Załącznik do zarządzenia Nr 21
Generalnego Dyrektora Dróg Krajowych i Autostrad
z dnia 24 maja 2018 r.

POLITYKA

OCHRONY DANYCH OSOBOWYCH W GDDKIA

Rozdział 1

Postanowienia ogólne

§ 1. Polityka ochrony danych osobowych w GDDKiA, zwana dalej „Polityką", została opracowana na podstawie art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej „Rozporządzeniem".

§ 2. Ilekroć w Polityce jest mowa o:

1) Administratorze Danych – rozumie się przez to Generalnego Dyrektora Dróg Krajowych i Autostrad;
2) aplikacji - rozumie się przez to program użytkowy, konkretny - ze względu na oferowaną użytkownikom funkcjonalność, element oprogramowania użytkowego;
3) ASI – rozumie się przez to Administratorów Systemów Informatycznych, którzy są odpowiedzialni za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych i logicznych zabezpieczeń systemów informatycznych;
4) autoryzacji – rozumie się przez to proces przyznawania użytkownikowi określonych uprawnień dostępu lub korzystania z zasobów danego programu, aplikacji lub systemu;
5) Centrali – rozumie się przez to Centralę GDDKiA;
6) danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden, bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7) elektronicznym nośniku informacji - rozumie się przez to narzędzie lub urządzenie służące do zbiorowego składowania oraz odczytu zebranych informacji, w tym w szczególności: dyskietkę, płytę CD lub DVD, dysk twardy, pen drive, flash disc, aparat fotograficzny, taśmę streamera, dysk magnetooptyczny oraz taśmę magnetyczną;

8) Generalnym Dyrektorze - rozumie się Generalnego Dyrektora Dróg Krajowych i Autostrad;
9) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
10) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę uprawnioną do przetwarzania danych osobowych w systemie informatycznym;
11) integralności danych – rozumie się przez to właściwość polegającą na zapewnieniu dokładności i kompletności danych osobowych;
12) IOD – rozumie się przez to Inspektora Ochrony Danych;
13) komórce organizacyjnej Centrali – rozumie się przez to komórkę organizacyjną Centrali, o której mowa w regulaminie organizacyjnym Generalnej Dyrekcji Dróg Krajowych i Autostrad;
14) komórce organizacyjnej Oddziału – rozumie się przez to komórkę organizacyjną Oddziału, o której mowa w ramowym regulaminie organizacyjnym oddziałów Generalnej Dyrekcji Dróg Krajowych i Autostrad;
15) koordynatorze ds. ochrony danych osobowych w Oddziale – rozumie się przez to pracownika Oddziału, wyznaczonego przez Dyrektora danego Oddziału do realizacji zadań w zakresie ochrony danych osobowych;
16) naruszeniu ochrony danych osobowych - 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;
17) odbiorcy – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
18) Oddziale – rozumie się przez to Oddział GDDKiA;
19) organie nadzorczym - rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych;

20) podmiocie przetwarzającym - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
21) poufności danych – rozumie się przez to właściwość polegającą na tym, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
22) przetwarzaniu – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie ;
23) rozliczalności – rozumie się przez to rozliczalność, o której mowa w art 5 ust. 2 Rozporządzenia;
24) utrwalaniu danych – rozumie się przez to zapisywanie danych w sposób trwały na wszelkiego rodzaju nośnikach papierowych lub elektronicznych;
25) użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w GDDKiA i uprawnioną do ich przetwarzania w systemach informatycznych;
26) zasobie teleinformatycznym – rozumie się przez to system, program, aplikację lub udział sieciowy, w szczególności folder na dysku sieciowym, w którym przetwarzane są dane osobowe;
27) zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rozdział 2

Cele i zakres Polityki

§ 3. Polityka określa podstawowe zasady ochrony danych osobowych.

§ 4. Polityka ma zastosowanie wobec:

1) osób upoważnionych do przetwarzania danych osobowych w GDDKiA;
2) wszystkich danych osobowych, przetwarzanych w GDDKiA, niezależnie od formy (tradycyjne, papierowe zbiory ewidencyjne, w systemach informatycznych) oraz miejsca przetwarzania;

3) wszystkich zasobów teleinformatycznych GDDKiA, w których przetwarzane są dane osobowe.

§ 5. Celem Polityki jest opis realizacji w GDDKiA obowiązków wynikających z Rozporządzenia oraz zasad ochrony danych osobowych przetwarzanych w GDDKiA.

§ 6. Cele Polityki realizowane są poprzez zapewnienie zgodności przetwarzania danych osobowych z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, a także poprzez bezpieczeństwo danych w tym zapewnienie integralności i poufności.

§ 7. Administrator danych, aby zapewnić rozliczalność dokumentuje, w jaki sposób zapewnia realizację zasad określonych w § 6.

Rozdział 3

Obowiązki i odpowiedzialność w zakresie zarządzania ochroną danych osobowych

§ 8. Generalny Dyrektor, jako Administrator Danych wykonuje obowiązki z zakresu przetwarzania i ochrony danych osobowych zgodnie z przepisami Rozporządzenia.

