DZIENNIK URZĘDOWY

Głównego Inspektoratu Transportu Drogowego

Warszawa, dnia 12 lutego 2015 r.

Poz. 9

Z A R Z Ą D Z E N I E N R 9 / 2 0 1 5

G Ł Ó W N E G O I N S P E K T O R A T R A N S P O R T U D R O G O W E G O

z dnia 12 lutego 2015 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Głównym Inspektoracie Transportu Drogowego

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) w związku z § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz art. 52 ust. 1 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2013 r. poz. 1414 oraz z 2014 r. poz. 486, 805, 915 i 1310), zarządza się, co następuje:

§ 1. W Głównym Inspektoracie Transportu Drogowego wprowadza się:

1) Politykę Bezpieczeństwa Danych Osobowych, stanowiącą załącznik nr 1 do niniejszego zarządzenia;
2) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem 15 lutego 2015 r.

Główny Inspektor Transportu Drogowego**:** *wz. M. Maksimiuk*

Załączniki do zarządzenia nr 9/2015
Głównego Inspektora Transportu Drogowego
z dnia 12 lutego 2015 r.

Załącznik nr 1

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W GŁÓWNYM INSPEKTORACIE TRANSPORTU DROGOWEGO

Spis treści

Rozdział 1.....5

Postanowienia ogólne 5

Rozdział 2.....5

Słownik pojęć 5

Rozdział 3.....7

Zakres przetwarzania danych osobowych..... 7

Rozdział 4.....8

Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem..... 8

Rozdział 5.....14

Dopuszczenie osób do przetwarzania danych osobowych 14

Rozdział 6.....15

Zasady przetwarzania danych osobowych 15

Ogólne zasady przetwarzania zbiorów danych osobowych..... 15
Realizacja obowiązku informacyjnego przy zbieraniu danych osobowych..... 16
Rejestracja zbiorów danych osobowych 17
Realizacja praw osób, których dane dotyczą..... 17
Udostępnianie danych osobowych innym podmiotom 18
Powierzanie przetwarzania danych osobowych..... 20
Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe..... 21
Przetwarzanie danych osobowych poza obszarem przetwarzania..... 22

Rozdział 7.....22

Przetwarzanie danych osobowych w systemie informatycznym i na nośnikach papierowych..... 22

Przetwarzanie danych w systemie informatycznym..... 22
Przetwarzanie danych osobowych w aplikacji poza bazą danych..... 23
Archiwizacja i tworzenie kopii zapasowych zbiorów danych osobowych w systemie informatycznym..... 24
Przetwarzanie danych osobowych znajdujących się na nośnikach papierowych 24

Rozdział 8.....24

Postępowanie w sytuacji naruszenia zasad ochrony danych osobowych 24

Rozdział 9.....25

Odpowiedzialność karna 25

Rozdział 10.....25

Postanowienia końcowe..... 25

Załącznik nr 1: Wzór wykazu zbiorów danych osobowych przetwarzanych w GITD 26

Załącznik nr 2: Wzór wykazu pomieszczeń - obszaru, w którym przetwarzane są dane osobowe 27

Załącznik nr 3: Wzór upoważnienia do nadawania upoważnień do przetwarzania danych osobowych w imieniu Głównego Inspektora Transportu Drogowego 28

Załącznik nr 4: Wzór oświadczenia dotyczącego zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia 29

Załącznik nr 5: Wzór upoważnienia do przetwarzania danych osobowych 32

Załącznik nr 6: Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych 32

Załącznik nr 7: Wzór oświadczenia dotyczącego zabezpieczenia danych osobowych przez pracownika wykonującego zadania służbowe w formie telepracy 32

Załącznik nr 8: Wzory klauzuli informacyjnej oraz oświadczenia zgody na przetwarzanie danych osobowych 33

Załącznik nr 9: Wzory dotyczące rejestrów udostępnień danych osobowych oraz sprzeciwów na przetwarzanie danych 34

Załącznik nr 10: Wzór postanowień dotyczących powierzenia czynności przetwarzania danych osobowych do umowy zlecenia usługi 35

Załącznik nr 11: Instrukcja postępowania w sytuacji naruszenia zasad ochrony danych osobowych 36

Załącznik nr 12: Wzór oświadczenia o zachowaniu poufności informacji dla osób przebywających w obszarze przetwarzania danych osobowych w Głównym Inspektoracie Transportu Drogowego 40

Rozdział 1

Postanowienia ogólne

§ 1. Polityka Bezpieczeństwa Danych Osobowych w Głównym Inspektoracie Transportu Drogowego, zwana dalej „Polityką”, określa zasady zarządzania bezpieczeństwem przetwarzania danych osobowych w Głównym Inspektoracie Transportu Drogowego, zwanym dalej „GITD”, zgodnie z obowiązującymi przepisami o ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182 i 1662).

Rozdział 2

Słownik pojęć

§ 2. Występujące w niniejszej Polityce pojęcia i skróty oznaczają:

1) Administrator danych – Głównego Inspektora Transportu Drogowego;
2) Administrator Bezpieczeństwa Informacji (ABI) – osobę powołaną przez Głównego Inspektora na podstawie art. 36a ust. 1 u.o.d.o., która realizuje zadania określone w art. 36a ust. 2 u.o.d.o.;
3) Administrator Bezpieczeństwa Systemów Informatycznych (ABSI) – osobę wyznaczoną przez Dyrektora Generalnego GITD odpowiedzialną za nadzór nad zabezpieczeniem systemów informatycznych, w których przetwarzane są dane osobowe w GITD;
4) Administrator Systemu Informatycznego (ASI) – wyznaczonego przez Dyrektora Generalnego GITD administratora systemu informatycznego/aplikacji w GITD, w którym są przetwarzane dane osobowe, odpowiedzialnego za realizację zabezpieczeń i odpowiednie funkcjonowanie systemu/aplikacji w GITD, w którym przetwarzane są dane osobowe;
5) aplikacja przetwarzająca dane osobowe – program oraz wszystkie niezbędne zasoby informatyczne, służące do przetwarzania zbioru danych osobowych;
6) BDG – Biuro Dyrektora Generalnego w GITD;
7) BFG – Biuro Finansowo Gospodarcze w GITD;
8) BIŁ – Biuro Informatyki i Łączności w GITD;
9) dane osobowe – wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgodnie z art. 6 ust. 1 i 2 u.o.d.o. ;
10) dane osobowe wrażliwe – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

11) DIT – Dyrektora Biura Informatyki i Łączności;
12) GIODO – Generalnego Inspektora Ochrony Danych Osobowych;
13) Główny Inspektor – Głównego Inspektora Transportu Drogowego;
14) GITD – Główny Inspektorat Transportu Drogowego;
15) komórka organizacyjna – biuro, Centrum Automatycznego Nadzoru nad Ruchem Drogowym, Gabinet Głównego Inspektora, delegatura terenowa GITD, wydział, sekcja, wieloosobowe lub samodzielne stanowisko pracy w ramach struktury organizacyjnej GITD;
16) KKO – kierującego komórką organizacyjną lub osobę zatrudnioną na samodzielnym stanowisku zarządzającą zasobem danych osobowych, odpowiedzialną za ochronę danych osobowych przetwarzanych w podległej komórce organizacyjnej. Rolę taką pełni również przewodniczący Komisji Socjalnej;
17) koordynator ds. ochrony danych osobowych – osobę wyznaczoną w delegaturze terenowej GITD, która nadzoruje bezpieczeństwo fizyczne danych osobowych przetwarzanych we właściwej dla niej delegaturze;
18) obszar przetwarzania danych osobowych – pomieszczenia lub części pomieszczeń na terenie GITD, w których są przetwarzane dane osobowe, zarówno w formie papierowej, jak i w systemie informatycznym;
19) odbiorca danych – zgodnie z art. 7 pkt 6 u.o.d.o. – każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych osobowych,
    c) przedstawiciela na terenie Rzeczypospolitej Polskiej administratora danych, który ma siedzibę lub miejsce zamieszkania w państwie trzecim,
    d) podmiotu, któremu administrator danych powierzył przetwarzanie danych osobowych,
    e) organów państwowych oraz organów samorządu terytorialnego, którym dane osobowe są udostępniane w związku z prowadzonym postępowaniem;
20) przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie (archiwizowanie), opracowywanie, zmienianie, udostępnianie i usuwanie;
21) rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);

