu poziomowi bezpieczeństwa danych osobowych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych osobowych przez Stronę planującą zmianę.
   f. Strony zobowiązują się do ograniczenia dostępu do danych osobowych wyłącznie do osób, których dostęp do danych osobowych jest potrzebny dla realizacji Umowy.
   g. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, które posiadają upoważnienie oraz zobowiązane są do zachowania danych osobowych w tajemnicy.

h. Każdy Współadministrator zobowiązuje się do prowadzenia i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych, w tym Rejestru Czynności Przetwarzania Danych (RCPD) w rozumieniu art. 30 RODO i Rejestru Kategorii Czynności Przetwarzania (RKPD) w rozumieniu art. 35 USTAWY. Każda ze Stron obowiązana jest udostępnić niezwłocznie na każde żądanie drugiej Strony prowadzony RCPD i RKPD objętych współadministrowaniem.

i. Każdy ze Współadministratorów zapewnia ochronę danych osobowych i podejmuje środki ochrony danych osobowych, o których mowa w art. 32 RODO i art. 32 USTAWY zgodnie z dalszymi postanowieniami Umowy.

j. Każdy ze Współadministratorów wyznaczył Inspektora Ochrony Danych (IOD).

k. Współadministratorzy zapewniają, że osoby dopuszczone do przetwarzania danych osobowych zostały uprzednio przeszkolone z zasad i przepisów o ochronie danych osobowych oraz konsekwencji ich naruszenia, w tym w szczególności z procedury zabezpieczenia danych osobowych oraz swoich rolach w tym zakresie.

l. Współadministratorzy informują osoby, których dane dotyczą o współadministrowaniu oraz o zasadniczej treści wspólnych uzgodnień określonych w niniejszej Umowie, a w szczególności o relacji pomiędzy Stronami, relacji pomiędzy Stronami a osobami, których dane dotyczą oraz o zakresie obowiązków każdej ze Stron. Ujawnienie informacji o współadministrowaniu oraz o zasadniczej treści wspólnych uzgodnień powinno nastąpić przy pozyskaniu danych osobowych na potrzeby współadministrowania. Informacja o zasadniczej treści wspólnych uzgodnień Współadministratorów może stanowić część obowiązku informacyjnego realizowanego zgodnie i na podstawie art. 13 i art. 14 RODO oraz art. 22 USTAWY. Informację o wspólnej treści uzgodnień Współadministratorów stanowi **Załącznik nr 3**.

m. Strony uzgadniają, że w przypadku naruszenia ochrony danych osobowych, Współadministrator wiodący jest odpowiedzialny za zgłoszenie naruszenia organowi nadzorczemu. Strony zobowiązują się do współpracy w zakresie wypełniania obowiązków związanych z naruszeniem ochrony danych osobowych, zgodnie z dalszymi postanowieniami UMOWY.

n. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Współadministrator

wiodący bez zbędnej zwłoki zawiadamia osobę, której dane osobowe dotyczą o takim naruszeniu. Strony zobowiązują się do współpracy w zakresie wypełniania obowiązków związanych z naruszeniem ochrony danych osobowych, zgodnie z dalszymi postanowieniami UMOWY.

§ 3 Powierzenie przetwarzania

1. Każda ze Stron może powierzyć przetwarzanie danych osobowych (Powierzenie) innemu podmiotowi przetwarzającemu (Przetwarzający) w drodze pisemnej umowy powierzenia przetwarzania danych osobowych (Umowa Powierzenia). W takiej sytuacji Strona powierzająca ma obowiązek przeprowadzić audyt sprawdzający i dopilnować realizacji obowiązków związanych z powierzeniem przetwarzania danych osobowych wynikających z RODO i USTAWY oraz poinformować Strony o tożsamości Przetwarzającego w wymaganym zakresie.
2. Lista zaakceptowanych przez Współadministratorów podmiotów przetwarzających stanowi **Załącznik nr 4**. Lista zaakceptowanych Przetwarzających.
3. Każda ze Stron może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia danych osobowych konkretnemu Przetwarzającemu. W razie zgłoszenia sprzeciwu Strona powierzająca nie ma prawa powierzyć przetwarzania danych osobowych Przetwarzającemu objętemu sprzeciwem. Strony mogą zgłosić sprzeciw także względem wcześniej zaakceptowanego Przetwarzającego. Wtedy Strona powierzająca musi niezwłocznie zakończyć Powierzenie objęte sprzeciwem. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Strona powierzająca zgłosi Stronie sprzeciwiającej się w czasie umożliwiającym zapewnienie ciągłości przetwarzania i uzgodnienie rozwiązań alternatywnych.

§ 4 Bezpieczeństwo danych osobowych

1. Każdy ze Współadministratorów przeprowadził własną analizę ryzyka przetwarzania danych osobowych i stosuje się do jej wyników co do organizacyjnych i technicznych środków ochrony danych osobowych odpowiadających ustalonemu ryzyku naruszenia praw i wolności osób, których dane osobowe dotyczą. Strony aktualizują swoją analizę ryzyka przetwarzania danych osobowych stosownie do potrzeb i wymogów RODO oraz USTAWY i informują pozostałe Strony o wynikach aktualizacji.

2. Strony potwierdzają, że poziom zabezpieczeń danych osobowych stosowany przez każdą ze Stron odpowiada ryzyku ustalonemu w wyniku analizy ryzyka, o której mowa w poprzednim ustępie. W szczególności każda Strona oceniła, poinformowała Strony i zobowiązuje się do aktualizowania informacji o zasadności i stosowanych technicznych i organizacyjnych środkach ochrony danych osobowych w zakresie:

a. pseudonimizacji i szyfrowania danych osobowych;
b. zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych osobowych;
c. zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d. regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

3. Jeżeli planowany rodzaj przetwarzania danych osobowych objęty współadministrowaniem – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Strony każdorazowo uzgodnią zasady współdziałania przy ocenie skutków planowanych operacji przetwarzania dla ochrony danych osobowych w rozumieniu art. 35 RODO.

§ 5 Czasy reakcji

1. Współadministrator zapewnia, że powiadomi Współadministratora wiodącego o każdym podejrzeniu naruszenia ochrony danych osobowych w terminie 12 godzin od zgłoszenia podejrzenia. Jeżeli prawdopodobieństwo naruszenia jest wysokie, umożliwia Współadministratorowi wiodącemu uczestnictwo w czynnościach wyjaśniających oraz, niezależnie, Współadministrator informuje pozostałe Strony (o ile występują) o stwierdzeniu lub wykluczeniu naruszenia w ciągu 12 godzin od dokonania takich ustaleń.

2. Zgłoszenie naruszenia organowi nadzorczemu dokonywane będzie przez Współadministratora wiodącego. Jeżeli naruszenie ochrony danych dotyczy Strony, która je stwierdziła, Strona ta bezzwłocznie opracowuje treść zgłoszenia.

3. Współadministrator wiodący prowadzi rejestr stwierdzonych naruszeń ochrony danych osobowych, w którym odnotowuje fakt powstania naruszenia, do którego doszło w ramach współadministrowania.

4. Współadministrator powiadamia Współadministratora wiodącego w ciągu 24 godzin o każdym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a w szczególności przepisów postępowania karnego lub przepisów dotyczących zapobiegania terroryzmowi lub praniu pieniędzy.
5. Współadministrator powiadamia Współadministratora wiodącego w ciągu 24 godzin o każdym otrzymanym żądaniu wykonania Prawa jednostki oraz przesyła w sposób bezpieczny wszelką niezbędną dokumentację dotyczącą wykonania Prawa jednostki, aby umożliwić Współadministratorowi wiodącemu poprawną realizację Praw jednostki.
6. Współadministratorzy ustalą sposoby komunikacji i osoby odpowiedzialne u wszystkich Współadministratorów w taki sposób, aby pewne było dotrzymanie terminów, o których mowa wyżej, w szczególności poprzez wymóg potwierdzenia odbioru i redundancję kanałów komunikacji i osób wyznaczonych do komunikacji u wszystkich Współadministratorów.

§ 6 Osoby kontaktowe

1. IOD pełni funkcję osoby kontaktowej dla potrzeb komunikacji dotyczącej naruszeń ochrony danych osobowych i dla osób, których dane osobowe dotyczą, dla Współadministratorów, jak i na potrzeby innych spraw związanych z ochroną danych osobowych.
2. IOD wyznaczonym u Współadministratora wiodącego jest .... , z którym należy się skontaktować pod numerem telefonu: ....., e-mail ..... .
3. IOD wyznaczonym u Współadministratora jest ..... , z którym należy się skontaktować pod numerem telefonu: ..... , e-mail ..... .
4. Wszelka komunikacja Stron związana z realizacją Umowy kierowana jest do IOD.

§ 7 Odpowiedzialność

1. Każdy ze Współadministratorów podlega środkom prawnym i sankcjom określonym w art. 77–79 oraz art. 82–84 RODO (odpowiedzialność solidarna) oraz art. 53–55 USTAWY. W rozliczeniach wzajemnych (regresy) Strony posługują się zasadą winy. Jeżeli jednak żadnej ze Stron nie można przypisać winy

lub stopień winy jest podobny, podział odpowiedzialności będzie dokonywany w częściach równych.

§ 8 Okres obowiązywania Umowy

1. Umowa zostaje zawarta na czas realizacji Umowy o sygnaturze ..... z dnia ..... .
2. Umowa może zostać wypowiedziana za jednomiesięcznym wypowiedzeniem upływającym na koniec ostatniego dnia następnego miesiąca.