§ 9. Administrator Danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpiecza dane osobowe przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 10. Zadania, o których mowa w § 9, w imieniu Administratora Danych wykonują:

1) kierownicy komórek organizacyjnych w Centrali i Oddziałach, w odniesieniu do danych osobowych przetwarzanych w podległych komórkach organizacyjnych;
2) Dyrektorzy Oddziałów, w odniesieniu do danych osobowych przetwarzanych w Oddziale;
3) osoby upoważnione do wykonywania określonych zadań w imieniu Administratora Danych.

§ 11. Wszystkie osoby upoważnione do przetwarzania danych zobowiązane są do:

1) przetwarzania i ochrony danych osobowych zgodnie z obowiązującymi przepisami;
2) postępowania zgodnie z ustaloną przez Administratora Danych Polityką;
3) ścisłego przestrzegania zakresu udzielonego upoważnienia;

4) zachowania w tajemnicy danych osobowych.

§ 12. Generalny Dyrektor wyznacza IOD.

§ 13. Dyrektorzy Oddziałów wyznaczają Koordynatorów ds. ochrony danych osobowych w Oddziałach.

§ 14. Do zadań IOD i Koordynatorów ds. ochrony danych osobowych należy:

1) monitorowanie przestrzegania Rozporządzenia, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, realizacja działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
2) podjęcie działań zgodnie z rozdziałem 8, w przypadku stwierdzenia naruszeń ochrony danych osobowych;
3) udzielanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie art. 35 Rozporządzenia;
4) opiniowanie projektów umów o powierzenie przetwarzania danych osobowych;
5) gromadzenie dokumentacji z analizy ryzyka dla ochrony danych osobowych;
6) monitorowanie odpowiednio w Centrali i Oddziałach sposobu przetwarzania danych osobowych;
7) informowanie Administratora Danych, oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

§ 15. Do zadań IOD ponadto należy:

1) prowadzenie rejestru czynności przetwarzania danych osobowych, o którym mowa w art. 30 Rozporządzenia;
2) współpraca z organem nadzorczym;
3) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

§ 16. Administrator Danych zapewni włączenie IOD i Koordynatorów ds. ochrony danych osobowych w Oddziałach do wszystkich spraw dotyczących ochrony danych osobowych

na ich początkowym etapie, przekazując niezbędne informacje, zgodnie z art. 38 Rozporządzenia.

§ 17. ASI są wyznaczani:

1) w Centrali przez:
   a) kierującego komórką właściwą ds. informatyki, w przypadku gdy system informatyczny jest zarządzany centralnie przez tę komórkę,
   b) kierownika właściwej komórki organizacyjnej, w przypadku gdy system informatyczny nie jest zarządzany centralnie przez kierującego komórką właściwą ds. informatyki;
2) w Oddziale przez Dyrektora Oddziału.

§ 18. Zadania ASI określa Polityka Bezpieczeństwa Teleinformatycznego.

§ 19. Kierujący komórką właściwą ds. informatyki realizuje czynności związane z zapewnieniem bezpieczeństwa systemów informatycznych zarządzanych centralnie przez tę komórkę, służących do przetwarzania danych osobowych.

§ 20. W zakresie zapewnienia bezpieczeństwa przetwarzania danych osobowych w eksploatowanych systemach informatycznych i sieciach teleinformatycznych do zadań kierującego komórką właściwą ds. informatyki należy, w szczególności:

1) wyznaczanie ASI dla systemów teleinformatycznych zarządzanych centralnie przez kierującego komórką właściwą ds. informatyki i określanie dla nich zadań, obowiązków i uprawnień w administrowanych systemach i sieciach teleinformatycznych;
2) dostosowanie systemów lub aplikacji oraz oprogramowania do wymogów, o których mowa w Rozporządzeniu i wewnętrznie obowiązujących aktach prawnych GDDKiA;
3) nadzorowanie technicznego zabezpieczenia i odpowiedniego wyposażenia obszarów przetwarzania danych osobowych.

§ 21. Kierujący komórką właściwą ds. obsługi urzędu w Centrali i Oddziale realizuje czynności w zakresie ochrony danych osobowych poprzez zapewnienie bezpieczeństwa fizycznego pomieszczeń i obiektów, które tworzą obszary przetwarzania danych.

§ 22. Do zadań kierującego komórką właściwą ds. obsługi urzędu w Centrali i Oddziale w zakresie ochrony danych osobowych, należy w szczególności wyposażenie obiektów

i pomieszczeń, w których przetwarzane są dane osobowe, w wymagane na mocy Polityki Bezpieczeństwa Fizycznego środki ochrony i zapewnienie ich właściwego funkcjonowania.

§ 23. Dyrektorzy Oddziałów są odpowiedzialni za nadzór nad zapewnieniem przestrzegania przepisów o ochronie danych osobowych w Oddziale, w tym za zastosowanie w podległym Oddziale, technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych przy uwzględnieniu analizy ryzyka, na zasadach określonych w rozdziale 12.

§ 24. Kierownicy komórek organizacyjnych Centrali i Oddziałów są odpowiedzialni za przestrzeganie przepisów dotyczących przetwarzania i ochrony danych osobowych w podległych im komórkach organizacyjnych.