22) system informatyczny przetwarzający dane osobowe – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych osobowych;
23) u.o.d.o. – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 i 1662);
24) usuwanie danych osobowych – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
25) użytkownik – osobę upoważnioną do przetwarzania danych osobowych przez Administratora danych lub osobę przez niego upoważnioną, mającą bezpośredni dostęp do danych przetwarzanych w systemie informatycznym lub aplikacji, posiadającą ustalony indywidualny identyfikator oraz hasło do dostępu do danych w systemie informatycznym;
26) WSO – Wydział Spraw Osobowych w BDG w GITD zajmujący się sprawami kadrowymi w GITD;
27) Zastępca Administratora Bezpieczeństwa Informacji (ZABI) – osobę powołaną przez Głównego Inspektora, która realizuje zadania ABI podczas jego nieobecności;
28) zasób danych osobowych – wszystkie dane osobowe, niezależnie od sposobu ich utrwalenia, zarówno w formie elektronicznej – w systemie informatycznym oraz na nośnikach (dyskietki, płyty CD/DVD/BD, pamięci flash i inne) jak i papierowej, występujące zarówno w zbiorach, jak i w formie nieuporządkowanej, przetwarzane przez komórkę organizacyjną w celu realizacji jej zadań;
29) zbiór danych osobowych – każdy, posiadający strukturę, zestaw (zasób) danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie;
30) Osoba Wykonująca Nadzór (OWN) – osobę wyznaczoną przez Głównego Inspektora do zapewnienia przestrzegania przepisów o ochronie danych osobowych, w przypadku niepowołania ABI.

Rozdział 3

Zakres przetwarzania danych osobowych

§ 3. 1. Postanowienia zawarte w niniejszej Polityce mają zastosowanie w stosunku do:
1) danych osobowych przetwarzanych w systemach informatycznych, w tradycyjnej formie papierowej oraz znajdujących się na wszelkich nośnikach danych;
2) danych osobowych przetwarzanych zarówno w zbiorach danych, w zestawach, jak i pojedynczych informacji osobowych;

3) informacji, dotyczących bezpieczeństwa danych osobowych, w szczególności nazw kont i haseł we wszystkich systemach/aplikacjach oraz ewidencji osób upoważnionych do przetwarzania danych osobowych.

2. Danymi osobowymi przetwarzanymi w GITD są w szczególności:

1) dane pracowników zatrudnionych na podstawie umowy o pracę, w tym dane inspektorów Inspekcji Transportu Drogowego;
2) dane osób, z którymi zostały zawarte umowy cywilnoprawne (umowa zlecenia, umowa o dzieło);
3) dane osób zewnętrznych, w szczególności:
   a) kierujących pojazdami - sprawców naruszeń i wykroczeń: w ruchu drogowym; związanych z elektronicznym poborem opłat; związanych z przekroczeniem dopuszczalnej wagi pojazdów na drodze,
   b) właścicieli/użytkowników/interesariuszy pojazdów związanych z naruszeniami i wykroczeniami,
   c) przewoźników posiadających uprawnienia związane z transportem międzynarodowym,
   d) kandydatów do pracy,
   e) praktykantów i stażystów,
   f) kontrahentów – osób fizycznych prowadzących działalność gospodarczą,
   g) przedstawicieli podmiotów współpracujących,
   h) gości wchodzących na teren GITD.

3. Pełny wykaz zbiorów danych osobowych znajduje się w odrębnym dokumencie: „**Wykaz zbiorów danych osobowych przetwarzanych w GITD**”.

Rozdział 4

Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem

§ 4. 1. Administratorem danych przetwarzanych w GITD w rozumieniu art. 7 pkt 4 u.o.d.o. jest Główny Inspektor.

2. Główny Inspektor jest odpowiedzialny za przetwarzanie i ochronę danych osobowych w GITD, zgodnie przepisami prawa, w tym za zaakceptowanie niniejszej Polityki.

3. Główny Inspektor może powołać **Administratora Bezpieczeństwa Informacji (ABI)**, który wykonuje zadania określone w u.o.d.o., w szczególności:

1) prowadzi rejestr zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust.1 u.o.d.o.;
2) zapewnia przestrzeganie przepisów o ochronie danych osobowych, poprzez:

a) nadzór nad przestrzeganiem zasad ochrony danych osobowych w GITD,

b) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i przyjętymi wewnętrznymi zasadami ochrony danych osobowych,

c) kontrolowanie stosowania klauzul informacyjnych, służących do zbierania danych osobowych,

d) kontrolowanie procesów udostępniania danych osobowych innym podmiotom,

e) kontrolowanie procesów związanych z powierzaniem przetwarzania danych osobowych przez GITD innym podmiotom,

f) nadzór nad wykonywaniem zadań przez ASI i ABSI w zakresie kontroli i zapewnienia bezpieczeństwa systemów informatycznych, służących do przetwarzania danych osobowych, w tym wdrożenia wymogów „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w GITD”,

g) opracowywanie sprawozdań dla administratora danych dotyczących sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

h) nadzorowanie opracowania i aktualizowania „Polityki bezpieczeństwa danych osobowych” i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, oraz przestrzegania zasad określonych w tych dokumentach,

i) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych, między innymi poprzez przygotowywanie materiałów informacyjnych dla osób upoważnionych do przetwarzania danych osobowych oraz nadzór nad szkoleniami dla pracowników, mających na celu pogłębienie wiedzy z zakresu ochrony danych osobowych.

4. Główny Inspektor może powierzyć ABI wykonywanie innych obowiązków, takich jak:

1) prowadzenie aktualnej dokumentacji, opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zabezpieczenia danych osobowych – „Polityki bezpieczeństwa danych osobowych” oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GITD”;

2) prowadzenia aktualnego „Wykazu zbiorów danych osobowych przetwarzanych w GITD” zgodnie ze wzorem zawartym w załączniku nr 1 do niniejszej Polityki;

3) prowadzenie aktualnego „Wykazu pomieszczeń - obszaru, w którym przetwarzane są dane osobowe w GITD”, zgodnie ze wzorem zawartym w załączniku nr 2 do niniejszej Polityki;

4) nadawania upoważnień do przetwarzania danych osobowych w GITD, zgodnie ze wzorem zawartym w załączniku nr 5 do niniejszej Polityki;

5) prowadzenia aktualnej „Ewidencji osób upoważnionych do przetwarzania danych osobowych w GITD”, zgodnie ze wzorem zawartym w załączniku nr 6 do niniejszej Polityki;
6) przygotowywanie w razie konieczności zgłoszeń zbiorów danych osobowych do rejestracji przez GIODO oraz aktualizacji zgłoszeń;
7) prowadzenie rejestrów udostępnień danych osobowych innym podmiotom, zgodnie ze wzorem zawartym w załączniku nr 9 do niniejszej Polityki;
8) wydawanie zaleceń dla KKO w zakresie zabezpieczenia danych osobowych;
9) podejmowanie działań zgodnie z przepisami i obowiązującymi w GITD procedurami w sytuacji naruszenia zasad przetwarzania danych osobowych;
10) prowadzenie rejestru zdarzeń, dotyczących naruszenia ochrony danych w GITD zgodnie ze wzorem zawartym w załączniku nr 11 do niniejszej Polityki;
11) udział w czynnościach kontrolnych wykonywanych w GITD przez GIODO.

5. W przypadku niepowołania ABI, Główny Inspektor wyznacza osobę lub osoby wykonujące nadzór nad przetwarzaniem danych osobowych (OWN). OWN wykonuje zadania określone w ust. 3 pkt 2 i ust. 4. W przypadku niepowołania ABI postanowienia niniejszej Polityki dotyczące ABI stosuje się odpowiednio do OWN.

6. Główny Inspektor wyznacza **Zastępcę Administratora Bezpieczeństwa Informacji (ZABI)**, który wykonuje wszelkie zadania ABI podczas jego nieobecności.

7. Kontrola podmiotów, którym zostały powierzone czynności przetwarzania danych osobowych należących do GITD jest przeprowadzana przez ABI zgodnie z postanowieniami zawartymi w umowach powierzenia przetwarzania danych osobowych.

8. W poszczególnych delegaturach terenowych GITD powoływani są przez Głównego Inspektora **koordynatorzy ds. ochrony danych osobowych,** którzy wykonują zadania w zakresie:
1) nadzoru nad fizycznym zabezpieczeniem danych osobowych przetwarzanych we właściwych dla nich delegaturach oraz oddziałach terenowych;
2) zgłaszania ABI naruszeń zasad ochrony danych osobowych.