§ 9 Postanowienia końcowe

1. Umowa zawiera następujące załączniki:
   a. Załącznik nr 1
      Rodzaj przetwarzanych danych osobowych;
   b. Załącznik nr 2
      Kategoria osób;
   c. Załącznik nr 3
      Wspólne uzgodnienia Współadministratorów;
   d. Załącznik nr 4
      Lista zaakceptowanych Przetwarzających.
2. Umowa wchodzi w życie z dniem jej podpisania przez Strony.
3. Wszelkie zmiany lub uzupełnienia Umowy wymagają zachowania formy dokumentowej pod rygorem nieważności.
4. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacją Umowy jest sąd właściwy dla siedziby Współadministratora wiodącego.
5. Umowę sporządzono po jednym egzemplarzu dla każdej ze Stron.
6. Umowa podlega RODO i USTAWIE oraz prawu polskiemu, w tym w szczególności przepisom Kodeksu cywilnego.

.....	.....
Data i czytelny podpis	Data i czytelny podpis

Załącznik nr 1

Rodzaj przetwarzanych danych osobowych
Np.:
Podstawowe dane identyfikacyjne;
Informacje dotyczące skazań i wyroków!;
Informacje dotyczące działań sądowych;
Dane dotyczące zamieszkania;
Dane dotyczące zdrowia fizycznego;
Dane dotyczące zdrowia psychicznego;
Zawód i zatrudnienie;
Aktualne zatrudnienie;
Wynagrodzenie;
Nagrania wideo;
Wizerunek.

Załącznik nr 2
Kategoria osób
Np.:
Świadkowie;
Podejrzani;
Pracownicy;
Obsługa;
Dostawcy;
Odwiedzający;
Inne.

Załącznik nr 3
Informacja o zasadniczej treści wspólnych uzgodnień Współadministratorów

Współadministrator wiodący i Współadministrator wspólnie administrują dane osobowe w następującym celu:

1. zawarcia i realizacji umowy na ..... ,
   na potrzeby realizacji zadań określonych w:
   a. art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 1990.16.95 ze zm.)
   oraz

b. art. 11 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) w zw. z ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) (USTAWA);

2. ustalenia, dochodzenia lub obrony ewentualnych roszczeń pomiędzy Panią/Panem a Współadministratorem wiodącym lub Współadministratorem, co jest prawnie uzasadnionym interesem Współadministratora wiodącego i Współadministratora.

Załącznik nr 4
Lista zaakceptowanych Przetwarzających
1. .....
2. .....

UMOWA POWIERZENIA PRZETWARZANIA
NR […]20[…]
(UMOWA)

zawarta dnia ..... w ....., pomiędzy:

..... z siedzibą w ..... ,
adres ..... , NIP ..... , REGON ..... ,
reprezentowanego przez: .....
(Administrator/ Zamawiający)
a
..... z siedzibą w ..... ,
adres ..... , NIP ..... , REGON ..... ,
reprezentowanego przez: .....
(Przetwarzający/ Wykonawca)

każda zwana także Stroną lub Stronami

Mając na uwadze, że:

1. Zamawiający oświadcza, że jest administratorem danych osobowych w rozumieniu przepisów:
   1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (RODO);
   2) ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) (USTAWA),

   powierzonych do przetwarzania na podstawie niniejszej UMOWY w celu realizacji umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ... ,
2. Przetwarzający zapewnia, że:
   1) posiada wdrożone – po uprzedniej identyfikacji ryzyk, ich analizie i uwzględnieniu wyznaczników zawartych:

a) w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2005.64.565 ze zm.)
oraz
b) 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 (Dz.U.2012.526)
adekwatne środki techniczne oraz organizacyjne, które zapewniają bezpieczeństwo powierzonym przez Administratora danym zgodnie z wymogami art. 32 RODO i art. 34 USTAWY.

2) stosuje się do wymogów:
a) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);
b) ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U.2018.723 ze zm.);
c) ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. 1994.121.591 ze zm.);
d) ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. 1974.24.141 ze zm.);

3) powierzone dane będą przetwarzały wyłącznie osoby, które zostały przeszkolone z bezpieczeństwa informacji, w tym ochrony danych osobowych, oraz zobowiązane do zachowania tajemnicy, a także działające z pisemnego upoważnienia Administratora.

3. Celem UMOWY jest ustalenie warunków, na jakich Przetwarzający może wykonywać operacje przetwarzania danych osobowych w imieniu Administratora.

4. Strony, zawierając UMOWĘ, mają na celu szczegółowe uregulowanie zasad przetwarzania danych osobowych, aby odpowiadały wszelkim obowiązkom przewidzianym prawem, w tym przepisom RODO i USTAWY

– Strony postanowiły zawrzeć UMOWĘ o następującej treści:

§ 1

1. Na warunkach określonych niniejszą UMOWĄ Administrator powierza Przetwarzającemu przetwarzanie dalej opisanych danych osobowych wyłącznie

w celu realizacji Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... .

2. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy podstawowej, z uwzględnieniem pozostałych postanowień niniejszej UMOWY oraz przepisów prawa, po czym przetwarzane dane zostaną usunięte, chyba że przepisy prawa zezwalają na dalsze ich przetwarzanie.

3. Charakter i cel przetwarzania powierzonych danych wynikają z zawartej Umowy, o której mowa w preambule niniejszej UMOWY oraz pkt 1.

4. Przetwarzanie obejmować będzie wszystkie rodzaje i kategorie danych osobowych, które zostały określone w Załączniku nr 1. Rodzaje powierzonych danych i Załączniku nr 2. Kategorie powierzonych danych, a zakres których jest niezbędny do prawidłowej realizacji zawartej Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... .

5. Administrator w zakresie przetwarzania, o którym mowa w pkt 4 deleguje uprawnienie na Przetwarzającego do:

1) nadawania upoważnień personelowi przetwarzającego dane w imieniu Przetwarzającego;
2) wydawania wiążących poleceń w zakresie przetwarzania danych.

§ 2

1. Zasadą jest, że Przetwarzający może powierzyć operacje przetwarzania danych (Dalszy przetwarzający), w drodze pisemnej umowy dalszego przetwarzania (Umową dalszego przetwarzania), innym Przetwarzającym (Dalsi przetwarzający).

2. Powierzenie przetwarzania danych Dalszemu przetwarzającemu wymaga uprzedniego zgłoszenia tego faktu Administratorowi w terminie 7 dni roboczych przed ich powierzeniem.

3. Administrator może zgłosić udokumentowany sprzeciw względem powierzenia danych konkretnemu Dalszemu przetwarzającemu. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć danych Dalszemu przetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Dalszego przetwarzającego musi niezwłocznie zakończyć Dalsze przetwarzanie przez ten podmiot.

4. Wątpliwości co do zasadności sprzeciwu Administratora i ewentualnych skutków, a tym samym negatywnych konsekwencji, Przetwarzający winien zgłosić Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania Stronom.
5. Dokonując Dalszego przetwarzania, Przetwarzający ma obowiązek zobowiązać Dalszego przetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z UMOWY, z wyjątkiem tych, które nie dotyczą konkretnego Dalszego przetwarzania.
6. Przetwarzający ma obowiązek zapewnić, aby Dalszy przetwarzający przed rozpoczęciem przetwarzania:
   a) został sprawdzony przez Przetwarzającego pod kątem wymagań stawianych przez Administratora w zakresie ochrony danych;
   b) daje gwarancje skutecznej ochrony powierzonych mu danych;
   c) efektywnie realizuje w szczególności obowiązki, o których mowa w art. 24, art. 25, art. 30 i art. 32 RODO oraz art. 31, art. 32 i art. 34 USTAWY.
7. Przetwarzający niezwłocznie po sprawdzeniu, o którym mowa w pkt 6, udostępnia Administratorowi kopię protokołu wraz z wnioskami końcowymi dokonującego sprawdzenia. Administrator przechowuje dokument z UMOWĄ.
8. Listę Dalszych przetwarzających, uprzednio sprawdzonych przez Przetwarzającego pod kątem spełniania w szczególności wymagań, o których mowa w art. 31, art. 32 i art. 34 USTAWY, zaakceptowanych przez Administratora, zawiera **Załącznik nr 3**. Lista zatwierdzonych Dalszych przetwarzających.
9. Wszelkie koszty powstałe z przeprowadzenia uprzedniego sprawdzenia Dalszego przetwarzania pod kątem spełniania wymagań określonych w UMOWIE z uwzględnieniem wymagań prawnych w niej wskazanych ponosi wyłącznie Przetwarzający.