§ 25. Do zadań kierowników komórek organizacyjnych w Centrali i Oddziałach należy, w szczególności:

1) zapewnienie zachowania szczególnej staranności przy przetwarzaniu danych osobowych, z uwzględnieniem zasad zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania;
2) identyfikowanie ryzyk naruszenia ochrony danych osobowych i zarządzanie tym ryzykiem w odniesieniu do danych osobowych przetwarzanych w kierowanej komórce organizacyjnej;
3) stosowanie zabezpieczeń danych osobowych zgodnie z wymogami określonymi w przepisach prawa powszechnie obowiązującego w zakresie ochrony danych osobowych a także w wewnętrznie obowiązujących aktach prawnych GDDKiA;
5) uwzględnianie ochrony danych osobowych w fazie projektowania oraz stosowanie zasady domyślnej ochrony danych zgodnie z art. 25 Rozporządzenia;
6) włączanie odpowiednio IOD lub Koordynatorów ds. ochrony danych osobowych w Oddziałach we wszystkie sprawy dotyczące ochrony danych osobowych na ich początkowym etapie;
7) rozpatrywanie wniosków o udostępnieniu danych osobowych przetwarzanych w podległej komórce organizacyjnej;
8) wnioskowanie o rejestrację, aktualizację i usunięcie czynności z rejestru czynności prowadzonego przez IOD;
9) wypełnianie obowiązków informacyjnych, o których mowa w art. 13 i 14 Rozporządzenia;

10) dokonywanie oceny skutków dla ochrony danych, o której mowa w art. 35 Rozporządzenia i wnioskowanie do Administratora Danych o uprzednie konsultacje, o których mowa w art. 36 Rozporządzenia;
11) przygotowywanie umów dotyczących powierzenia przetwarzania danych osobom, zgodnie z art. 28 Rozporządzenia i nadzór nad ich realizacją;
12) rozpatrywanie, w porozumieniu z IOD lub Koordynatorami ds. ochrony danych osobowych, skarg, wniosków i żądań osób, których dane dotyczą w związku z przetwarzaniem ich danych osobowych;
13) nadzór nad przestrzeganiem przez podległą komórkę organizacyjną przepisów w zakresie ochrony danych osobowych.

Rozdział 4

Dopuszczalność przetwarzania danych osobowych

§ 26. Przetwarzanie danych osobowych jest dopuszczalne po spełnieniu co najmniej jednej z przesłanek wymienionych w art. 6, 9 lub 10 Rozporządzenia i z uwzględnieniem zasad, o których mowa w art. 5 Rozporządzenia.

Rozdział 5

Obowiązki Informacyjne

§ 27. W przypadku zbierania danych osobowych od osoby, której one dotyczą, konieczne jest podanie tej osobie informacji zgodnie z art. 13 ust. 1-3 Rozporządzenia z zastrzeżeniem ust. 4 powołanego artykułu.

§ 28. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której one dotyczą, konieczne jest podanie tej osobie informacji zgodnie z art. 14 ust. 1-4 Rozporządzenia z zastrzeżeniem ust. 5 powołanego artykułu.

Rozdział 6

Zasady dopuszczania osób do przetwarzania danych osobowych

§ 29. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie od Administratora Danych, zapoznane z przepisami o ochronie danych osobowych oraz zobowiązane do zachowania danych osobowych w tajemnicy.

§ 30. Kierujący komórką właściwą ds. pracowniczych odpowiednio w Centrali lub Oddziale GDDKiA kieruje pracownika, wolontariusza, praktykanta lub stażystę odpowiednio do IOD lub Koordynatora ds. ochrony danych osobowych w Oddziale w celu zapoznania z przepisami o ochronie danych osobowych i wewnętrznie obowiązującymi w GDDKiA aktami prawnymi w tym zakresie.

§ 31. Kierownik komórki organizacyjnej odpowiednio w Centrali lub Oddziale GDDKiA kieruje osobę będącą stroną umowy cywilnoprawnej odpowiednio do IOD lub Koordynatora ds. ochrony danych osobowych w Oddziale w celu zapoznania z przepisami o ochronie danych osobowych i wewnętrznie obowiązującymi w GDDKiA aktami prawnymi w tym zakresie.

§ 32. IOD lub Koordynator ds. ochrony danych osobowych w Oddziale odbiera pisemne oświadczenie o zapoznaniu z przepisami o ochronie danych osobowych i wewnętrznie obowiązującymi w GDDKiA aktami prawnymi w tym zakresie, o którym mowa w § 30 oraz 31.

§ 33. Wzór oświadczenia osoby przetwarzającej dane osobowe, o którym mowa w § 32, stanowi załącznik nr 1 do Polityki.

§ 34. Upoważnienie do przetwarzania danych osobowych dla:

1) pracowników zajmujących stanowisko, z którym wiąże się przetwarzanie danych osobowych – jest opracowywane, przedkładane do podpisu oraz wydawane pracownikowi, podczas podpisywania umowy o pracę, przez kierującego komórką właściwą ds. pracowniczych odpowiednio w Centrali lub Oddziale GDDKiA;
2) stażystów, praktykantów lub wolontariuszy realizujących zadania, z którymi wiąże się przetwarzanie danych osobowych – jest opracowywane, przedkładane do podpisu oraz wydawane, w dniu rozpoczęcia stażu, praktyk lub wolontariatu, przez kierującego komórką właściwą ds. pracowniczych odpowiednio w Centrali lub Oddziale GDDKiA.;
3) osób wykonujących zadania na podstawie umów cywilnoprawnych – stanowi załącznik do umowy zawieranej z daną osobą.