9. KKO są odpowiedzialni za zarządzanie procesami przetwarzania danych osobowych w podległych komórkach organizacyjnych. Do obowiązków KKO należy:
1) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez swoje komórki organizacyjne;
2) występowanie z wnioskami o nadanie, zmianę lub cofnięcie uprawnień pracownikom do określonego zbioru danych osobowych przetwarzanych w systemie informatycznym, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych;

3) zapoznanie podległych pracowników i innych osób (np. współpracowników, przedstawicieli kontrahentów) z zasadami przetwarzania i ochrony danych osobowych w podległej komórce organizacyjnej;
4) wypełnianie obowiązków dotyczących zabezpieczenia obszaru przetwarzanych danych osobowych w podległej komórce organizacyjnej;
5) zgłaszanie do ABI zamiaru utworzenia nowego zbioru danych osobowych lub zmiany w przetwarzaniu istniejącego zbioru (dotyczy to papierowych i elektronicznych zbiorów, także zawartych w plikach aplikacji biurowych typu MS Word i MS Excel);
6) w przypadku realizacji procesu zbierania danych osobowych, konsultowanie z ABI podstaw prawnych przetwarzania danych osobowych, w tym konieczności zbierania i archiwizowania zgód osób, upoważniających GITD do przetwarzania danych osobowych;
7) ustalanie w porozumieniu z ABI i ABSI zasad tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w podległej komórce organizacyjnej;
8) realizacja procesu udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
9) realizacja procesów związanych z powierzaniem przetwarzania danych osobowych przez GITD innym podmiotom – zgodnie z zawartymi umowami powierzenia przetwarzania danych osobowych.

10. Pracownicy WSO są odpowiedzialni za:

1) przekazanie nowozatrudnionym pracownikom wzoru oświadczenia dotyczącego zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, zgodnie ze wzorem zawartym w załączniku nr 4 do niniejszej Polityki;
2) przekazywanie ABI informacji o ustaniu stosunku zatrudnienia pracowników;
3) odbieranie od pracowników wykonujących zadania służbowe w formie telepracy, oświadczeń dotyczących zabezpieczenia miejsca przetwarzania danych osobowych w swoich domach, zgodnie ze wzorem zawartym w załączniku nr 7 do niniejszej Polityki.

11. **DIT** jest odpowiedzialny za zabezpieczenie danych osobowych przetwarzanych w systemie informatycznym. Do jego obowiązków w tym zakresie należy:

1) zapewnienie wdrożenia wymaganych zabezpieczeń technicznych danych osobowych przetwarzanych w systemach informatycznych;
2) nadzór nad właściwym funkcjonowaniem systemu informatycznego, w którym przetwarzane są dane osobowe;
3) wyznaczanie ASI oraz kontrola ich działań;

4) podejmowanie decyzji o dopuszczeniu do eksploatacji systemów informatycznych przetwarzających dane osobowe;
5) decydowanie o instalacji nowych elementów w systemie informatycznym przetwarzającym dane osobowe;
6) współpraca z ABI i ABSI w zakresie zapewnienia bezpieczeństwa systemów informatycznych przetwarzających dane osobowe.

12. **Administratorzy Systemów Informatycznych (ASI),** w których przetwarzane są dane osobowe są odpowiedzialni za realizację zabezpieczeń i odpowiednie funkcjonowanie systemów informatycznych/aplikacji. Do obowiązków ASI należy:

1) fizyczne nadawanie dostępu do systemu/aplikacji osobom upoważnionym do przetwarzania danych osobowych na wniosek KKO;
2) usuwanie i modyfikacja uprawnień do dostępu do danych osobowych w systemie/aplikacji;
3) ustalanie i kontrola identyfikatorów dostępu do systemu/aplikacji oraz informowanie ABI o nadanych użytkownikom identyfikatorach;
4) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
5) przeciwdziałanie dostępowi osób nieupoważnionych do systemu/aplikacji, w którym przetwarzane są dane osobowe;
6) realizacja zadań obejmujących procesy przetwarzania i archiwizowania danych osobowych oraz wspomaganie użytkowników w sytuacjach problemowych;
7) przekazywanie ABI i ABSI informacji o nowych aplikacjach, serwerach i innych zmianach systemu informatycznego, ważnych z punktu przetwarzania danych osobowych;
8) wykonywanie kopii zapasowych systemów/aplikacji, zabezpieczenie przechowywania kopii oraz okresowe ich sprawdzanie pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu;
9) zgłaszanie do ABI i ABSI informacji niezbędnych do aktualizacji „Polityki bezpieczeństwa danych osobowych w GITD” oraz w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GITD” w zakresie bezpieczeństwa systemów/aplikacji;
10) tworzenie na polecenie DIT procedur zarządzania kontami użytkowników, procedur wykonywania kopii zapasowych, procedur kryzysowych, itp.

13. Dyrektor Generalny GITD może wyznaczyć osobę do pełnienia funkcji **Administratora Bezpieczeństwa Systemów Informatycznych (ABSI)**, która jest odpowiedzialna za nadzór

i kontrolę zabezpieczenia systemów informatycznych/aplikacji, w których przetwarzane są dane osobowe. Jeżeli ABSI nie jest wyznaczony jego rolę pełni DIT.

14. Do obowiązków ABSI należy:

1) nadzór nad realizacją postanowień „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GITD”;
2) nadzorowanie zgodności wszystkich wdrażanych systemów z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GITD” oraz procedurami obowiązującymi w GITD;
3) kontrolowanie bezpieczeństwa wszystkich systemów informatycznych służących do przetwarzania danych osobowych w GITD;
4) analiza wszelkich zdarzeń związanych z naruszeniem ochrony danych osobowych w systemach informatycznych przetwarzających dane osobowe;
5) podejmowanie działań zgodnie z przepisami i obowiązującymi w GITD procedurami w sytuacji stwierdzenia naruszenia ochrony danych osobowych przetwarzanych w systemie;
6) prowadzenie dokumentacji zdarzeń powodujących naruszenia bezpieczeństwa danych osobowych oraz systemów informatycznych;
7) nadzór nad realizacją napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe;
8) nadzór nad rozwiązywaniem sytuacji kryzysowych, pojawiających się w systemie informatycznym;
9) nadzór nad bezpiecznym przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
10) nadzór nad niezawodnością awaryjnego zasilania serwerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych;
11) składanie w porozumieniu z ABI wniosków do DIT (o ile ABSI nie jest DIT), dotyczących propozycji zakupu oprogramowania lub sprzętu, w celu realizacji lub podniesienia poziomu bezpieczeństwa systemów informatycznych, bezpieczeństwa kopii zapasowych itp.;
12) ustalanie w porozumieniu z ABI sposobów ochrony danych osobowych w systemie informatycznym oraz akceptowanie wdrożenia rozwiązań przygotowanych w tym celu;
13) składanie na żądanie ABI wyjaśnień, raportów, sprawozdań w zakresie realizacji obowiązków określonych w pkt 1-12.

Rozdział 5

Dopuszczenie osób do przetwarzania danych osobowych

§ 5. 1. Na podstawie u.o.d.o. Główny Inspektor jest upoważniony do przetwarzania danych osobowych występujących we wszystkich zasobach danych osobowych w GITD.

2. Główny Inspektor może upoważnić ABI do nadawania upoważnień do przetwarzania danych osobowych w GITD (wzór upoważnienia stanowi załącznik nr 3 do niniejszej Polityki).

3. Nowozatrudniany pracownik GITD, po podpisaniu umowy o pracę, wypełnia przekazany mu przez WSO wzór oświadczenia o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, a następnie kierowany jest przez WSO do ABI, który odbiera powyższe oświadczenie (wzór oświadczenia o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia stanowi załącznik nr 4 do niniejszej Polityki).

4. WSO w terminie 3 dni roboczych przed datą podpisania umowy o pracę przekazuje ABI informacje o planowanym zatrudnieniu na adres poczty elektronicznej.

5. Główny Inspektor lub ABI upoważnia osoby zatrudniane w GITD do przetwarzania danych osobowych w zakresie niezbędnym do wykonania zadań na zajmowanym stanowisku pracy (wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 5 do niniejszej Polityki).

6. Upoważnienia do przetwarzania danych osobowych osobom mającym wykonywać dla GITD czynności związane z dostępem do danych osobowych na podstawie umów cywilnoprawnych (np. umowy zlecenia/o dzieło) nadaje Główny Inspektor lub ABI na podstawie upoważnienia Głównego Inspektora. Dane do upoważnienia podaje KKO zlecający powyższe czynności. Nadając upoważnienie do przetwarzania danych osobowych ABI odbiera od osoby upoważnianej oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

7. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z u.o.d.o., rozporządzeniem, oraz niniejszą Polityką i „Instrukcją zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w GITD" obowiązującymi w GITD.