§ 3

1. Przetwarzający zobowiązany jest do:
   1) przetwarzania danych zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora, do których zaliczyć należy zawartą Umowę o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... ;

2) nieprzekazywania danych do państwa trzeciego lub organizacji międzynarodowej, czyli poza Europejski Obszar Gospodarczy (zwany dalej EOG), oraz niekorzystania z podwykonawców, którzy przekazują dane poza EOG, chyba że wynika to z obowiązku prawnego;
3) informowania Administratora o zamiarze lub obowiązku przekazywania danych poza EOG z należytym wyprzedzeniem, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub do zakończenia powierzenia przetwarzania;
4) informowania Administratora, o ile prawo mu tego nie zabrania, przed rozpoczęciem przetwarzania o obowiązku prawnym dotyczącym przetwarzania, jeżeli prawo nakłada na Przetwarzającego obowiązek ochrony danych w celu realizacji tego obowiązku;
5) uzyskania od osób, które zostały upoważnione do przetwarzania danych w wykonaniu Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... , udokumentowanego zobowiązania do zachowania tajemnicy lub ewentualnie upewnienia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy;
6) zapewnienia ochrony danych i podejmowania środków ochrony danych, o których w szczególności mowa w art. 24, art. 25, art. 30 i art. 35 RODO oraz art. art. 31, art. 32 i art. 34 USTAWY, zgodnie z dalszymi postanowieniami UMOWY;
7) przestrzegania warunków korzystania z usług Dalszego przetwarzającego;
8) zapewnienia współpracy przy obsłudze wykonywania praw podmiotu, których dane dotyczą;
9) współpracy z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych, w szczególności w zakresie prawidłowości zgłaszania naruszeń organowi nadzorczemu, zawiadamiania osób dotkniętych naruszeniem ochrony danych, dokonywania oceny skutków dla ochrony danych, a także realizowania uprzednich konsultacji z organem nadzorczym, o ile taka konieczność wystąpi;
10) natychmiastowego informowania Administratora o powzięciu przez Przetwarzającego wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji (w sposób udokumentowany

i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu;

11) zastosowania się do wymogu projektowania prywatności przy planowaniu zmian w sposobie przetwarzania danych oraz do informowania Administratora z wyprzedzeniem o planowanych zmianach – w taki sposób i w takich terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa danych lub zwiększają ryzyko naruszenia praw lub wolności osób wskutek przetwarzania danych przez Przetwarzającego;

12) ograniczenia dostępu do danych poprzez przyznanie go wyłącznie tym osobom, którym dostęp do danych jest potrzebny dla realizacji Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... , i które posiadają odpowiednie upoważnienie, przeszkolenie oraz zostały zobowiązane do zachowania w tajemnicy informacji prawnie chronionych;

13) prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym Rejestru kategorii czynności przetwarzania danych (Rejestr) – Przetwarzający jednocześnie oświadcza, że prowadzi Rejestr zgodnie z wymogami ustawy, i udostępnia na żądanie Administratora prowadzony Rejestr, z wyłączeniem informacji stanowiących prawnie chronioną tajemnicę innych Przetwarzających;

14) informowania Administratora o każdym planowanym procesie zautomatyzowanego przetwarzania, w tym profilowania, dokonywanym w celu realizacji Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... , innym niż określony w tej Umowie;

15) zapewnienia, aby osoby upoważnione do przetwarzania danych otrzymały odpowiednie szkolenie z zakresu ochrony informacji, w tym ochrony danych, oraz aby podpisały zobowiązanie do zachowania w tajemnicy informacji prawnie chronionych;

16) udostępnienia:

a) kopii umów powierzenia przetwarzania danych z Dalszymi przetwarzającymi, które Przetwarzający zawarł w celu realizacji

Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... ;

b) kopii wyników uprzednich sprawdzeń/ kontroli/ audytów Dalszych przetwarzających, przeprowadzonych pod kątem spełniania wymagań, o których w szczególności mowa w art. 24, art. 25, art. 30 i art. 35 RODO oraz w art. 31, art. 32 i art. 34 USTAWY;

17) informowania, o każdym zgłoszonym lub ujawnionym przez Przetwarzającego naruszeniu ochrony danych osobowych.

§ 4

1. Przetwarzający przedkłada wykaz systemów, programów lub innych narzędzi biorących udział w przetwarzaniu, za które odpowiada, według wzoru określonego w **Załączniku nr 4**. Wykaz systemów biorących udział w przetwarzaniu.
2. W przypadku stosowania narzędzi, wobec których wymagana jest ochrona prawna wynikająca np. z licencji oraz innych wiążących i zgodnych z prawem ustaleń, Przetwarzający zobowiązuje się do niezwłocznego przedłożenia Administratorowi odpowiedniego dokumentu wykazującego uprawnienia do korzystania z takiego systemu.

§ 5

1. Administrator jest zobowiązany współdziałać z Przetwarzającym w wykonaniu niniejszej UMOWY, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, a także wywiązywać się terminowo ze swoich szczegółowych obowiązków, które mogą by określone w niniejszej UMOWIE, Umowie o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... lub w innych udokumentowanych ustaleniach Stron.
2. Administrator powiadamia inspektora ochrony danych o treści i zawarciu Umowy powierzenia.
3. Administrator, zawierając niniejszą UMOWĘ, oświadcza, że przetwarza dane zgodnie z zasadami określonymi w art. 24, art. 25, art. 30 i art. 35 RODO oraz art. 31, art. 32 i art. 34 USTAWY.

§ 6

1. Przetwarzający, w każdym czasie, na wniosek Administratora, przeprowadza dodatkową analizę ryzyka przetwarzania obejmującą powierzone dane, w zakresie organizacyjnych i technicznych środków ochrony danych, a następnie udostępnia ją Administratorowi na jego wniosek oraz przedstawia Administratorowi informację o zastosowaniu się do wyników tej analizy.

§ 7

1. Przetwarzający powiadamia Administratora o podejrzeniu naruszenia ochrony danych nie później niż w ciągu 12 godzin od jego stwierdzenia. Przetwarzający umożliwia Administratorowi, na jego żądanie, uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.
2. Powiadomienie o stwierdzeniu naruszenia powinno być skutecznie dostarczone wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzorczego.
3. Strony w **Załączniku nr 6**. Obszary współpracy przy realizacji praw jednostki, wyznaczyły obszary współpracy przy realizacji praw jednostki.

§ 8

1. Strony wyznaczyły Inspektorów ochrony danych, którzy dla potrzeb zapewnienia komunikacji w związku z realizacją UMOWY, w tym dotyczących naruszeń ochrony danych, jak i innych spaw związanych z ochroną danych osobowych.
2. Inspektorem ochrony danych u Administratora jest ..... , z którym należy się skontaktować pod numerem telefonu ..... lub za pośrednictwem adresu e-mail: ..... , nie później niż w 12 godzin od pierwszego wystąpienia podejrzenia naruszenia ochrony danych.
3. Inspektorem ochrony danych u Przetwarzającego jest ..... , z którym należy się skontaktować za pośrednictwem adresu e-mail ..... , nie później niż w ciągu 12 godzin od pierwszego wystąpienia podejrzenia naruszenia ochrony danych.

§ 9

1. W przypadku zdarzenia wyjątkowego, gdy nie jest możliwe poinformowanie inspektora ochrony danych Administratora o zdarzeniu, o którym mowa w § 8 UMOWY, Przetwarzający kontaktuje się z Administratorem za pośrednictwem ..... , z którym należy się skontaktować pod numerem telefonu ..... lub za pośrednictwem adresu e-mail ..... , nie później niż w 12 godzin od pierwszego wystąpienia podejrzenia naruszenia ochrony danych.
2. W przypadku zdarzenia wyjątkowego, gdy nie jest możliwe poinformowanie inspektora ochrony danych Przetwarzającego o zdarzeniu, które może mieć wpływ na jego zasoby informacyjne, Administrator za pośrednictwem ..... kontaktuje się z ..... , z którym należy się skontaktować pod numerem telefonu ..... lub za pośrednictwem adresu e-mail ..... , nie później niż w 12 godzin od uzyskania informacji.

§ 10

1. Zasadą jest, że Administrator kontroluje sposób przetwarzania powierzonych danych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli.
2. Administrator lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są dane, oraz do wglądu do dokumentacji i systemów IT związanych z przetwarzaniem danych Administratora.
3. Administrator jest uprawniony do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania danych oraz udostępnienia Rejestru.
4. Przetwarzający współpracuje z organem nadzorczym, tj. Urzędem Ochrony Danych Osobowych z siedzibą w Warszawie przy ulicy Stawki 2, lub innym upoważnionym organem w zakresie wykonywanych zadań.
5. Przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, o których mowa w niniejszej Umowie, oraz umożliwia Administratorowi lub upoważnionemu przez Administratora audytorowi/ osobie wyznaczonej (wskazanej) przeprowadzanie sprawdzeń, kontroli, audytów, w tym inspekcji.

6. Administrator jest zobowiązany uprzedzić Przetwarzającego o planowym sprawdzeniu, kontroli lub audycie co najmniej pięć dni roboczych przed ich rozpoczęciem, z wyjątkiem sytuacji gdy:
   a) niezbędność przeprowadzenia czynności sprawdzających wynika z potrzeby niezwłocznego zabezpieczenia dowodów lub
   b) Administrator uzyskał informację o możliwym naruszeniu zasad ochrony informacji, w tym danych osobowych, przez Przetwarzającego lub Dalszego przetwarzającego.
7. Koszty związane z przeprowadzeniem audytu, sprawdzenia lub kontroli ponosi Strona, która zleciła ich przeprowadzenie.
8. Stronie kontrolującej przysługuje prawo żądania zwrotu rzeczywistych poniesionych kosztów przeprowadzonego audytu, sprawdzania lub kontroli od Strony kontrolowanej w przypadku wykazania nieprawidłowości.
9. Audyt, sprawdzenie lub kontrola mogą zostać przeprowadzone w każdy dzień tygodnia, w tym także poza godzinami pracy Przetwarzającego, o ile wynika to z:
   a) konieczności niezwłocznego zabezpieczenia dowodów naruszenia zasad ochrony danych lub
   b) uzyskania informacji o możliwie występujących naruszeniach zasad ochrony informacji, w tym danych osobowych.
10. Ustalenia określone w pkt 1–9 odnoszą się także do Dalszego przetwarzającego, o czym Przetwarzający obowiązany jest go poinformować oraz skutecznie egzekwować.
11. Administrator w **Załączniku nr 5**. Lista kontrolna, w celu uprzedniego sprawdzenia Przetwarzającego, określił warunki wstępnej weryfikacji Przetwarzającego.
12. Listę wymagań, o których mowa w pkt 11 Administrator udostępnia Przetwarzającemu jeszcze przed zawarciem UMOWY, którą Przetwarzający obwiązany jest wypełnić zgodnie ze stanem faktycznym na dzień zawarcia Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... .
13. Przetwarzający obowiązany jest udostępnić Administratorowi do wglądu także obowiązującą na dzień zawarcia Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia

..... Politykę ochrony danych lub inny dokument określający system wraz z zasadami ochrony danych osobowych u Przetwarzającego jeszcze przed podpisaniem niniejszej UMOWY.