§ 35. Upoważnienie do przetwarzania danych osobowych nadawane jest na czas:

1) trwania stosunku pracy;
2) współpracy z osobą niebędącą pracownikiem.

§ 36. Wzór upoważnienia do przetwarzania danych osobowych, stanowi załącznik nr 2 do Polityki.

§ 37. W przypadku wątpliwości, co do zakresu przetwarzania danych osobowych, o zakresie tym decyduje kierownik komórki organizacyjnej w Centrali lub Oddziale, gdzie dana osoba jest zatrudniona na podstawie umowy o pracę, lub z którą dana osoba współpracuje na innej podstawie.

§ 38. Tryb nadawania, zmiany i odbierania uprawnień do przetwarzania danych w systemach informatycznych określa Polityka Bezpieczeństwa Teleinformatycznego.

Rozdział 7

Przekazywanie, udostępnianie i powierzanie przetwarzania danych osobowych

§ 39. Przekazywanie danych wewnątrz GDDKiA może następować wyłącznie pomiędzy osobami posiadającymi ważne upoważnienie do przetwarzania danych osobowych. Zakres przekazywanych danych nie może wykraczać poza dane, których przetwarzanie jest niezbędne w ramach wykonywanych zadań przez osobę odbierającą dane osobowe.

§ 40. Dane osobowe przetwarzane w GDDKiA mogą być udostępnione na zewnątrz GDDKiA jedynie na podstawie przepisów prawa.

§ 41. Dane osobowe mogą być udostępniane na wniosek osoby, której dane dotyczą, w ramach przysługującego jej prawa dostępu, zgodnie z art. 15 Rozporządzenia.

§ 42. W przypadku dokonywania zlecenia świadczenia usług, z którym wiąże się przetwarzanie, przez podmiot przetwarzający, danych osobowych w imieniu Generalnego Dyrektora, należy dokonać powierzenia przetwarzania danych osobowych stosownie do wymogów określonych w art. 28 Rozporządzenia.

§ 43. Powierzenie przetwarzania nastąpić może wyłącznie w drodze umowy zawartej na piśmie wiążącej Podmiot przetwarzający i Administratora Danych. Administratora Danych mogą reprezentować osoby przez niego upoważnione.

§ 44. Projekt umowy (porozumienia) o powierzenie przetwarzania danych osobowych wymaga uzgodnienia odpowiednio z IOD, albo Koordynatorem ds. ochrony danych osobowych w Oddziale.

§ 45. Rejestr powierzeń przetwarzania danych osobowych zawiera dane podmiotu przetwarzającego, przedmiot umowy, numer i datę zawarcia umowy. Rejestr powierzeń jest prowadzony przez komórką merytoryczną nadzorującą wykonanie umowy.

§ 46. Wzór umowy o powierzenie przetwarzania danych osobowych, stanowi załącznik nr 3 do Polityki.

Rozdział 8

Procedura postępowania w przypadku naruszenia ochrony danych osobowych

§ 47. Naruszenie ochrony danych osobowych następuje w szczególności w przypadku pożaru, w wyniku którego utracone zostaną dokumenty zawierające dane osobowe, zgubienia nośnika pendrive, laptopa, w których zapisane były pliki zawierające dane osobowe, ataku hakerskiego, którego skutkiem jest nieuprawniony dostęp do systemów teleinformatycznych, w których przetwarzane są dane osobowe.

§ 48. W przypadku stwierdzenia naruszenia ochrony danych osobowych, każda osoba upoważniona do przetwarzania danych osobowych w GDDKiA jest zobowiązana do:

1) niezwłocznego zawiadomienia o powyższym bezpośredniego przełożonego; IOD (w przypadku Centrali) lub właściwego koordynatora ds. Ochrony Danych Osobowych w Oddziale (w przypadku Oddziałów). Jeżeli naruszenie lub okoliczności wskazujące na możliwość jego zaistnienia dotyczą danych osobowych przetwarzanych w systemach informatycznych należy ponadto zawiadomić o nich ASI;
2) powstrzymania się od wszelkich działań mogących spowodować zatarcie śladów, bądź dowodów naruszenia.

§ 49. Kierownik komórki organizacyjnej Centrali i Oddziału zawiadamia o naruszeniu IOD lub Koordynatora ds. ochrony danych osobowych w Oddziale, w miarę możliwości, nie później niż w terminie 24 godzin po stwierdzeniu naruszenia.

§ 50. Zawiadomienie, o którym mowa w § 49 powinno, co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) zawierać imię i nazwisko oraz dane kontaktowe osoby, od której można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§ 51. Kierownicy komórek organizacyjnych Centrali i Oddziałów są obowiązani gromadzić wszelkie dokumenty związane z naruszeniem, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze i przekazywać je do IOD lub Koordynatora ds. ochrony danych osobowych w Oddziale.

§ 52. Odpowiednio IOD lub Koordynator ds. ochrony danych osobowych w Oddziale sporządza raport z naruszenia. Wzór raportu naruszenia ochrony danych osobowych, stanowi załącznik nr 4 do Polityki.