8. Każda osoba przed przystąpieniem do pracy przy przetwarzaniu danych osobowych (zarówno zatrudniona na podstawie umowy o pracę, jak również współpracująca z GITD na podstawie innego stosunku prawnego) zostaje zapoznana z zasadami ochrony danych osobowych obowiązujących w GITD. Szkolenia w ww. zakresie organizowane są w przypadku wystąpienia istotnych zmian w regulacjach dotyczących ochrony danych osobowych.

9. KKO przed dopuszczeniem osoby do pracy przy przetwarzaniu danych osobowych:

1) sprawdza, czy pracownik otrzymał upoważnienie do przetwarzania danych osobowych oraz złożył oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczenia w tajemnicy;
2) zapoznaje podległych pracowników z zasadami przetwarzania i ochrony danych osobowych w podległej komórce organizacyjnej (szczegółowe sposoby zabezpieczania i przetwarzania danych osobowych);
3) występuje, w zależności od potrzeb, z wnioskiem do DIT o nadanie lub zmianę uprawnień podległym pracownikom do określonego zasobu danych osobowych, przetwarzanych w systemie informatycznym zgodnie z zasadami określonymi w „Polityce Bezpieczeństwa Systemów Informatycznych w GITD”.

10. Oryginały podpisanych upoważnień do przetwarzania danych osobowych i oświadczeń o zachowaniu poufności przechowuje ABI.

11. BIŁ udostępnia ABI informacje o przyznanych identyfikatorach dla osób dopuszczonych do przetwarzania danych osobowych w systemie informatycznym.

12. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera:

1) imię i nazwisko osoby upoważnionej;
2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) identyfikator - jeżeli osoba ma dostęp do przetwarzania danych w systemie informatycznym/aplikacji.

13. Główny Inspektor lub ABI mogą cofnąć nadane upoważnienie do przetwarzania danych osobowych, na wniosek KKO lub z własnej inicjatywy, w szczególności w związku z naruszeniem przez osobę zasad przetwarzania i ochrony danych osobowych lub zmianą stanowiska pracy.

14. Upoważnienie wygasa wraz z rozwiązaniem umowy o pracę lub zakończeniem wykonywania czynności związanych z przetwarzaniem danych osobowych określonych umową zlecenia / o dzieło. KKO zlecający czynności w ramach umowy zlecenia / o dzieło, a w przypadku pracowników GITD wyznaczony pracownik WSO, informuje ABI o powyższym fakcie, za pomocą poczty elektronicznej w terminie 3 dni od dnia, w którym wygasło upoważnienie.

Rozdział 6

Zasady przetwarzania danych osobowych

§ 6. Ogólne zasady przetwarzania zbiorów danych osobowych

1. Dane osobowe w utworzonych zbiorach muszą być zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

2. Zbierane dane osobowe muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

3. Rodzaj i treść danych osobowych nie może wykraczać poza potrzeby wynikające z celu ich zbierania.

4. Zabronione jest zbieranie wszelkich danych osobowych nieistotnych, nie mających znaczenia lub o większym stopniu szczegółowości niż wynika to z określonego celu.

5. Zabronione jest przetwarzanie danych osobowych:

1) których zakres i cel przetwarzania nie został zatwierdzony przez Głównego Inspektora;
2) niezgodne z zakresem i celem zatwierdzonym przez Głównego Inspektora.

6. Dane osobowe powinny być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

7. Okres przechowywania danych osobowych może zostać wydłużony nawet po osiągnięciu celu przetwarzania, jeżeli przepisy ustaw szczególnych takie postępowanie dopuszczają.

§ 7. Realizacja obowiązku informacyjnego przy zbieraniu danych osobowych

1. W przypadku zbierania danych osobowych bezpośrednio od osób - na formularzach, umowach, kwestionariuszach, drukach, zarówno papierowych, jak i elektronicznych, należy umieszczać na nich klauzulę informacyjną, zgodnie ze wzorem zawartym w załączniku nr 8 do niniejszej Polityki.

2. Klauzula informacyjna zgodnie z art. 24 u.o.d.o. zawiera:

1) pełną nazwę i adres GITD;
2) cel zbierania danych osobowych;
3) nazwy lub kategorie podmiotów, którym dane osobowe mogą być udostępniane;
4) informacje o prawie dostępu do treści danych osobowych oraz ich poprawiania;
5) informacje czy podanie określonych danych osobowych jest obowiązkowe, czy też dobrowolne. W sytuacji, gdy podanie danych osobowych jest obowiązkowe, należy wskazać podstawę prawną umożliwiającą przetwarzanie danych bez zgody osoby, której dane dotyczą.

3. W sytuacji braku podstawy prawnej na przetwarzanie danych osobowych w danym celu lub zakresie, należy pod klauzulą informacyjną umieścić klauzulę zgody wraz z odrębnym miejscem na podpis, zgodnie ze wzorem zawartym w załączniku nr 8 do niniejszej Polityki.

4. KKO odpowiedzialny za proces związany ze zbieraniem danych osobowych ma obowiązek ustalić sposób realizacji obowiązku informacyjnego oraz przygotować według ustalonego wzoru klauzulę informacyjną.

5. Klauzule informacyjne zatwierdza ABI, na podstawie propozycji przedłożonej przez KKO.

6. KKO zobowiązany jest do nadzoru nad stosowaniem klauzul informacyjnych w podległej komórce organizacyjnej.

7. W sytuacji zbierania danych osobowych nie od osoby, której dane dotyczą, ABI przygotowuje treść listu informacyjnego zawierającego odpowiednie informacje zgodnie z art. 25 u.o.d.o., który następnie jest wysyłany do osób, których dane zostały pozyskane.

8. Za wysyłkę listów informacyjnych odpowiedzialny jest KKO, która zbiera dane osobowe.

§ 8. Rejestracja zbiorów danych osobowych

1. ABI prowadzi wykaz zbiorów danych osobowych w GITD na podstawie informacji otrzymywanych od KKO.

2. KKO zgłasza ABI zamiar utworzenia nowego zbioru danych osobowych przed rozpoczęciem procesu zbierania danych osobowych, podając jednocześnie informacje dotyczące zakresu i celu zbierania danych, formy prowadzenia zbioru (papierowa czy elektroniczna), zamiaru udostępniania lub powierzania przetwarzania danych na zewnątrz, obszaru przetwarzania oraz proponowanych środków zabezpieczeń.

3. ABI określa:

1) czy nowy zbiór wchodzi w zakres istniejących już w GITD zbiorów danych osobowych;
2) czy nowy zbiór należy zgłosić do rejestracji GIODO.

4. W sytuacji, jeżeli zgłoszenie jest ustawowo wymagane, ABI przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, na podstawie obowiązującego wzoru zgłoszenia.

5. Przygotowany projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, ABI przekazuje do podpisu Głównemu Inspektorowi lub innej upoważnionej osobie.

6. ABI wysyła podpisany wniosek rejestracyjny do GIODO.

7. KKO zgłasza do ABI w ciągu 5 dni wszelkie zmiany, dotyczące przetwarzania danych osobowych w zarejestrowanym zbiorze danych osobowych (w tym: zmiana celu przetwarzania danych, zmiana zakresu przetwarzanych danych, usunięcie zbioru itp.).

8. ABI przygotowuje aktualizację zgłoszenia zbioru danych osobowych do GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze, na podstawie obowiązującego wzoru.

9. Tryb postępowania określony w niniejszym paragrafie stosuje się odpowiednio w razie konieczności aktualizacji zgłoszenia zbioru danych osobowych do rejestracji GIODO.

§ 9. Realizacja praw osób, których dane osobowe dotyczą

1. W przypadku otrzymania wniosku o udzielenie informacji na temat przetwarzania danych osobowych od osoby, której dane dotyczą, odpowiedź musi nastąpić w terminie 30 dni od daty jego otrzymania.

2. Osoba, której dane dotyczą, może się zwracać z wnioskiem o udzielenie informacji – raz na 6 miesięcy.

3. Przesłany wniosek od osoby, której dane dotyczą jest przekazywany do ABI.

4. ABI ustala KKO, do którego zwraca się wnioskiem o zebranie niezbędnych informacji na temat przetwarzanych danych osoby, która zwróciła się do GITD z pisemnym wnioskiem.