§ 11

1. Przetwarzający odpowiada w pełnym zakresie za szkody materialne i niematerialne spowodowane swoim działaniem lub zaniechaniem w związku z niedopełnieniem obowiązków, które ustawa nakłada bezpośrednio na Przetwarzającego, albo spowodowane działaniem poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada w pełnej wysokości za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa.
2. Jeżeli Dalszy przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora oraz osób trzecich za wypełnienie obowiązków przez Dalszego przetwarzającego spoczywa na Przetwarzającym.

§ 12

1. Umowa powierzenia zostaje zawarta na czas obowiązywania Umowy podstawowej.
2. Rozwiązanie Umowy podstawowej skutkuje rozwiązaniem Umowy i realizacją zobowiązania, o którym mowa w § 13.

§ 13

1. Po zakończeniu UMOWY Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych danych i jest zobowiązany do usunięcia powierzonych danych po upływie 14 dni od zakończenia UMOWY, chyba że Administrator postanowi inaczej na podstawie obowiązujących przepisów prawa i jest w stanie to wykazać.Sposób bezpiecznego usunięcia danych oraz sposób anonimizacji danych po zakończeniu UMOWY zostanie uzgodniony pomiędzy Stronami przed przystąpieniem do usuwania danych, o ile nie zostało to doprecyzowane już w trakcie zawierania umowy w innych umowach lub porozumieniach zawartych między Stronami w związku z realizacją Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... .

2. Po wykonaniu usunięcia danych, o którym mowa pkt 1, Przetwarzający niezwłocznie, nie później niż w terminie 14 od dnia usunięcia, złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich danych.
3. Jeżeli Przetwarzający nie może usunąć danych w wyznaczonym przez Administratora terminie ze względu na przepisy prawa, które nakazują przechowywanie tych danych w dłuższym okresie, informuje o tym pisemnie Administratora, wskazując podstawy prawne to uzasadniające.
4. Informacja, o której mowa w pkt 4, powinna zawierać zakres, rodzaj i podstawę prawną dalszego przetwarzania danych, a także zobowiązanie do zapewnienia dalszej ochrony tychże danych oraz podejmowania skutecznych środków ochrony danych, o których mowa w art. 32 RODO i art. 32 USTAWY.

§ 14

1. Treść Umowy, a także wszelkie informacje przekazywane w związku z jej realizacją przez którąkolwiek ze Stron Umowy lub osób upoważnionych ze strony Przetwarzającego do przetwarzania danych mają charakter poufny i z tego względu Strony zobowiązują się nie ujawniać tej treści osobom trzecim, chyba że:
   a) na ujawnienie tych informacji pozwala przepis prawa wskazany przez Stronę udostępniającą je drugiej Stronie lub
   b) Strony tak uzgodniły.
2. Informacje zawarte w załącznikach nr 1–5 do UMOWY stanowią tajemnicę prawnie chronioną i nie podlegają upublicznieniu, ponieważ ich upublicznienie może narazić Administratora oraz Przetwarzającego na niebezpieczeństwo utraty poufności przetwarzanych informacji.

§ 15

1. Umowa wchodzi w życie z dniem jej podpisania przez Strony.
2. W razie sprzeczności pomiędzy postanowieniami UMOWY a postanowieniami Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ....., w zakresie regulującym przetwarzanie danych, pierwszeństwo mają postanowienia niniejszej UMOWY. Oznacza to, że kwestie odnoszące się do przetwarzania danych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmianę niniejszej UMOWY lub poszczególnych jej postanowień.

3. Wszelkie zmiany lub uzupełnienia UMOWY wymagają zachowania formy pisemnej pod rygorem nieważności.
4. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacją UMOWY jest sąd właściwy dla siedziby Administratora.
5. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
6. Umowa podlega prawu polskiemu i wszystkie jej postanowienia powinny być interpretowane zgodnie z nim.
7. Obowiązek informacyjny lub model realizacji obowiązku informacyjnego, o którym mowa w art. 13 RODO i art. 22 USTAWY z uwzględnieniem prawnych wyłączeń realizacji, określa Umowa o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... (lub: Obowiązek informacyjny, o którym mowa w art. 13 RODO i art. 22 USTAWY, Strony dopełniły w dniu zawarcia Umowy o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... wobec reprezentantów Stron oraz osób uczestniczących w jej realizacji).
8. Integralną część Umowy stanowią następujące załączniki:
   1) Załącznik nr 1. Rodzaje powierzonych danych;
   2) Załącznik nr 2. Kategorie powierzonych danych;
   3) Załącznik nr 3. Lista zatwierdzonych Dalszych przetwarzających;
   4) Załącznik nr 4. Wykaz systemów biorących udział w przetwarzaniu;
   5) Załącznik nr 5. Lista kontrolna w celu uprzedniego sprawdzenia Przetwarzającego;
   6) Załącznik nr 6. Obszary współpracy przy realizacji praw jednostki.

Administrator	Przetwarzający
.....	.....

Załącznik nr 1
Rodzaje powierzonych danych
1. .....
2. .....

Załącznik nr 2

Kategorie powierzonych danych

1. .....
2. .....

Załącznik nr 3

Lista zatwierdzonych Dalszych przetwarzających

Lp.	Nazwa podmiotu	NIP	Siedziba	Osoba fizyczna/ prawna	Cel podpowierzenia	Kategoria powierzonych danych	Zakres podpowierzonych danych	Kontakt do IOD lub osoby odpowiedzialnej za ochronę danych	Data uprzedniej kontroli/ audytu/ sprawdzenia	Okres obowiązywania	UWAGI
1.											

Załącznik nr 4

Lista systemów biorących udział w przetwarzaniu danych

Lp.	Nazwa systemu	Zakres przetwarzanych danych	Dostawca	Licencja	Okres ważności	Serwis	Współpracuje z systemem	Bezpieczeństwo danych w rozumieniu art. 32 RODO i art. 32 USTAWY	Rozliczalność w rozumieniu art. 5 ust. 2 RODO	Administrator systemu	UWAGI
1.											

Załącznik nr 5

Lista kontrolna w celu uprzedniego sprawdzenia Przetwarzającego

Lp.	Pytanie	TAK/NIE	Uwagi
1.	Czy Przetwarzający weryfikuje, czy przetwarza dane osobowe, które są adekwatne, stosowne i niezbędne do celów, dla których są przetwarzane?		
2.	Czy Przetwarzający przetwarza dane osobowe zgodnie z zasadami bezpieczeństwa danych osobowych, w tym zapewnia ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych i jest w stanie to wykazać?		
3.	Czy pracownicy Przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych, zostali zobowiązani do zachowania poufności?		
4.	Czy Przetwarzający stosuje procedury i mechanizmy weryfikacji prawidłowości przetwarzanych danych, w tym umożliwia ich aktualizację osobom, które są ich właścicielem?		
5.	Czy Przetwarzający opracował zasady ustalania granic czasowych przetwarzania danych dla realizacji poszczególnych celów przetwarzania?		
6.	Czy Przetwarzający jest w stanie każdorazowo wykazać przestrzeganie zasad dotyczących przetwarzania danych osobowych, w tym czy posiada dokumentację zapewniającą realizację zasad przetwarzania?		
7.	Czy Przetwarzający weryfikuje i zapewnia możliwość efektywnego wykonania Praw Jednostki przez swoich przetwarzających?		
8.	Czy Przetwarzający przekazuje osobom prawem wymagane informacje przy zbieraniu danych osobowych?		
9.	Czy Przetwarzający informuje osobę, której dane dotyczą, o przetwarzaniu jej danych przy pozyskiwaniu tych danych?		
10.	Czy Przetwarzający informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu tych danych niebezpośrednio od danej osoby?		
11.	Czy Przetwarzający dokonuje okresowego przeglądu posiadanych danych pod kątem czasu ich przechowywania, w terminach i uzgodnionych przez niego z IOD lub inną osobą odpowiedzialną?		