§ 53. ASI reagują na naruszenia dotyczące danych osobowych przetwarzanych w systemach informatycznych, aby zmniejszyć ich skutki, a także aby zapobiec podobnym przypadkom w przyszłości.

§ 54. Kierownicy komórek organizacyjnych Centrali i Oddziałów są obowiązani do przekazywania IOD zgłoszeń naruszeń dokonywanych przez podmioty przetwarzające, w wykonaniu umów o powierzenie przetwarzania danych osobowych, których realizację nadzorują.

§ 55. Koordynatorzy ds. ochrony danych osobowych w Oddziałach przekazują do IOD niezbędne informacje i dokumenty w celu realizacji obowiązku, o którym mowa w art. 33 i 34 Rozporządzenia.

§ 56. IOD na podstawie otrzymanych informacji i dokumentów przygotowuje Administratorowi Danych zgłoszenie naruszenia organowi nadzorczemu, a jeżeli jest wymagane, także zawiadomienie osoby, której dane dotyczą.

Rozdział 9

Archiwizacja i usuwanie danych osobowych

§ 57. Dane osobowe podlegają archiwizacji zgodnie z powszechnie obowiązującymi przepisami prawa.

§ 58. Szczegółowe zasady dotyczące archiwizacji danych w GDDKiA reguluje instrukcja kancelaryjna.

§ 59. Usunięcie danych następuje gdy cel, dla którego zebrano dane został osiągnięty lub dane są już zbędne dla osiągnięcia tego celu.

§ 60. Zasada ograniczenia okresu przechowywania danych osobowych do ścisłego minimum ma zastosowanie do wszelkich form przetwarzania danych (papierowej i elektronicznej).

§ 61. W celu zapobieżenia przechowywaniu danych osobowych przez okres dłuższy niż wymagany, kierownicy komórek organizacyjnych Centrali i Oddziałów zobowiązani są do ustalenia procedury usuwania poszczególnych danych przetwarzanych w nadzorowanej komórce. Procedura powinna określać w szczególności terminy okresowego przeglądu poszczególnych danych i ich usuwania.

Rozdział 10

Rejestrowanie czynności przetwarzania danych osobowych

§ 62. Rejestr czynności przetwarzania danych osobowych jest prowadzony przez IOD, na podstawie informacji przekazanych przez kierowników komórek organizacyjnych Centrali i Dyrektorów Oddziałów.

§ 63. Informacje przekazywane zgodnie z § 62 obejmują:

1) cel przetwarzania;
2) opis kategorii osób i kategorii danych jakie będą przetwarzane;
3) podstawę prawną przetwarzania danych;
4) odbiorców lub kategorię odbiorców, którym dane mogą być przekazywane;
5) planowane terminy usunięcia poszczególnych kategorii danych;
6) formę danych (papierowa, elektroniczna);
7) ewentualne przekazywanie danych do państwa trzeciego lub organizacji międzynarodowych;
8) opis fizycznych, technicznych i organizacyjnych środków bezpieczeństwa.

Rozdział 11

Sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

§ 64. Monitorowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz Polityką w GDDKiA jest zadaniem IOD oraz Koordynatorów ds. ochrony danych osobowych w Oddziałach.

§ 65. Monitorowanie, o którym mowa w § 64 odbywa się w formie sprawdzeń.

§ 66. Sprawdzenia mogą być przeprowadzane także przy wsparciu specjalistycznych podmiotów zewnętrznych.

§ 67. Sprawdzenia mogą być przeprowadzane w trybie sprawdzenia planowego lub doraźnego.

§ 68. IOD opracowuje plan sprawdzeń na dany rok i przedkłada go do wiadomości Administratorowi Danych.

§ 69. Koordynatorzy ds. ochrony danych osobowych w Oddziałach opracowują plany sprawdzeń na dany rok i przedkładają je do wiadomości Dyrektorom Oddziałów oraz IOD.

§ 70. Osoba uprawniona do sprawdzenia ma prawo do:

1) wstępu do pomieszczeń, w których są przetwarzane dane osobowe w obecności osoby zajmującej pomieszczenie lub powołanej komisji;
2) żądania złożenia pisemnych lub ustnych wyjaśnień oraz okazania dokumentów i zrobienia ich kopii, przez osoby zatrudnione przy przetwarzaniu danych osobowych, w zakresie niezbędnym do przeprowadzenia sprawdzenia;
3) przeprowadzania oględzin urządzeń, nośników informacji i systemów informatycznych służących do przetwarzania danych osobowych.

§ 71. IOD sporządza sprawozdanie ze sprawdzenia, zawierające w szczególności przedmiot sprawdzenia, stwierdzone nieprawidłowości i propozycje działań mających na celu przywrócenie przetwarzania danych osobowych zgodnego z prawem.

§ 72. IOD przedkłada sprawozdanie Administratorowi Danych oraz kierownikowi komórki organizacyjnej, w której dokonano sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

§ 73. Kierownik komórki organizacyjnej, w której stwierdzono nieprawidłowości ma prawo do zgłoszenia, w terminie 14 dni od dnia otrzymania sprawozdania, umotywowanych pisemnych zastrzeżeń do przedstawionego sprawozdania.