5. KKO jest zobowiązany do przygotowania odpowiedzi na wniosek osoby w ciągu 10 dni.

6. Odpowiedź na wniosek zatwierdza Główny Inspektor lub osoba przez niego upoważniona.

7. Odpowiedź na wniosek jest wysyłana listem poleconym za potwierdzeniem odbioru.

8. ABI prowadzi „Rejestr udostępnień danych osobowych osobom, których one dotyczą", zgodnie ze wzorem zawartym w załączniku nr 9 do niniejszej Polityki.

9. W sytuacji wniosku, od osoby której dane dotyczą, zawierającego żądanie: uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania, ABI określa procedurę działania oraz przygotowuje stosowną do sytuacji odpowiedź na wniosek. Przepisy ust. 6 i 7 stosuje się odpowiednio.

10. W sytuacji wniesienia przez osobę sprzeciwu wobec przetwarzania jej danych, informacja o wniesieniu sprzeciwu przekazywana jest do ABI, który ocenia zasadność otrzymanego wniosku.

11. W sytuacji, gdy sprzeciw jest zasadny, informacja o konieczności zaprzestania przetwarzania danych osobowych wskazanej osoby – w określonych celach – zostaje przekazana do KKO zarządzającego przetwarzaniem danego zbioru oraz do ASI celem zablokowania bądź wykreślenia danych w systemie tradycyjnym lub informatycznym.

12. ABI przygotowuje odpowiedź na wniosek dotyczący wniesienia sprzeciwu, zawierającą informację o uwzględnieniu sprzeciwu bądź o jego odrzuceniu. Przepisy ust. 6 i 7 stosuje się odpowiednio.

13. ABI prowadzi „Rejestr sprzeciwów na przetwarzanie danych", zgodnie ze wzorem zawartym w załączniku nr 9 do niniejszej Polityki.

§ 10. Udostępnianie danych osobowych innym podmiotom

1. Dane osobowe mogą być udostępniane innym podmiotom w następujących przypadkach:

1) na podstawie przepisów prawa, w sytuacji kiedy udostępnienie jest obowiązkiem wprost określonym w przepisach;
2) na podstawie wniosku od podmiotu uprawnionego do otrzymania danych osobowych na podstawie przepisów prawa;

3) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych osobowych.

2. Dane osobowe udostępnia się podmiotom współpracującym na podstawie pisemnej umowy, pod warunkiem, że istnieją podstawy prawne udostępnienia danych.

3. Dane osobowe udostępnia się podmiotom uprawnionym na pisemny umotywowany wniosek, o ile przepisy szczególne nie stanowią inaczej.

4. Wpływające do danej komórki organizacyjnej GITD wnioski o udostępnienie danych osobowych przekazywane są niezwłocznie do ABI.

5. Każdy wniosek o udostępnienie danych osobowych wpływający do GITD podlega rejestracji przez ABI w rejestrze udostępnień, zgodnie ze wzorem zawartym w załączniku nr 9 do niniejszej Polityki.

6. ABI sprawdza wniosek pod względem formalnym kierując się obowiązującymi w tym zakresie przepisami prawa oraz dokonuje adnotacji, wyrażając zgodę lub odmawiając udostępnienia żądanych danych osobowych.

7. ABI przygotowuje odpowiedź odmowną na wniosek o udostępnienie danych osobowych do wnioskodawcy (w sprawach budzących wątpliwości we współpracy z radcą prawnym) przy zachowaniu zasady, że powinna ona zawierać uzasadnienie powołujące się na właściwe przepisy prawa.

8. Kopia odpowiedzi odmownej przekazywana jest do komórki organizacyjnej, do której wpłynął rozpatrywany wniosek.

9. Komórka organizacyjna, która otrzymała od ABI zgodę na udostępnienie danych osobowych, zbiera informacje niezbędne do udzielenia odpowiedzi oraz opracowuje jej projekt.

10. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

11. ABSI nadzoruje przestrzeganie zasad bezpieczeństwa, w przypadku udostępniania danych osobowych drogą elektroniczną.

12. Odpowiedź na wniosek o udostępnienie danych osobowych zarówno pozytywna lub odmowna, jest podpisywana przez Głównego Inspektora lub osobę przez niego upoważnioną.

13. Informacje zawierające dane osobowe, przekazywane są uprawnionym podmiotom lub osobom, za potwierdzeniem odbioru, w następujący sposób:

1) pocztą kurierską;
2) listem poleconym za pokwitowaniem odbioru;
3) za pomocą teletransmisji danych - zgodnie z procedurami ochrony danych osobowych;
4) osobiście za potwierdzeniem odbioru;

5) w inny, określony konkretnym wymogiem prawnym lub umową, sposób.

14. KKO zobowiązany jest do umożliwienia ABI przeprowadzenia czynności kontrolnych dotyczących stosowania prawidłowych zasad udostępniania danych osobowych.

§ 11. Powierzanie przetwarzania danych osobowych

1. Zlecanie jakichkolwiek czynności, związanych z przetwarzaniem danych osobowych podmiotom zewnętrznym w imieniu GITD, jest formą powierzenia przetwarzania danych osobowych.

2. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje Główny Inspektor lub osoba przez niego upoważniona do zawierania umów, na podstawie których dochodzi do powierzenia przetwarzania danych osobowych.

3. Powierzenie przetwarzania danych osobowych musi odbywać się zgodne z art. 31 u.o.d.o., na podstawie umowy zawartej na piśmie pomiędzy GITD a danym podmiotem, któremu zleca się czynności, związane z przetwarzaniem danych osobowych.

4. KKO odpowiedzialny za realizację umowy, na podstawie której dochodzi do powierzenia przetwarzania danych osobowych, odpowiada za umieszczenie w umowie postanowień o powierzeniu, zgodnie ze wzorem zamieszczonym w załączniku nr 10 do niniejszej Polityki. Postanowienia dotyczące powierzenia przetwarzania danych osobowych mogą znajdować się w treści umowy zlecenia usług podmiotowi zewnętrznemu lub w odrębnej umowie powierzenia.

5. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.

6. W sytuacji powierzenia czynności związanych z archiwizacją lub niszczeniem zasobów danych osobowych innemu podmiotowi, w umowie określa się co najmniej zakres powierzonych danych osobowych i wymagania, co do zabezpieczenia danych osobowych.

7. Jeżeli powierzenie danych osobowych jest związane z przetwarzaniem danych w systemie informatycznym, takim jak: przesył danych czy zdalne udostępnianie danych, KKO uzgadnia z DIT postanowienia w umowie, dotyczące:

1) udostępniania danych osobowych w systemie informatycznym;
2) przesyłania danych osobowych drogą teletransmisji.

8. Projekt umowy powierzenia przetwarzania danych osobowych przekazywany jest ABI do akceptacji.

9. ABI analizuje zgodność projektu z przepisami u.o.d.o. i wewnętrznymi regulacjami w GITD.

10. W przypadku braku uwag, ABI odsyła zaparafowany projekt do podpisu lub przekazuje zalecenia wprowadzenia zmian w projekcie.

11. Umowę powierzenia przetwarzania danych osobowych podpisuje Główny Inspektor lub osoba przez niego upoważniona.

12. Tryb postępowania określony w niniejszym paragrafie stosuje się odpowiednio w razie powierzenia GITD przetwarzania danych osobowych przez inny pomiot.

§ 12. Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

1. Obszarem przetwarzania danych osobowych w GITD są budynki, pomieszczenia lub części pomieszczeń, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i w systemie informatycznym.

2. KKO wskazują obszar przetwarzania danych osobowych, za których ochronę odpowiadają i przekazują informacje na jego temat ABI.

3. Do obszaru przetwarzania danych osobowych w GITD zalicza się pomieszczenia, w których pracownicy wykonują zadania służbowe w formie telepracy. Informacje na temat adresu oraz zabezpieczania pomieszczeń pracownicy wykonujący zadania w formie telepracy przekazują do BDG.

4. Wszelkie zmiany dotyczące obszaru przetwarzania danych osobowych, muszą być na bieżąco przekazywane do ABI.

5. ABI jest odpowiedzialny za prowadzenie aktualnego wykazu pomieszczeń, w których przetwarzane są dane osobowe w GITD, zgodnie ze wzorem określonym w załączniku nr 2 do niniejszej Polityki.

6. Przebywanie wewnątrz obszaru, o którym mowa w ust. 2 i 3, osób nieuprawnionych do dostępu do danych osobowych - jest dopuszczalne tylko w obecności osoby dopuszczonej do przetwarzania tych danych lub za zgodą KKO.

7. Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru, o którym mowa w ust. 2 i 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.