12.	Czy Przetwarzający stosuje kontrolę dostępu fizycznego do pomieszczeń i urządzeń, w których przetwarzane są dane?		
13.	Czy Przetwarzający dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie Pracowników i Osób Trzecich i zmianach ról Pracowników i Osób Trzecich, oraz zmianach Dalszych Przetwarzających?		
14.	Czy Przetwarzający dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania?		
15.	Czy Przetwarzający rozpoczynając nową czynność przetwarzania, określa zakres danych niezbędnych do realizacji tej czynności?		
16.	Czy Przetwarzający w zawartych umowach powierzenia przetwarzania danych określa sposób usuwania danych z zasobów Dalszych Przetwarzających Dane lub procedurę uzgodnienia takiego sposobu, a także obowiązek protokolarnego potwierdzenia usunięcia danych przez Dalszych Przetwarzających dane?		
17.	Czy Przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/ podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?		
18.	Czy osoby przetwarzające dane osobowe zostały upoważnione do przetwarzania danych osobowych i znają zakres czynności przetwarzania danych, do których posiadają upoważnienie?		
19.	Czy Przetwarzający stosuje procedurę zarządzania upoważnieniami do przetwarzania danych (nadawanie, wycofywanie nadawanych upoważnień)?		
20.	Czy Przetwarzający opracował, prowadzi i utrzymuje Rejestr Kategorii Czynności Przetwarzania jako Podmiot Przetwarzający?		
21.	Czy Przetwarzający dokonuje sprawdzeń w zgodzie z opracowanym planem sprawdzeń?		
22.	Czy Przetwarzający zastosował środki kontroli dostępu fizycznego do budynku tylko dla autoryzowanego personelu?		
23.	Czy dostęp do pomieszczeń po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany?		

24.	Czy zastosowano mechanizm nadawania indywidualnych uprawnień do systemów IT? Czy istnieje mechanizm kontroli/ zatwierdzania/ cofania/ odbioru tych uprawnień?		
25.	Czy systemy IT zapewniają wymuszanie zmiany haseł?		
26.	Czy istnieje kontrola nadawania indywidualnych uprawnień do połączeń VPN i wifi?		
27.	Czy pracownicy są zobowiązani do stosowania polityki czystego ekranu i polityki czystego biurka?		
28.	Czy stosowane jest szyfrowanie dysków?		
29.	Czy stosowane jest szyfrowanie urządzeń mobilnych?		
30.	Czy Przetwarzający zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób wskutek przetwarzania danych?		
31.	Czy Przetwarzający przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia?		
32.	Czy Przetwarzający szczególnie planując nowe rozwiązania informatyczne, weryfikuje możliwość wykorzystania pseudonimizacji lub anonimizacji do ograniczenia dostępu do danych i zwiększenia ich bezpieczeństwa?		
33.	Czy Przetwarzający wprowadza zasady ochrony danych w przesyle (dane na laptopach, telefonach komórkowych, pendrive'ach, płytach CD, kartach pamięci, przesyłanych e-mailem), w tym w szczególności zasady co do szyfrowania lub rezygnacji z szyfrowania takich danych lub nośników, na których się znajdują?		
34.	Czy Przetwarzający tworzy kopie zapasowe danych z uwzględnieniem podstawowych zasad takich jak: zdolności przywrócenia danych z kopii zapasowych czy okresu przydatności (przechowywania) kopii zapasowych w sposób ograniczony?		
35.	Czy Przetwarzający stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Organowi Nadzorczemu w terminie?		

36.	Czy Przetwarzający przeprowadza ocenę skutków dla ochrony danych (DPIA) w rozumieniu art. 35 RODO?		
37.	Czy Przetwarzający powołał IOD oraz określił zakres jego odpowiedzialności?		
38.	Czy IOD został wyznaczony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań nałożonych przez RODO i USTAWĘ?		
39.	Czy Przetwarzający zapewnił, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych?		
40.	Czy Przetwarzający prowadzi bieżący monitoring aktywności Organu Nadzorczego w zakresie informacji dotyczących aktualnych wymagań prawych?		
41.	Czy Przetwarzający dba o to, aby przyjęty i funkcjonujący w ramach jego organizacji system ochrony danych był zgodny z obowiązującym prawem i kształtującą się praktyką w obszarze ochrony prywatności i danych i w tym celu zapewnia odpowiednie szkolenia?		
42.	Czy Przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracownika w zakresie zagadnień dotyczących ochrony danych osobowych?		
43.	Czy Przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?		
44.	Czy Przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO?		
45.	Czy Przetwarzający rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (Unia Europejska, Islandia, Lichtenstein i Norwegia) lub do organizacji międzynarodowej?		
46.	Czy Przetwarzający przekazuje dane do państwa trzeciego w ramach umowy powierzenia przetwarzania danych przy zastosowaniu standardowych klauzul umownych?		

Załącznik nr 6
Obszary współpracy przy realizacji praw jednostki

1. Administrator i Przetwarzający podejmują współpracę w ramach realizacji praw jednostki przy uwzględnieniu możliwości technicznych i organizacyjnych.
2. Prawa jednostki, których dotyczy współpraca to w szczególności prowadzenia wspólnych działań w celu zapewnienia ochrony przetwarzanym danym oraz umożliwienia
   1) sprostowania danych,
   2) uzupełnienia danych,
   3) usunięcia danych,
   4) ograniczenia przetwarzania danych,
   5) przeniesienia danych.
   6) realizacji sprzeciwu wobec przetwarzania danych,
   7) realizacji innych praw jednostki,
   8) zapewnienia poprawnej weryfikacji i możliwości wykorzystania pseudonimizacji lub anonimizacji do ograniczenia dostępu do danych i zwiększenia ich bezpieczeństwa.
3. Administrator i Przetwarzający, poza osobami wskazanymi w Umowie o świadczenie usług o sygnaturze ..... w zakresie ..... nr ..... z dnia ..... oraz UMOWIE, mogą wyznaczyć także inne osoby kontaktowe do współpracy w ramach ww. czynności. Wyznaczenie innych osób wymaga zachowania formy pisemnej.

Wzór wykazu kategorii czynności przetwarzania za które odpowiada komendant w Straży Gminnej (Miejskiej) w […]

Lp.	Nazwa kategorii czynności przetwarzania	Cele przetwarzania	Podstawa prawna przetwarzania	Systemy i programy biorące udział w przetwarzaniu danych	Niezbędność przetwarzania	Opis kategorii osób, których dane dotyczą	Informacje o stosowaniu profilowania	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione	Kategorie danych osobowych przekazanych do państwa trzeciego	Planowany termin przeglądu	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych	Uwagi
					Kategorie danych osobowych			Kategoria odbiorców, którym dane osobowe zostały lub zostaną ujawnione w państwach trzecich					
1.													
2.													
3.													

Przegląd wykazu

Data i czytelny podpis osoby dokonującej przeglądu

Uwagi

Strona 1 z 10

Wzór wykazu kategorii czynności przetwarzania danych w imieniu komendanta Straży Gminnej (Miejskiej) w […]

Lp.	Kategorie danych osobowych przetwarzanych w imieniu administratora	Nazwa czynności przetwarzania, w ramach której dochodzi do przetwarzania danych	Cele przetwarzania	Podstawa prawna przetwarzania	Niezbędność przetwarzania	Informacje o stosowaniu profilowania	Systemy i programy biorące udział w przetwarzaniu danych	Przekazywanie danych do państw poza EOG		Przekazywanie danych do USA		Planowany termin przeglądu	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych	Uwagi
								Państwo, dane kontaktowe podmiotu, cel przekazania, nazwa produktu		Dane kontaktowe podmiotu, cel przekazania, nazwa produktu					
1.															
2.															
3.															

Przegląd wykazu

Data i czytelny podpis osoby dokonującej przeglądu

Uwagi

[…], […].[…].20[…] r.

Numer protokołu: […].20[…]

Skład zespołu:

1. ..... – imię i nazwisko/ organizacja/ funkcja
2. ..... – imię i nazwisko/ organizacja/ funkcja

PROTOKÓŁ
zniszczenia informatycznych nośników danych w Straży Gminnej (Miejskiej) w […]

1. Na podstawie:
   a. ..... ;
   b. ..... ;

2. Dokonano trwałego zniszczenia następujących nośników:
   a. ..... – numer seryjny nośnika/ numer z rejestru nośników;
   b. ..... – numer seryjny nośnika/ numer z rejestru nośników.

3. Liczba zniszczonych nośników: ..... .

4. Trwałe zniszczenie nośników informatycznych nastąpiło poprzez:
   a. ..... ;
   b. ..... .

5. Liczba trwale zniszczonych nośników: ..... .

Na tym protokół w dniu […] o godz. […] zakończono.

Data i podpisy członków zespołu:
1. .....
2. .....

Data przekazania protokołu komendantowi: .....
Forma przekazania protokołu komendantowi: .....

Data i podpis osoby, która dokonała przekazania
.....

Data i podpis komendanta
.....

[…], […].[…].20[…] r.

Numer wniosku […].20[…]

Wniosek o nadanie/ odebranie* upoważnienia
do przetwarzania danych osobowych w Straży Gminnej (Miejskiej) w […]

1. Data wpłynięcia wniosku: […].[…].20[…] r.

Niniejszym wnoszę o nadanie/ odebranie* upoważnienia do przetwarzania danych osobowych:
1. ..... – imię i nazwisko osoby, której wniosek dotyczy.

Kategorie czynności przetwarzania:
1. ..... – kategorie czynności przetwarzania w oparciu o wykaz kategorii przetwarzania.

Zakres przetwarzania danych:
1. ..... – (art. 13 i/lub art. 14) ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125).

Sposób przetwarzania danych:
1. Informatyczny: w zakresie upoważnienia / nadanych dostępów do systemów teleinformatycznych.
2. Manualny (papierowy): w zakresie nadanego upoważnienia.

Cel nadania/ odebrania upoważnienia: ..... .

Okres ważności upoważnienia: ..... .

Data i czytelny podpis osoby wnioskującej: ..... .