§ 74. W przypadku stwierdzenia nieprawidłowości, Administrator Danych decyduje o podjęciu działań naprawczych i w tym celu kieruje, odpowiednio, do kierownika komórki organizacyjnej Centrali lub Dyrektora Oddziału zalecenia usunięcia nieprawidłowości.

§ 75. Koordynator ds. ochrony danych osobowych w Oddziale sporządza sprawozdanie ze sprawdzenia, zawierające w szczególności przedmiot sprawdzenia, stwierdzone

nieprawidłowości i propozycje działań mających na celu przywrócenie przetwarzania danych osobowych zgodnego z prawem.

§ 76. Koordynator ds. ochrony danych osobowych w Oddziale przedkłada sprawozdanie Dyrektorowi Oddziału, IOD oraz kierownikowi komórki organizacyjnej w Oddziale, w której dokonano sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

§ 77. Kierownik komórki organizacyjnej w Oddziale, gdzie stwierdzono nieprawidłowości ma prawo do zgłoszenia, w terminie 14 dni od dnia otrzymania sprawozdania, umotywowanych pisemnych zastrzeżeń do przedstawionego sprawozdania.

§ 78. W przypadku stwierdzenia nieprawidłowości, Dyrektor Oddziału decyduje o podjęciu działań naprawczych i w tym celu kieruje do kierownika komórki organizacyjnej w Oddziale zalecenia usunięcia nieprawidłowości.

§ 79. Osoba odpowiedzialna za obszar, w którym stwierdzono naruszenie zasad ochrony danych osobowych, w terminie 14 dni od otrzymania zaleceń, informuje na piśmie odpowiednio Administratora Danych lub Dyrektora Oddziału o podjętych czynnościach naprawczych lub składa wyjaśnienia o przeszkodach w podjęciu tych czynności.

Rozdział 12

Analiza ryzyka

§ 80. Przetwarzanie danych osobowych w GDDKiA odbywa się z uwzględnieniem oceny ryzyka, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą.

§ 81. Ryzyko należy określać poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

§ 82. Kierownicy komórek organizacyjnych w Centrali i Oddziałach są odpowiedzialni za identyfikowanie ryzyk i zarządzanie nimi, w odniesieniu do danych osobowych przetwarzanych w kierowanej komórce organizacyjnej.

§ 83. Analiza ryzyka powinna być wykonywana raz w roku, w terminie do 30 września, a także każdorazowo w przypadku zaistnienia okoliczności mających wpływ na ryzyko,

np. wystąpienia naruszeń, wdrażania nowych systemów informatycznych służących do przetwarzania danych osobowych lub zmian związanych z przetwarzaniem danych osobowych.

§ 84. Kierownicy komórek organizacyjnych w Centrali i Oddziałach przekazują kopię dokumentacji z analizy ryzyka odpowiednio do IOD lub Koordynatorów ds. ochrony danych osobowych w Oddziałach, w terminie 30 dni od dokonania analizy ryzyka lub jej zmiany.

§ 85. Koordynatorzy ds. ochrony danych osobowych w Oddziałach, niezwłocznie, przekazują IOD kopie dokumentacji z analizy ryzyka, zaakceptowane przez Dyrektorów Oddziałów.

Rozdział 13

Środki ochrony

§ 86. Stosowane środki powinny uwzględniać stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

§ 87. Ochrona danych osobowych w GDDKiA zapewniana jest poprzez zastosowanie:

1) środków ochrony fizycznej;
2) środków ochrony teleinformatycznej;
3) środków organizacyjnych.

§ 88. Środki ochrony fizycznej danych osobowych określa Polityka Bezpieczeństwa Fizycznego.

§ 89. Środki ochrony teleinformatycznej danych osobowych określa Polityka Bezpieczeństwa Teleinformatycznego.

§ 90. Do środków organizacyjnych zalicza się:

1) wyznaczenie IOD w Centrali oraz wyznaczenie Koordynatorów ds. ochrony danych osobowych w Oddziałach;
2) monitorowanie przestrzegania przepisów o ochronie danych osobowych;
3) dopuszczanie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie;
4) zapewnianie zapoznania osób przetwarzających dane osobowe z przepisami o ochronie danych osobowych;

5) zobowiązanie osób przetwarzających dane osobowe do zachowania danych osobowych w tajemnicy;
6) niszczenie dokumentów zawierających dane osobowe po ustaniu ich przydatności, za pomocą mechanicznych niszczarek dokumentów;
7) zakaz pozostawiania bez nadzoru dokumentów zawierających dane osobowe.

§ 91. W sprawach nieuregulowanych zastosowanie mają przepisy Rozporządzenia.

Załącznik nr 1 do Polityki

WZÓR

.....
(imię i nazwisko)

.....
(stanowisko służbowe)

.....
(nazwa komórki organizacyjnej)

OŚWIADCZENIE

OSOBY PRZETWARZAJĄCEJ DANE OSOBOWE

Oświadczam, że zostałam zapoznana/zostałem zapoznany z obowiązującymi przepisami prawa i wewnętrznie obowiązującymi w GDDKiA aktami prawnymi w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

....
(miejscowość i data) *(podpis osoby składającej oświadczenie)*

Załącznik nr 2 do Polityki

WZÓR

GENERALNY DYREKTOR
DRÓG KRAJOWYCH I AUTOSTRAD

Miejscowość, data .....