8. Pracownicy serwisów (np. sprzątania, ochrony itp.) lub innych firm współpracujących, przebywający w obszarze przetwarzania danych osobowych, są zobowiązani do podpisania imiennego oświadczenia o zachowaniu poufności informacji należących do GITD, zgodnie ze wzorem określonym w załączniku nr 12 do niniejszej Polityki. Wzór oświadczenia powinien być dołączony do umów zawieranych z tymi podmiotami.

9. KKO odpowiedzialny za realizację umowy odpowiada za podpisanie i przechowywanie oświadczeń, o których mowa w ust. 8.

10. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

11. Dyrektor Generalny GITD na wniosek Dyrektora BFG lub ABI może wprowadzić szczegółowe zasady ochrony pomieszczeń i budynków stanowiących obszar przetwarzania danych osobowych, w tym pomieszczeń, w których przetwarzane są dane wrażliwe oraz pomieszczeń serwerowni.

§ 13. Przetwarzanie danych osobowych poza obszarem przetwarzania

1. Niedopuszczalne jest wynoszenie jakichkolwiek nośników (papierowych i elektronicznych) zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot nośników zawierających dane osobowe odpowiada osoba upoważniona do ich wyniesienia oraz dany KKO (przełożony osoby).

2. W sytuacji przetwarzania danych osobowych przez pracowników na komputerach przenośnych lub dokumentach papierowych poza obszarem wymienionym w § 12 ust. 2, są oni zobowiązani chronić dane przed dostępem do nich osób nieupoważnionych.

3. Pracownik, który wykonuje zadania służbowe i obowiązki pracownicze w formie telepracy w swoim domu, jest zobowiązany do zabezpieczenia miejsca przetwarzania danych osobowych i podpisania oświadczenia, którego wzór jest zawarty w załączniku nr 7 do niniejszej Polityki.

4. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe oraz komputerów pracowników wykonujących zadania służbowe w formie telepracy, określa i wdraża DIT w porozumieniu z ABI.

5. Zasady ochrony pomieszczeń przez pracownika wykonującego zadania służbowe w formie telepracy w swoim domu określa ABI.

Rozdział 7

Przetwarzanie danych osobowych w systemie informatycznym i na nośnikach papierowych

§ 14. Przetwarzanie danych osobowych w systemie informatycznym

1. Dane osobowe mogą być przetwarzane wyłącznie w systemach informatycznych spełniających wymogi u.o.d.o. oraz rozporządzenia.

2. Zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określa dokument „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GITD”, w zakresie m.in.:

1) procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury, związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych, służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe,
   b) kopii zapasowych, o których mowa w pkt 4;
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych osobowych.

3. Za wdrożenie i aktualizację instrukcji wymienionej w ust. 2 odpowiedzialny jest DIT lub wyznaczona przez niego osoba.

§ 15. Przetwarzanie danych osobowych w aplikacji poza bazą danych

1. Jeżeli zachodzi taka konieczność, dopuszcza się przetwarzanie danych osobowych w plikach poza bazą danych, znajdującą się w określonym systemie informatycznym/aplikacji.

2. Potrzebę przetwarzania danych osobowych w takiej formie pracownik zgłasza do KKO, który wydaje na to zgodę.

3. KKO lub wyznaczona przez niego osoba przekazuje informacje ABI o prowadzeniu ewidencji, rejestrów i baz danych prowadzonych w danej komórce organizacyjnej w plikach programów biurowych typu: MS Word, MS Excel, MS Access itp.

4. KKO przed utworzeniem zestawień, ewidencji czy rejestrów z danymi osobowymi w plikach przetwarzanych poza bazą danych, ma obowiązek zwrócić się do ABI i ABSI o określenie zasad ochrony nowego zasobu danych.

§ 16. Archiwizacja i tworzenie kopii zapasowych zbiorów danych osobowych w systemie informatycznym

1. Sposób, częstotliwość tworzenia, przechowywania oraz likwidacji kopii zapasowych baz danych osobowych przetwarzanych w systemie informatycznym, określone zostały w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GITD" oraz w szczegółowych procedurach dla poszczególnych systemów informatycznych.

2. Tworzenie kopii zbiorów danych osobowych na dowolnym nośniku, w celu innym niż wymienione kopie zapasowe, może się odbywać za zgodą KKO. O fakcie tym informowany jest ABI i ABSI.

3. Tworzenie kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników (kopie bazy, ewidencje celowe, rejestry) odbywa się za zgodą KKO przez upoważnionego pracownika. KKO informuje o tym fakcie ABI i ABSI.

4. KKO w porozumieniu z ABI i ABSI określa zasady tworzenia, przechowywania i ewidencjonowania kopii zapasowych plików, o których mowa w ust. 3, oraz typ nośnika, na którym wykonuje się kopię.

5. W przypadku umieszczenia plików z danymi osobowymi na serwerze plików, stosuje się zasady tworzenia kopii zapasowych bazy danych dla serwerów.

§ 17. Przetwarzanie danych osobowych znajdujących się na nośnikach papierowych

1. Dane osobowe zawarte w dokumentacji papierowej mogą być przetwarzane jedynie przez osoby upoważnione do przetwarzania danych osobowych, zgodnie z zasadami niniejszej Polityki.

2. Decyzję o dopuszczeniu osoby do przetwarzania danych osobowych na nośnikach papierowych podejmuje KKO, który zarządza procesami przetwarzania danego zasobu danych osobowych.

3. Kopie papierowe z danymi osobowymi muszą być przechowywane w zamykanych na klucz nieoszklonych szafach, szufladach lub sejfach. Obowiązuje w tym wypadku tzw. „zasada czystego biurka".

4. Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych, określają przepisy kancelaryjne w GITD.

Rozdział 8

Postępowanie w sytuacji naruszenia zasad ochrony danych osobowych

§ 18. 1. W sytuacji naruszenia lub podejrzenia naruszenia zasad ochrony danych osobowych należy postępować zgodnie z regułami opisanymi w „Instrukcji postępowania w sytuacji naruszenia zasad ochrony danych osobowych", zawartej w załączniku nr 11 do niniejszej Polityki.

2. ABI prowadzi rejestr wszystkich zdarzeń, dotyczących naruszenia ochrony danych osobowych w GITD, zgodnie z Instrukcją, o której mowa w ust. 1.

Rozdział 9

Odpowiedzialność karna

§ 19. 1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w art. 49 – 54a u.o.d.o. oraz w art. 130, art. 266 - 269, art. 287 ustawy z dnia 1997 r. – Kodeks Karny (Dz. U. Nr 88, poz. 553, z późn. zm.[1)]).

2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w GITD, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Rozdział 10

Postanowienia końcowe

§ 20. 1. ABI przygotowuje propozycje zmian do Polityki, które przedkłada Głównemu Inspektorowi.

2. Po przyjęciu zmian przez Głównego Inspektora, ABI przygotowuje tekst jednolity Polityki.

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 128, poz. 840, z 1999 r. Nr 64, poz. 729 i Nr 83, poz. 931, z 2000 r. Nr 48, poz. 548, Nr 93, poz. 1027 i Nr 116, poz. 1216, z 2001 r. Nr 98, poz. 1071, z 2003 r. Nr 111, poz. 1061, Nr 121, poz. 1142, Nr 179, poz. 1750, Nr 199, poz. 1935 i Nr 228, poz. 2255, z 2004 r. Nr 25, poz. 219, Nr 69, poz. 626, Nr 93, poz. 889 i Nr 243, poz. 2426, z 2005 r. Nr 86, poz. 732, Nr 90, poz. 757, Nr 132, poz. 1109, Nr 163, poz. 1363, Nr 178, poz. 1479 i Nr 180, poz. 1493, z 2006 r. Nr 190, poz. 1409, Nr 218, poz. 1592 i Nr 226, poz. 1648, z 2007 r. Nr 89, poz. 589, Nr 123, poz. 850, Nr 124, poz. 859 i Nr 192, poz. 1378, z 2008 r. Nr 90, poz. 560, Nr 122, poz. 782, Nr 171, poz. 1056, Nr 173, poz. 1080 i Nr 214, poz. 1344, z 2009 r. Nr 62, poz. 504, Nr 63, poz. 533, Nr 166, poz. 1317, Nr 168, poz. 1323, Nr 190, poz. 1474, Nr 201, poz. 1540 i Nr 206, poz. 1589, z 2010 r. Nr 7, poz. 46, Nr 40, poz. 227 i 229, Nr 98, poz. 625 i 626, Nr 125, poz. 842, Nr 127, poz. 857, Nr 152, poz. 1018 i 1021, Nr 182, poz. 1228, Nr 225, poz. 1474 i Nr 240, poz. 1602, z 2011 r. Nr 17, poz. 78, Nr 24, poz. 130, Nr 39, poz. 202, Nr 48, poz. 245, Nr 72, poz. 381, Nr 94, poz. 549, Nr 117, poz. 678, Nr 133, poz. 767, Nr 160, poz. 964, Nr 191, poz. 1135, Nr 217, poz. 1280, Nr 233, poz. 1381 i Nr 240, poz. 1431, z 2012 r. poz. 611, z 2013 r. poz. 849, 905, 1036 i 1247 oraz z 2014 r. poz. 538.