Oświadczenie osoby, której wniosek dotyczy:

1. Zostałem/am przeszkolony/a oraz zapoznany/a z przepisami oraz dokumentacją i procedurami obowiązującymi w Straży Gminnej (Miejskiej) w […]w zakresie zapewnienia bezpieczeństwa informacji oraz ochrony danych osobowych.
2. Zobowiązuję się do zapewnienia bezpieczeństwa informacji oraz ochrony danych osobowych, do których uzyskam dostęp w trakcie wykonywania obowiązków służbowych, w tym także do ich ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
3. Zobowiązuję się do zachowania w poufności wszelkich informacji chronionych, do których otrzymam dostęp, oraz metod i sposobów ich zabezpieczenia, także po cofnięciu upoważnienia.
4. Zostałem/am pouczony/a o odpowiedzialności za niedozwolone lub niezgodne z prawem przetwarzanie danych osobowych oraz za dopuszczenie do ich przypadkowej utraty, zniszczenia lub uszkodzenia, a także za naruszenie poufności informacji o ich zabezpieczeniu.

Data i czytelny podpis osoby, której wniosek dotyczy:
.....

Data przekazania wniosku komendantowi: .....

1. Data rozpatrzenia wniosku: […].[…].20[…] r.
2. Data udzielenia upoważnienia do przetwarzania danych osobowych: […].[…].20[…] r.
3. Okres ważności upoważnienia: ..... .
4. Data odebrania upoważnienia do przetwarzania danych osobowych: […].[…].20[…] r.

Zastrzeżenia: .....
..... .

5. Data odmowy udzielenia upoważnienia do przetwarzania danych osobowych: […].[…].20[…] r.

Data i podpis komendanta

.....

Wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych w Straży Gminnej (Miejskiej) w […]												
Lp.	Imię i nazwisko osoby upoważnionej	Data udzielania upoważnienia	Imię i nazwisko osoby udzielającej upoważnienia	Okres ważności / Cel nadania		Kategoria czynności	Zakres upoważnienia	Sposób przetwarzania	Identyfikator w systemie informatycznym	Data odebrania upoważnienia / Przyczyna/ Imię i nazwisko odbierającego		Uwagi
1.												
2.												
Przegląd ewidencji												
Data i czytelny podpis osoby dokonującej przeglądu				Uwagi								
Strona 1 z 10												

Wzór Rejestru wniosków o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w Straży Gminnej (Miejskiej) w […]

Lp.	Imię i nazwisko Stanowisko	Data wpływu wniosku	Imię i nazwisko wnioskującego	Data udzielenia upoważnienia	Imię i nazwisko osoby udzielającej upoważnienia	Okres ważności Cel nadania	Kategoria czynności	Zakres upoważnienia	Sposób przetwarzania	Identyfikator w systemie informatycznym	Data odebrania upoważnienia Przyczyna/ Imię i nazwisko odbierającego	Data odmowy Przyczyna	Uwagi
1.													
2.													

Przegląd rejestru

Data i czytelny podpis osoby dokonującej przeglądu

Strona 1 z 10

[…], […].[…].20[…] r.

Inspektor Ochrony Danych
Straż Gminna (Miejska) w […]

Komendant

Straż Gminna (Miejska) w […]

Sprawozdanie
z
działań IOD w Straży Gminnej (Miejskiej) w […] za okres

Numer sprawozdania: […].20[…]

Zakres sprawozdania:

1. Informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych:
   a. ..... data, zakres, sposób realizacji i udokumentowania.
2. Prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania:
   a. .....,..... data, zakres, sposób realizacji i udokumentowania.
3. Monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych zgodnie z obowiązującymi przepisami:
   a. ..... data, zakres, sposób realizacji i udokumentowania, ujawnione nieprawidłowości, podjęte działania.
4. Monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem:

a. ..... data, podjęte działania, zakres, sposób realizacji i udokumentowania, ujawnione nieprawidłowości, podjęte działania.

5. Współpraca z Prezesem Urzędu Ochrony Danych Osobowych:
   a. ..... data, cel, podjęte działania, zakres, sposób realizacji i udokumentowania.
6. Monitorowanie realizacji zaleceń wydanych przez Prezesa Urzędu Ochrony Danych Osobowych oraz przedstawianie Prezesowi Urzędu stanu ich realizacji:
   a. ..... data, cel, podjęte działania, zakres, sposób realizacji i udokumentowania.
7. Pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu w kwestiach związanych z przetwarzaniem danych osobowych, w tym sprawach związanych z prowadzeniem uprzednich konsultacji, gdy administrator przed rozpoczęciem przetwarzania danych osobowych, które będzie częścią mającego powstać nowego zbioru danych, wykaże, że przetwarzanie danych osobowych będzie powodowało wysokie ryzyko naruszenia praw i wolności osób fizycznych w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka, lub gdy dany rodzaj przetwarzania danych osobowych stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach:
   a. ..... data, podjęte działania, zakres, sposób realizacji i udokumentowania.
8. Pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących jej praw:
   a. ..... data, podjęte działania, zakres, sposób realizacji i udokumentowania.
9. Realizowanie zadań z uwzględnieniem określonego ryzyka związanego z operacjami przetwarzania danych osobowych:
   a. ..... nazwa procesu, data oceny i szacowania ryzyka dla operacji przetwarzania danych osobowych.
10. Przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku gdy dany rodzaj przetwarzania danych osobowych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych oraz monitorowanie wykonania tych zaleceń:

a. ..... data, zakres, podjęte działania, sposób realizacji i udokumentowania.

11. Inne:

a. ..... data, zakres, podjęte działania, sposób realizacji i udokumentowania.

Na tym sprawozdanie w dniu […] o godz. […] zakończono.
Data i podpis IOD .....

Data przekazania sprawozdania komendantowi: .....
Forma przekazania sprawozdania komendantowi: .....

Data i podpis komendanta: .....

[…], […].[…].20[…] r.

Inspektor Ochrony Danych
Straż Gminna (Miejska) w […]

Komendant
Straż Gminna (Miejska) w […]

Roczne sprawozdanie
z
działań IOD w Straży Gminnej (Miejskiej) w […]
za okres od 00.00.[…] r. do 00.00.[…] r.

Numer sprawozdania: […].R.[20…]

Zakres sprawozdania:

1. Informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... .
2. Prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... ;
3. Monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych zgodnie z obowiązującymi przepisami:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... .

4. Monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... .
5. Współpraca z Prezesem Urzędu Ochrony Danych Osobowych:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... .
6. Monitorowanie realizacji zaleceń wydanych przez Prezesa Urzędu Ochrony Danych Osobowych oraz przedstawianie Prezesowi Urzędu stanu ich realizacji:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... .
7. Pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu w kwestiach związanych z przetwarzaniem danych osobowych, w tym sprawach związanych z prowadzeniem uprzednich konsultacji, gdy administrator przed rozpoczęciem przetwarzania danych osobowych, które będzie częścią mającego powstać nowego zbioru danych, wykaże, że przetwarzanie danych osobowych będzie powodowało wysokie ryzyko naruszenia praw i wolności osób fizycznych w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka, lub gdy dany rodzaj przetwarzania danych osobowych stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... .
8. Pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą, w zakresie przysługujących jej praw:
   a. liczba podjętych działań: ..... ;
   b. liczba zakończonych działań: ..... ;
   c. liczba niezakończonych działań: ..... .
9. Przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku gdy dany rodzaj przetwarzania danych osobowych,

w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych oraz monitorowanie wykonania tych zaleceń:

a. liczba podjętych działań: ..... ;
b. liczba zakończonych działań: ..... ;
c. liczba niezakończonych działań: ..... .

10. Realizowanie zadań z uwzględnieniem określonego ryzyka związanego z operacjami przetwarzania danych osobowych:

a. liczba dokonanych ocen i szacowań ryzyka dla operacji przetwarzania danych osobowych ..... ;

11. Inne:

a. liczba podjętych działań: ..... ;
b. liczba zakończonych działań: ..... ;
c. liczba niezakończonych działań: ..... .

Na tym sprawozdanie w dniu [...] o godz. [...] zakończono.
Data i podpis IOD .....

Data przekazania sprawozdania komendantowi: .....
Forma przekazania sprawozdania komendantowi: .....

Data i podpis komendanta .....