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 oraz art. 32 ust. 4 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, Generalny Dyrektor Dróg Krajowych i Autostrad, jako Administrator Danych, upoważnia Panią/Pana

.....

(imię, nazwisko)

do przetwarzania danych osobowych w formie papierowej lub elektronicznej, w zakresie niezbędnym do:

1) realizacji zadań służbowych, zgodnie z zakresem czynności, oraz powierzonych jednorazowo lub na stałe przez przełożonego *(w przypadku pracowników);*
2) realizacji zadań wynikających z zawartej umowy *(w przypadku stron umów cywilnoprawnych);*
5) realizacji zadań w ramach odbywanego stażu *(w przypadku stażystów;)*
4) realizacji zadań w ramach odbywanych praktyk (*w przypadku praktykantów);*

3) realizacji zadań w ramach świadczenia usług wolontarystycznych *(w przypadku wolontariuszy).*

Dla potrzeb realizacji zadań, upoważniam Panią/Pana do przetwarzania danych osobowych, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w GDDKiA.

Upoważnienie jest ważne przez okres świadczenia pracy (*w przypadku pracowników*)/ od dnia …. do dnia …… (*w przypadku innych osób niż pracownicy*).

Przyjmuję do wiadomości i stosowania,

a także zobowiązuję się do zachowania

danych osobowych w tajemnicy

…….. ……

(podpis osoby upoważnionej)

(podpis Administratora Danych lub osoby umocowanej do nadania upoważnienia)

Załącznik nr 3 do Polityki

WZÓR

UMOWA

O POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ..... w ....., zwana dalej „Umową o powierzenie"

pomiędzy:

Generalnym Dyrektorem Dróg Krajowych i Autostrad, reprezentowanym przez:

....., zwanym dalej „Administratorem Danych"

a ....., wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd ....., nr KRS ..... REGON ....., NIP ....., reprezentowaną przez:

....., zwaną dalej **„Wykonawcą",**

łącznie zwane **„Stronami"**

§ 1.

Powierzenie przetwarzania danych osobowych

1. W celu wykonania umowy Nr..... z dnia ..... (dalej „Umowa"), Administrator Danych powierza Wykonawcy przetwarzanie danych osobowych w trybie art. 28 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", dalej „Rozporządzenie",

2. Przetwarzanie danych przez Wykonawcę obejmuje dane osobowe .....

..... *(należy określić kategorie osób, których dane dotyczą, np. pracowników, właścicieli nieruchomości, osób zawartych w dokumentacji przetargowej)* w zakresie:.....

(należy wskazać rodzaj (zakres) danych osobowych określonych kategorii osób, których dane dotyczą np. imię, nazwisko, adres zamieszkania, nr Pesel, nr rachunku bankowego, nr telefonu, adres e-mail, wizerunek).

3. Wykonawca jest uprawniony do wykonywania, na powyższych danych osobowych, następujących operacji: ..... *(należy określić właściwe operacje, np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie, niszczenie, inne).*

4. Przetwarzanie przez Wykonawcę powierzonych danych osobowych będzie trwało w okresie ..... *(np. od....do..., realizacji Umowy).*

5. Wykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celu i zakresie oraz w sposób i przez czas określony w ust. 1 – 4 .

6. Wykonawca oświadcza, że nie będzie przetwarzał powierzonych danych osobowych w państwie trzecim, tj. w państwie nienależącym do Europejskiego Obszaru Gospodarczego.

§ 2.

Zasady przetwarzania powierzonych danych osobowych

1. Wykonawca zobowiązuje się wykonać wszelkie czynności wynikające z Umowy o powierzenie i przepisów o ochronie danych osobowych z najwyższą starannością.

2. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Administratora Danych za przetwarzanie powierzonych danych osobowych, Wykonawca zobowiązuje się niezwłocznie podjąć działania w celu ich usunięcia oraz natychmiast zawiadomić o nich Administratora Danych.

3. Administrator Danych wyraża zgodę na ewentualne dalsze powierzenie przetwarzania danych osobowych, przez Wykonawcę innemu podmiotowi przetwarzającemu. Dalsze powierzenie może nastąpić na podstawie pisemnej umowy, na mocy której zostaną nałożone te same obowiązki, jak w niniejszej Umowie o powierzenie. O zamiarze dalszego powierzenia Wykonawca każdorazowo poinformuje Administratora Danych.

W przypadku niewyrażenia przez Administratora Danych sprzeciwu w terminie ..... dni od dnia otrzymania informacji przez Administratora Danych umowa może zostać zawarta. Po zawarciu umowy Wykonawca jest zobowiązany poinformować o tym fakcie Administratora Danych podając dane podmiotu, któremu powierzył przetwarzanie danych. W przypadku nie wywiązania się przez inny podmiot przetwarzający ze spoczywających na nim obowiązków ochrony danych osobowych, pełną odpowiedzialność wobec Administratora Danych za ich wypełnienie ponosi Wykonawca.

§ 3.

Zabezpieczenie powierzonych danych osobowych

1. Wykonawca zapewnia, że wdroży odpowiednie środki techniczne i organizacyjne, aby przetwarzanie spełniało wymogi określone w obowiązujących przepisach prawa i chroniło prawa osób, których dane dotyczą.