Załącznik nr 1 do Polityki Bezpieczeństwa Danych Osobowych

Wzór wykazu zbiorów danych osobowych przetwarzanych w GITD

L.p.	Nazwa zbioru/zasobu danych osobowych	Cel przetwarzania	System/aplikacja/ ewidencja, w której przetwarzane są dane (podać nazwę)	Opis struktury zbiorów wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (zakres danych)	Sposób przepływu danych pomiędzy poszczególnymi systemami	Komórki organizacyjne korzystające ze zbioru/zasobu
1.						
2.						
3.						
4.						
5.						
6.						

Załącznik nr 2 do Polityki Bezpieczeństwa Danych Osobowych

Wzór wykazu pomieszczeń - obszaru, w którym przetwarzane są dane osobowe

Lokalizacja – adres i numer budynku	Numer pomieszczenia/ przeznaczenie	Komórka organizacyjna użytkująca pomieszczenie	Zabezpieczenie pomieszczenia

Załącznik nr 3 do Polityki Bezpieczeństwa Danych Osobowych

Wzór upoważnienia do nadawania upoważnień do przetwarzania danych osobowych w imieniu Głównego Inspektora Transportu Drogowego

UPOWAŻNIENIE

Na podstawie ……*/wstawić odpowiednie zapisy dotyczące udzielenia pełnomocnictwa/*, w odniesieniu do art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182 i 1662).

Główny Inspektor Transportu Drogowego

Upoważnia

Panią/Pana .....

/nazwa stanowiska, komórka organizacyjna/ …….

do nadawania w imieniu Głównego Inspektora Transportu Drogowego upoważnień do przetwarzania danych osobowych pracownikom i współpracownikom Głównego Inspektoratu Transportu Drogowego oraz odbierania od nich oświadczeń o zachowaniu tajemnicy danych osobowych zgodnie ze wzorem określonym w Polityce Bezpieczeństwa Danych Osobowych w Głównym Inspektoracie Transportu Drogowego.

Warszawa, dnia ..... …….....

podpis Głównego Inspektora

Potwierdzenie odbioru upoważnienia:

…….

data i podpis

Załącznik nr 4 do Polityki Bezpieczeństwa Danych Osobowych

Wzór oświadczenia dotyczącego zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia

OŚWIADCZENIE OSOBY UPOWAŻNIONEJ

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał (a) dostęp w związku z wykonywaniem prac na rzecz Głównego Inspektoratu Transportu Drogowego (GITD).

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w GITD dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów należących do GITD, jak i zbiorów powierzonych do przetwarzania GITD przez inne podmioty.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami ustawy o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182 i 1662) w tym o grożącej stosownie do przepisów rozdziału 8 ustawy odpowiedzialności karnej.

dn. ..... r.
miejsce i data złożenia oświadczenia

.....
podpis osoby składającej oświadczenie

Załącznik nr 5 do Polityki Bezpieczeństwa Danych Osobowych

Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
(Dz. U. 2014 r. poz. 1182 i 1662)

Upoważniam

Pana/Panią ……..

do przetwarzania danych osobowych w ramach pełnionych obowiązków służbowych, wynikających z:
*umowy o pracę / umowy cywilnoprawnej (np. umowy zlecenia, o dzieło) / umowy praktyki / stażu**
oraz obowiązków zleconych jednorazowo lub na stałe przez przełożonego.

Zakres upoważnienia do przetwarzania danych osobowych w systemach informatycznych jest określany poprzez indywidualnie przyznawane prawa dostępu do każdego z systemów.
Jednocześnie upoważniam wyżej wymienionego / wymienioną do tworzenia dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi w plikach programów biurowych (np. MS Word, MS Excel, MS Access) oraz podręcznych archiwach papierowych z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Głównym Inspektoracie Transportu Drogowego.

Upoważnienie wygasa wraz z rozwiązaniem umowy o pracę lub zakończeniem wykonywania prac określonych umową zlecenia / umową o dzieło / staż / praktykę.*

* - *niepotrzebne skreślić*

……

Podpis

Załącznik nr 6 do Polityki Bezpieczeństwa Danych Osobowych

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko/ komórka organizacyjna GITD	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator w danym systemie informatycznym
1.						
2.						
3.						
4.						
5.						

Załącznik nr 7 do Polityki Bezpieczeństwa Danych Osobowych

Wzór oświadczenia dotyczącego zabezpieczenia danych osobowych przez pracownika wykonującego zadania służbowe w formie telepracy

_____
(imię i nazwisko)

_____
(stanowisko)

_____
(komórka organizacyjna)

OŚWIADCZENIE

Niniejszym zobowiązuję się do zabezpieczenia danych osobowych przed dostępem osób niepowołanych, do których będę miał dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w formie telepracy, w Głównym Inspektoracie Transportu Drogowego.

Jednocześnie zobowiązuję się do przetwarzania danych osobowych jedynie pod niżej wskazanym adresem: _____

Przyjmuję do wiadomości, iż ww. adres zostanie umieszczony w wykazie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

..... **.....**

(miejscowość i data) **(podpis pracownika)**

Załącznik nr 8 do Polityki Bezpieczeństwa Danych Osobowych

Wzory klauzuli informacyjnej oraz oświadczenia zgody na przetwarzanie danych osobowych

Klauzula informacyjna do formularzy służących do zbierania danych osobowych

Administratorem podanych na formularzu danych osobowych jest Główny Inspektor Transportu Drogowego, z siedzibą: ul. Postępu 21, 02-676 Warszawa. Dane będą przetwarzane zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz. U. 2014 r. poz. 1182 i 1662) w celach …… ……. (podać cel przetwarzania).
Każda osoba ma prawo dostępu do treści swoich danych oraz ich poprawiania.
Podanie danych jest:
obowiązkowe i wynika z…….. (podać przepis prawa) *)
dobrowolne ale niezbędne do ……. (podać cel) *)

*) niepotrzebne skreślić

Oświadczenie zgody na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie podanych przeze mnie moich danych osobowych przez Głównego Inspektora Transportu Drogowego w celach ……*(podać cel przetwarzania).*

..... …….…….....
(miejscowość i data) (podpis osoby)

Załącznik nr 9 do Polityki Bezpieczeństwa Danych Osobowych

Wzory dotyczące rejestrów udostępnień danych osobowych oraz sprzeciwów na przetwarzanie danych

Wzór Rejestru udostępnień danych osobowych osobom, których one dotyczą

Data wpłynięcia wniosku od osoby	Imię i nazwisko osoby wnioskującej	Data udostępnienia	Rodzaj zbioru/zasobu i jego lokalizacja

Wzór Rejestru sprzeciwów na przetwarzanie danych od osób, których one dotyczą

Data wpłynięcia wniosku ze sprzeciwem osoby	Imię i nazwisko osoby wnioskującej	Decyzja dotycząca wniosku	Data wykonania decyzji	Rodzaj zbioru/zasobu i jego lokalizacja

Wzór Rejestru udostępnień danych osobowych innym podmiotom

Data wpłynięcia wniosku/ lub data podpisania umowy	Imiona i nazwiska osób lub kategorie danych których dotyczy udostępnienie	Data udostępnienia/ lub odmowy	Nazwa podmiotu, któremu udostępniono dane	Cel udostępnienia (podstawa prawna)	Zakres udostępnionych danych	Forma udostępnienia danych (nośnik elektroniczny, dokument papierowy, oznaczenie kancelaryjne)	Rodzaj zbioru/zasobu i jego lokalizacja

Załącznik nr 10 do Polityki Bezpieczeństwa Danych Osobowych

Wzór postanowień dotyczących powierzenia czynności przetwarzania danych osobowych do umowy zlecenia usługi

§ ….