Wzór Rejestru sprawozdań z działań IOD w Straży Gminnej (Miejskiej) w [...]														
Lp.	Data wpływu sprawozdania	Imię i nazwisko sporządzającego Imię i nazwisko przekazującego	Forma przekazania	Rodzaj sprawozdania:		Okres sprawozdania	Wykazane:				Osoby odpowiedzialne	Podjęte działania	Uwagi
				miesięczne	roczne		braki	nieprawidłowości	incydenty	oceny i szacowanie ryzyka			
1.													
2.													
Przegląd rejestru													
Data i czytelny podpis osoby dokonującej przeglądu			Uwagi										
Strona 1 z 10													

Arkusz oceny ryzyka procesów przetwarzania w zakresie wydanych rekomendacji przez IOD w Straży Gminnej (Miejskiej) w […]	
Proces poddany ocenie	
Nazwa procesu:	
Dane wyjściowe	
Data oceny:	
Właściciel ryzyka:	
Zarządzający ryzykiem:	
Inne:	
Zaangażowanie administratora	
Data ujawnienia procesu	
Data poinformowania IOD o procesie	
Forma powiadomienia	
Podjęte działania przez administratora przed powiadomieniem IOD	
Inne	
Zasoby	
Sprzęt IT	
Systemy	
Oprogramowanie	
Sieć	

Personel	
Pomieszczenia	
Inne	
Informacje	
Podstawa przetwarzania	
Cel przetwarzania	
Niezbędność przetwarzania	
Kategoria	
Rodzaj	
Zakres	
Dostępność	
Dane osobowe	
Podstawa przetwarzania	
Cel przetwarzania	
Niezbędność przetwarzania	
Kategoria	
Rodzaj	
Zakres	
Dostępność	

Zidentyfikowane zagrożenia zewnętrzne	
Kategoria	
Źródło	
Przyczyna	
Następstwa	
Działania umyślne	
Działania nieumyślne	
Przyroda	
Poufność	
Integralność	
Dostępność	
Niezaprzeczalność	
Inne	
Zidentyfikowane zagrożenia wewnętrzne	
Kategoria	
Źródło	
Przyczyna	
Następstwa	
Działania umyślne	
Działania nieumyślne	

Przyroda	
Poufność	
Integralność	
Dostępność	
Niezaprzeczalność	
Inne	
Zagrożenia szczątkowe	
Kategoria	
Źródło	
Przyczyna	
Następstwa	
Działania umyślne	
Działania nieumyślne	
Przyroda	
Poufność	
Integralność	
Dostępność	
Niezaprzeczalność	
Inne	


Istniejące zabezpieczenia organizacyjne
Istniejące zabezpieczenia techniczne
Braki w istniejących zabezpieczeniach technicznych
Braki w istniejących zabezpieczeniach organizacyjnych
Ocena procesu
Treść wydanej rekomendacji lub zalecenia
Data wydanej rekomendacji

Forma i sposób przekazania rekomendacji	
Data i podpis IOD:	
Przegląd arkusza	
Data i czytelny podpis osoby dokonującej przeglądu:	Uwagi
Strona 1 z 10	

Rejestr przeprowadzonych ocen ryzyka procesów przetwarzania w zakresie wydanych rekomendacji przez IOD w Straży Gminnej (Miejskiej) w […]

Lp.	Data oceny	Nazwa procesu	Istotne ryzyka	Istota rekomendacji	Data przekazania rekomendacji	Istota decyzji komendanta	Uwagi
1.							
2.							
3.							

Przegląd rejestru

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

Strona 1 z 10

Wzór Listy obecności ze szkolenia w Straży Gminnej (Miejskiej) w […]																
Lp.	Nazwisko	Imię	Stanowisko	Data szkolenia	Miejsce szkolenia	Forma szkolenia	Zakres szkolenia	Uczestniczył		Egzamin		Przeprowadzający:		Godzina:		Uwagi
								TAK	NIE	Zdał	Nie zdał	szkolenie	egzamin	rozpoczęcia	zakończenia	
1.																
2.																
3.																
Podpis przeprowadzającego szkolenie								Podpis przeprowadzającego egzamin								
Przegląd listy																
Data i czytelny podpis osoby dokonującej przeglądu					Uwagi											
Strona 1 z 1																

Administratorem danych przetwarzanych w celu przeszkolenia i przeegzaminowania jest komendant straży gminnej (miejskiej) w […]

Regulamin określa zasady funkcjonowania monitoringu wizyjnego na terenie gminy […].

§ 1

Użyte w Regulaminie określenia oznaczają:

1. „Monitoring" lub „system monitoringu" – system monitoringu wizyjnego na terenie gminy […]. W skład systemu monitoringu wizyjnego wchodzą kamery, rejestratory oraz inne zasoby umożliwiające rejestrację oraz udostępnianie obrazu, a także systemu umożliwiające anonimizację danych osobowych utrwalonych na nagraniu.
2. „Administrator" – Wójt Gminy […].
3. „Współadministrator" – Komendant Straży Gminnej (Miejskiej) w […].
4. „Operator" – Straż Gminna (Miejska) w […].
5. „Nagranie" – materiał w formie nagrania obrazu uzyskany z wykorzystaniem systemu monitoringu.
6. „Kamera" – część systemu monitoringu.

§ 2

1. Cele i podstawy prawne zastosowania monitoringu:
   a. utrwalanie dowodów popełnienia przestępstwa lub wykroczenia;
   b. przeciwdziałanie przypadkom naruszania spokoju i porządku w miejscach publicznych;
   c. ochrona obiektów komunalnych i urządzeń użyteczności publicznej;
   d. ochrona przeciwpożarowa i przeciwpowodziowa.
2. Monitoring wprowadzony został na podstawie:
   a. art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 1990.16.95 ze zm.);
   b. art. 50 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 1990.16.95 ze zm.);
   c. art. 11 ust.2 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. 1997.123.779 ze zm.);
   d. uchwały nr […] w sprawie monitoringu wizyjnego oraz określenia zasad współadministrowania danymi.

§ 3

1. Rejestracja zdarzeń z wykorzystaniem systemu monitoringu nie może naruszać w szczególności godności osobistej oraz prawa do prywatności i tajemnicy korespondencji.
2. Nagrania nie są rozpowszechniane publicznie.
3. System monitoringu rejestruje zdarzenia, do których dochodzi wyłącznie w miejscach publicznych.

§ 4

1. Nagrania uzyskiwane są za pośrednictwem kamer oznaczonych w miejscu, w którym są usytuowane.
2. Systemem monitoringu objęte są następujące obszary:
3. ..... .
4. W strefie objętej zasięgiem kamer znajdują się tablice z niezbędnymi informacjami dotyczącymi systemu monitoringu, których wzór stanowi **załącznik nr 1** i **załącznik nr 1.1**.

§ 5

1. System monitoringu rejestruje zdarzenia w systemie 24h na dobę.
2. Rejestracji podlega tylko obraz (bez dźwięku).
3. Nagrania zawierające dane osobowe przetwarza się wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres wyznaczony na podstawie przepisów prawa.
4. Rejestracja nagrań z kamer dokonywana jest w tzw. „ pętli”
5. Nagrania po 30 dniach są automatycznie i bezpowrotnie kasowane z wyjątkiem sytuacji, gdy w okresie poprzedzającym ich usunięcie:
    a. Operator bądź administrator powziął informacje o tym, że nagranie może stanowić dowód w postępowaniu. W takim przypadkach okres przechowywania nagrania określany jest czasem trwania prowadzonego postępowania.
    b. Operator lub administrator otrzyma wniosek o zabezpieczenie nagrania. W takim przypadku okres przechowywania nagrania wyniesie nie dłużej niż 14 dni do dnia wpłynięcia wniosku.
6. Dostęp do systemu monitoringu mają wyłącznie osoby posiadające pisemne upoważnienie wydane przez administratora oraz współadministratora.

7. Administrator i współadministrator wdrożył wymagane prawem zabezpieczenia organizacyjno-techniczne na podstawie uprzednio zidentyfikowanych zagrożeń.

§ 6

1. Nagrania mogą zostać zabezpieczone dla celów dowodowych:
   a. uprawnionym organom lub instytucjom w zakresie prowadzonych przez nie czynności procesowych;
   b. osobom fizycznym.
2. Zabezpieczenie lub udostępnienie nagrania następuje na pisemny wniosek wnioskującego, którego wzór stanowi **załącznik nr 2**.
3. Nagrania zabezpiecza i udostępnia wyłącznie Operator.
4. Wnioskujący ma prawo do zapoznania się z zabezpieczonym materiałem przed jego przekazaniem wyłącznie w obecności przedstawiciela Operatora w zakresie złożonego wniosku przy uwzględnieniu zastrzeżeń, o których mowa w pkt 5.
5. Nagrania z systemu monitoringu mogą zostać udostępnione osobom fizycznym oraz osobom trzecim na udostępnionych nośnikach, o ile nie występują przypadki wyłączające prawo dostępu do danych, o których mowa w przepisach:
   a. ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019.125 ze zm.);
   b. 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.U.UE.L.2016.119.1);
   c. ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2001.112.1198 ze zm.).
6. O niezbędności zabezpieczenia nagrań decyduje Operator oraz administrator.
7. Każdorazowe umożliwienie zapoznania z zabezpieczonym nagraniem oraz jego udostępnienie wymaga akceptacji współadministratora.

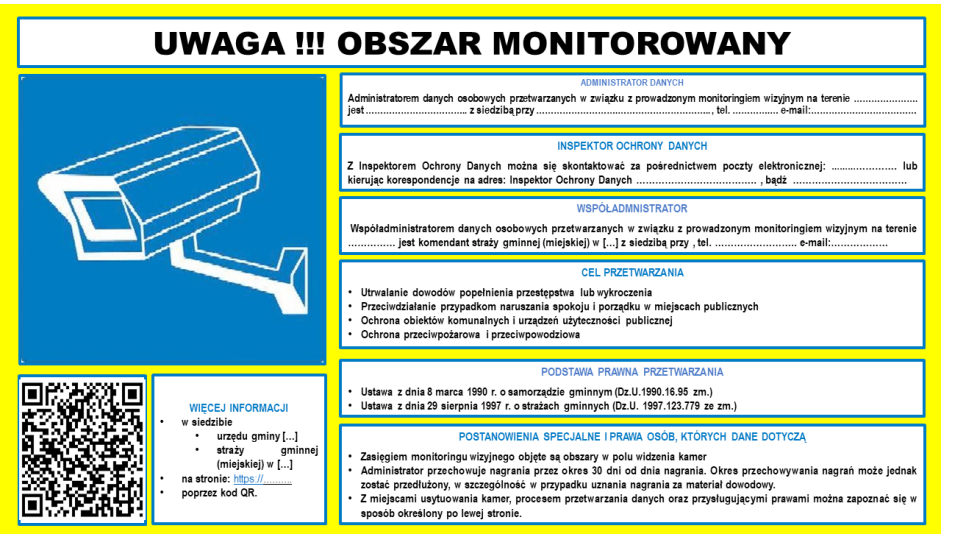
§ 7

1. Współadministrator:
   a. prowadzi Rejestr udostępnień nagrań z monitoringu wizyjnego z podziałem na kategorię danych, którego wzór stanowi **załącznik nr 3** oraz
   b. dokonuje corocznej analizy skuteczności i niezbędności prowadzenia działań z wykorzystaniem monitoringu wizyjnego na podstawie danych zawartych w Rejestrze zdarzeń odnotowanych przez Operatora stanowiący **załącznik nr 4**.
2. Operator prowadzi Rejestr zdarzeń odnotowanych za pośrednictwem systemu monitoringu wizyjnego zgodnie ze wzorem stanowiącym załącznik.