2. Wykonawca oświadcza, że posiada niezbędną wiedzę w zakresie przetwarzania danych osobowych, wiarygodność oraz zasoby do należytego wykonania niniejszej Umowy.

3. Wykonawca zobowiązuje się w szczególności do:

1) przetwarzania danych wyłącznie na udokumentowane polecenie Administratora Danych; za udokumentowane polecenie uznaje się zadania nałożone na Wykonawcę w Umowie;
2) podjęcia wszelkich środków, aby zapewnić bezpieczeństwo przetwarzania danych osobowych zgodnie z wymogami nałożonymi na mocy art. 32 Rozporządzenia;
3) dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających wydane przez niego upoważnienie i zapoznanych przez niego z przepisami o ochronie danych osobowych;
4) zapewnienia, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania danych osobowych w tajemnicy;
5) pomagania Administratorowi Danych poprzez odpowiednie środki techniczne i organizacyjne wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale 3, a także z obowiązków określonych w art. 32-36 Rozporządzenia;
6) udostępniania Administratorowi Danych wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia;
7) prowadzenia rejestru kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 Rozporządzenia, jeżeli jest wymagane na mocy Rozporządzenia.

4. Wykonawca zobowiązuje się bez zbędnej zwłoki zgłosić Administratorowi Danych:

1) stwierdzenie naruszenia ochrony danych osobowych, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, zawierające co najmniej informacje, o których mowa w art. 33 ust. 3 Rozporządzenia;
2) otrzymanie żądania od osoby, której dane przetwarza, w zakresie przetwarzania dotyczących jej danych osobowych;
3) wszczęcie u Wykonawcy, przez organ właściwy ds. ochrony danych osobowych, kontroli sposobu przetwarzania powierzonych danych osobowych.

§ 4.

Nadzór nad wykonaniem Umowy o powierzenie

1. Administrator Danych jest uprawniony do audytu wykonywania przez Wykonawcę obowiązków określonych w niniejszej Umowie o powierzenie.

2. Wykonawca umożliwia Administratorowi Danych lub audytorowi upoważnionemu przez Administratora Danych przeprowadzenie audytów, w tym inspekcji. W szczególności Wykonawca:

1) zapewni wstęp do pomieszczeń, w których Wykonawca przetwarza powierzone dane osobowe;
2) przekaże pisemne lub ustne wyjaśnienia w celu ustalenia stanu faktycznego;
3) umożliwi przeprowadzenie oględzin dokumentów a także urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.

3. Z czynności sporządza się protokół, którego jeden egzemplarz doręcza się kontrolowanemu.

4. W przypadku stwierdzenia uchybień w zakresie wykonywania Umowy o powierzenie lub przepisów o ochronie danych osobowych, Administratorowi Danych przysługuje prawo do żądania natychmiastowego wstrzymania przetwarzania danych osobowych i wyznaczenia Wykonawcy terminu na usunięcie uchybień.

§ 5.

Odpowiedzialność Wykonawcy

Wykonawca zobowiązuje się do naprawienia szkody wyrządzonej Administratorowi Danych w wyniku naruszenia danych osobowych z winy Wykonawcy. W szczególności zobowiązuje się do pokrycia kar zapłaconych przez Administratora Danych, poniesionych

przez Administratora Danych, kosztów procesu i zastępstwa procesowego, a także odszkodowania na rzecz osoby, której naruszenie dotyczyło.

§ 6.

Wygaśnięcie Umowy

1. Umowa o powierzenie zostaje zawarta na okres od dnia … do dnia …….

2. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych, Wykonawca zobowiązuje się niezwłocznie, nie później niż w terminie ……. dni (do decyzji Administratora Danych) usunąć lub zwrócić Administratorowi Danych wszelkie dane osobowe oraz skutecznie usunąć wszelkie istniejące kopie, chyba że przepisy prawa nakazują przechowywanie danych. Z czynności usunięcia lub zwrotu należy sporządzić pisemny protokół. Powierzenie trwa do czasu wykonania tych czynności.

§ 7.

Postanowienia końcowe

1. Wszelkie zmiany i uzupełnienia Umowy o powierzenie dokonywane będą w formie pisemnej pod rygorem nieważności.

2. W sprawach nieuregulowanych zastosowanie znajdują przepisy o ochronie danych osobowych.

3. W przypadku sporów wynikających z realizacji Umowy o powierzenie Strony poddają jej rozstrzygnięciu przez sąd właściwy ze względu na siedzibę Administratora Danych.

4. Umowa została sporządzona w ……. jednobrzmiących egzemplarzach, ….. dla Administratora Danych, …… dla Wykonawcy.

…….. ……

Administrator Danych Wykonawca

Załącznik nr 4 do Polityki

WZÓR

RAPORT Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Data wykrycia naruszenia:

.....

2. Nazwa komórki/jednostki organizacyjnej, w której nastąpiło zdarzenie:

.....

3. Krótki opis zaistniałej sytuacji:

.....

.....

.....

4. Rodzaj i zakres informacji, których ochrona została naruszona:

.....

5. Działania podjęte w związku ze zdarzeniem:

.....

.....

.....

.....

Data i podpis osoby sporządzającej raport