§ 8

Niniejszy Regulamin wraz z załącznikami obowiązuje od dnia jego uchwalenia.

Załącznik nr 1
Wzór tablicy informacyjnej



Załącznik nr 1.1
Wzór Klauzuli informacyjnej

Zgodnie z treścią art. 22 ust. 1 i 2 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125) w zw. z art. 10a ust. 2 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.) – zwaną dalej **Ustawą**, informuję że:

I. ADMINISTRATOR DANYCH

Administratorem Państwa danych osobowych przetwarzanych w związku z prowadzonym monitoringiem wizyjnym jest Wójt […], z którym można się skontaktować w następujący sposób:

a. listownie:
   Wójt […]
   ul. […]
   00-000 […];
b. za pośrednictwem poczty elektronicznej:
   […]@[…];
c. telefonicznie:
   +48 (71) 503 031 715 .

II. WSPÓŁADMINISTRATOR

Współadministratorem Państwa danych osobowych przetwarzanych w związku z prowadzonym monitoringiem wizyjnym jest Komendant Straży Gminnej (Miejskiej) w […], z którym można się skontaktować w następujący sposób:

a. listownie:
   Komendant Straży Gminnej (Miejskiej) w […]
   ul. […]
   00-000 […];
b. za pośrednictwem poczty elektronicznej:
   […]@[…];
c. telefonicznie:
   +48 (71) 503 031 715.

III. OPERATOR SYSTEMU

Operatorem systemu monitoringu wizyjnego jest:

1. Straż Gminna (Miejska) w [...]
   ul. [...]
   00-000 [...].
1. Kontakt:
   a. za pośrednictwem poczty elektronicznej:
      [...]@[...];
   b. telefoniczny:
      +48 (71) 503 031 715.

IV. INSPEKTOR OCHRONY DANYCH

W sprawach związanych z ochroną danych osobowych należy się kontaktować z:

Inspektorem Ochrony Danych w Urzędzie Gminy (Miejskim) w [...] p. [...]:

1. listownie:
   Inspektor Ochrony Danych
   Urząd Gminy (Miejski) w [...]
   ul. [...]
   00-000 [...];
2. za pośrednictwem poczty elektronicznej:
   [...]@[...];
   lub

Inspektorem Ochrony Danych w Straży Gminnej (Miejskiej) w [...] p.[...]:

1. listownie:
   Inspektor Ochrony Danych
   Straż Gminna (Miejska) w [...]
   ul. [...]
   00-000 [...];
2. za pośrednictwem poczty elektronicznej:
   [...]@[...];

V. CEL PRZETWARZANIA DANYCH OSOBOWYCH

Państwa dane osobowe będą przetwarzane w celu:

1. utrwalania dowodów popełnienia przestępstwa lub wykroczenia;
2. przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych;
3. ochrony obiektów komunalnych i urządzeń użyteczności publicznej;
4. ochrony przeciwpożarowej i przeciwpowodziowej.

VI. PODSTAWA PRAWNA

1. art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.1990.16.95 ze zm.);
2. art. 50 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U.1990.16.95 ze zm.);
3. art. 11 ust. 2 pkt a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U.1997.123.779 ze zm.).

VII. PRZETWARZANIE DANYCH POZA EOG

Państwa dane osobowe nie są przekazywane poza Europejski Obszar Gospodarczy.

VIII. PRAWO DO WNIESIENIA SKARGI

Każdej osobie, której dane dotyczą przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie przy ul. Stawki 2, 00-193 Warszawa, gdy uzna ona, że jej prawa zostały naruszone w wyniku przetwarzania danych osobowych przez Straż Gminną (Miejską) w [...]

Skargę można składać w następujący sposób:

1. listownie:
   Prezes Urzędu Ochrony Danych Osobowych
   ul. Stawki 2
   00-193 Warszawa;
2. za pośrednictwem elektronicznej skrzynki podawczej dostępnej na stronie WWW:
   https://www.uodo.gov.pl/pl/p/kontakt;
   a także

3. kierując skargę na adres Inspektora Ochrony Danych wskazany w pkt II.
4. kierując skargę do Wójta [...], jako organu sprawującego na mocy art. 7 ust. 2 ustawy nadzór nad działaniami Komendanta Straży Gminnej (Miejskiej) w [...], za pośrednictwem:
   a. skrzynki podawczej dostępnej na stronie WWW:
      https://epuap.gov.pl/[...];
   b. poczty elektronicznej
      [...]@[...]
      lub
   c. listownie:
      Wójt [...]
      ul. [...]
      00-000 [...];
   d. telefonicznie:
      +48 (71) 503 031 715;
   e. osobiście pod adresem wskazanym w pkt powyżej, w każdy:
      - [...], w godz. 00.00-00.00;
      - [...], w godz. 00.00-00.00.

IX. PRAWO DO ŻĄDANIA

Osoba, której dane dotyczą, posiada prawo żądania od administratora danych:

1. dostępu do danych osobowych,
2. sprostowania,
3. usunięcia danych osobowych,
4. ograniczenia przetwarzania danych osobowych.

X. Klauzula informacyjna jest dostępna:

1. na stronie WWW BIP:
   https://[...];
2. w siedzibie Straży Gminnej (Miejskiej) w [...] pod adresem wskazanym w pkt II.

Załącznik nr 2
Wzór Wniosku o zabezpieczenie i udostępnienie nagrania

[…], dnia […].[…].20[…] r.

Pozycja w rejestrze udostępnień: […]

Imię i nazwisko: .....

Dane kontaktowe: ....

Wniosek
o zabezpieczenie/ udostępnienie nagrania z monitoringu wizyjnego obszaru przy ul. .....

1. Zakres czasowy: .....
2. Obszar (umiejscowienie kamer): .....
3. Opis potencjalnie utrwalonego zdarzenia: .....
4. Cel uzyskania nagrań: .....
5. Podstawa żądania: .....

Data i czytelny podpis wnioskującego: .....

Adnotacja Operatora (strażnika):

1. Materiał zawiera następujący zakres informacji: .....
2. Kategoriadanych:.....
3. Dokonano anonimizacji z uwagi na: .....
4. Nie dokonano anonimizacji z uwagi na: .....
5. Nagranie zabezpieczono na nośniku: .....

Podpis strażnika: .....

Adnotacje Komendanta:

1. Zgoda na udostępnienie danych
2. Brak zgody na udostępnienie danych*

Uzasadnienie

1. .....

Polecenie:

2. .....

Data i podpis komendanta: .....

Adnotacja Operatora (strażnika):

1. Nagranie udostępniono na nośniku: .....
2. Udostępnione nagranie zostało zabezpieczone z uwagi na: .....

.....

3. Udostępnione nagranie nie zostało zabezpieczone z uwagi na: .....

.....

Data, podpis i stanowisko udostępniającego: .....

Załącznik nr 3

Wzór Rejestru udostępnień nagrań z monitoringu

Rejestr udostępnień nagrań z monitoringu												
Lp.	Wnioskujący	Zakres żądania	Zakres udostępniony danych	Forma udostępnienia	Dane zanonimizowane	Dane zabezpieczone kryptograficznie	Data i godzina udostępnienia	Odmowa udostępnienia	Zgoda komendanta	Udostępniający	Kategoria danych	
1.												
2.												
3.												
Przegląd rejestru:												
Data i czytelny podpis osoby dokonującej przeglądu						Uwagi:						
Strona 1 z 10												

Załącznik nr 4

Wzór Rejestru zdarzeń odnotowanych przez Operatora

Rejestr zdarzeń odnotowanych przez Operatora Straży Gminnej (Miejskiej) w [...]

Lp.	Rok	Miesiąc	Dzień	Godzina	Rodzaj zdarzenia	Miejsce zdarzenia	Podjęte czynności	Zgłaszający	Kategorie danych	Operator	Uwagi
1.											
2.											
3.											

Podsumowanie miesięczne

Liczba zdarzeń zgłoszonych		Liczba zdarzeń wykrytych samodzielnie przez Operatora:		Uwagi

Przegląd rejestru:

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

Strona 1 z 10

Wzór Rejestru zmian w Polityce ochrony danych osobowych w Straży Gminnej (Miejskiej) w […]

Lp.	Data zmiany	Przyczyna zmiany	Zakres zmiany	Podstawa prawna zmiany	Proponujący zmiany	Wprowadzający zmiany	Uwagi
1.							
2.							
3.							

Przegląd rejestru

Data i czytelny podpis osoby dokonującej przeglądu	Uwagi

Strona 1 z 10

ISBN: 978-83-64971-95-2