1. W ramach umowy Główny Inspektor Transportu Drogowego jako administrator danych osobowych, na podstawie art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182 i 1662) powierza Zleceniobiorcy czynności, związane z przetwarzaniem danych osobowych.
2. Powierzone czynności dotyczą ……[1]
3. Zakres powierzonych danych obejmuje ..... [2]
4. Zleceniobiorca zobowiązuje się przetwarzać powierzone dane osobowe jedynie w celu i zakresie, określonych odpowiednio w punktach 2 i 3.
5. Zgodnie z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182 i 1662) Zleceniobiorca jest odpowiedzialny za ochronę powierzonych do przetwarzania danych osobowych.
6. Zleceniobiorca jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 wymienionej ustawy oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy.
7. W zakresie przestrzegania wymienionych w punktach 5 i 6 przepisów Zleceniobiorca ponosi odpowiedzialność jak administrator danych.
8. Główny Inspektor Transportu Drogowego zastrzega sobie możliwość kontroli sposobu wypełnienia przez Zleceniobiorcę wymagań wymienionych w pkt 6.

[1] *np. obsługi systemu informatycznego; zebrania danych; niszczenia dokumentacji itp.*

[2] *ten punkt uzupełniamy tylko w sytuacji, kiedy zlecamy innemu podmiotowi* ***zbieranie danych*** *(ponieważ zleceniobiorca nie może zebrać więcej danych niż zlecił mu zleceniodawca), czyli niszczenie dokumentów, obsługa systemu informatycznego, archiwizowanie danych itp. czynności, nie wymagają podania zakresu powierzonych danych, bo Zleceniobiorca nie będzie ich uzupełniał, modyfikował*

Załącznik nr 11 do Polityki Bezpieczeństwa Danych Osobowych

Instrukcja postępowania w sytuacji naruszenia zasad ochrony danych osobowych

Niniejsza instrukcja określa zasady postępowania w sytuacji naruszenia zasad ochrony danych osobowych przetwarzanych w Głównym Inspektoracie Transportu Drogowego (GITD).

§ 1

1. Sytuacją naruszenia zasad ochrony danych osobowych, zwaną również sytuacją kryzysową jest wystąpienie, zagrożenie lub domniemanie nieautoryzowanego dostępu, powielania, ujawnienia, modyfikacji, wykorzystania, zniszczenia, utraty, kradzieży oraz zatajenia informacji zawierającej dane osobowe.
2. Za naruszenie lub uzasadnione podejrzenie naruszenia zasad ochrony danych osobowych uznaje się:
   1) świadome lub nieświadome ujawnienie informacji zawierających dane osobowe osobie nieupoważnionej (nie posiadającej nadanego pisemnego upoważnienia do przetwarzania danych osobowych);
   2) sytuacje dotyczące systemu informatycznego:
      i. brak lub niedostpność spodziewanych danych,
      ii. niezgodność danych w systemie komputerowym z danymi w postaci papierowej lub innymi kopiami elektronicznymi,
      iii. pozostawione ślady włamania komputerowego, np. zmiany konfiguracji,
      iv. zmiany sum kontrolnych plików,
      v. wszelkie zapisy w logach systemów świadczące o naruszeniu bezpieczeństwa, wykonywaniu niedozwolonych operacji itp.,
      vi. samodzielne akcje podejmowane przez system (nawiązywanie połączeń, wysyłanie maili, itp.),
      vii. intensywna praca dysku w czasie, gdy z komputera nikt nie korzysta,
      viii. powtarzające się „zawieszenia" na ogół stabilnego systemu,
      ix. spowolnienie pracy systemu lub sieci,
      x. inne niż zwykle lub dodatkowe okna powitalne i proszące o podanie hasła,
      xi. odmowa przyjęcia hasła użytkownika,
      xii. pojawianie się niestandardowych okien, napisów i innych elementów ekranu,
      xiii. znaczące zmiany w zajętości dysku,
      xiv. nienaturalne rozmiary zapisywanych na dysku plików,
      xv. nietypowe nazwy plików lub katalogów,
      xvi. wykonujący nieuzasadnione połączenia lub odbierający nieuzasadnione połączenia modem podłączony do komputera,
      xvii. powtarzające się nagłe zrywanie połączeń sieciowych,
      xviii. ujawnienie indywidualnych haseł dostępu do informacji chronionych,
      xix. otrzymanie niespodziewanego listu z załącznikami (najczęściej typu .doc, .exe, .com);
   3) sytuacje dotyczące nośników informacji z danymi osobowymi (elektroniczne i papierowe):
      i. nieuprawnione wykonanie kopii nośników informacji zawierających dane osobowe,
      ii. zmiana lub usunięcie danych osobowych zapisanych na kopiach bezpieczeństwa lub archiwalnych,
      iii. zgubienie nośnika zawierającego dane osobowe,
      iv. wykrycie braku nośnika informacji z danymi osobowymi w jego miejscu przechowywania,

v. odkrycie niezniszczonych nośników informacji z danymi osobowymi w koszu na śmieci,
vi. przekazanie nośnika z danymi osobowymi osobie nieuprawnionej do ich otrzymania,
vii. znalezienie nośnika z danymi osobowymi;

4) sytuacje dotyczące pomieszczeń:
i. nieuprawniony dostęp lub próba dostępu do pomieszczeń, gdzie przetwarza się dane osobowe,
ii. pozostawienie bez nadzoru osoby nieupoważnionej w pomieszczeniu, gdzie znajdują się dane osobowe;
iii. niewłaściwe działanie fizycznych zabezpieczeń pomieszczeń gdzie przetwarza się dane osobowe,
iv. niewłaściwe parametry środowiska takie jak temperatura, wilgotność, dla pomieszczeń, w których są przetwarzane dane osobowe w systemie informatycznymi i na nośnikach papierowych i elektronicznych;

5) sytuacje dotyczące naruszenia szczegółowych zasad przetwarzania danych osobowych:
i. dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień;
ii. udostępnianie danych osobowych osobom nieupoważnionym;
iii. udostępnianie danych osobowych nieuprawnionym podmiotom;
iv. powierzanie przetwarzania danych osobowych innym podmiotom bez pisemnej umowy;
v. zbieranie danych osobowych bez wykonywania obowiązków informacyjnych;
vi. pozyskiwanie danych osobowych z nielegalnych źródeł;
vii. przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem;
viii. przetwarzanie danych osobowych w okresie dłuższym niż uprawniony;
ix. tworzenie nowych zasobów danych osobowych lub modyfikacja istniejących bez zgody Administratora Bezpieczeństwa Informacji (ABI);
x. niewykonanie obowiązku zgłoszenia zbioru danych osobowych do rejestracji GIODO lub aktualizacji tego zgłoszenia;
xi. przetwarzanie danych osobowych w obszarze nie zabezpieczonym;
xii. przetwarzanie danych osobowych w systemie, który nie spełnia wymogów „Polityki Bezpieczeństwa Danych Osobowych w GITD" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GITD";
xiii. wykonanie nieuprawnionych kopii danych osobowych;
xiv. brak aktualnych kopii bezpieczeństwa danych osobowych;
xv. niewłaściwe niszczenie nośników z danymi osobowymi, pozwalające na ich odczyt;
xvi. brak przeszkolenia pracowników w zakresie zasad przetwarzania danych osobowych.

§ 2

Osoba, która podejrzewa lub stwierdzi naruszenie zasad ochrony danych osobowych ma obowiązek niezwłocznie:

1) powiadomić Administratora Bezpieczeństwa Systemów Informatycznych (ABSI) oraz Administratora Systemu Informatycznego (ASI), jeżeli sytuacja dotyczy systemu informatycznego. W przypadku delegatury terenowej GITD należy poinformować Koordynatora ds. ochrony danych osobowych;

2) nie podejmować dalszej pracy w systemie informatycznym bez decyzji ABSI lub ASI;

3) powiadomić o zaistniałym zdarzeniu Dyrektora BFG oraz swojego bezpośredniego przełożonego jeżeli sytuacja dotyczy naruszenia bezpieczeństwa pomieszczeń. W przypadku delegatury terenowej GITD należy poinformować Koordynatora ds. ochrony danych osobowych;

4) powiadomić o zaistniałym zdarzeniu ABI oraz swojego bezpośredniego przełożonego jeżeli sytuacja dotyczy innych sytuacji przetwarzania danych osobowych. W przypadku delegatury terenowej GITD należy poinformować Koordynatora ds. ochrony danych osobowych;

5) określić (opisać) symptomy, świadczące o możliwości naruszenia lub naruszeniu zasad ochrony danych;

6) określić sytuację i czas, w jakim je zauważono;

7) podać wszelkie istotne informacje, mogące pomóc w ustaleniu przyczyny naruszenia zasad ochrony danych osobowych.

§ 3

1. Po otrzymaniu informacji o danej sytuacji naruszenia odpowiednio Dyrektor BFG lub ABI ocenia sytuację i podejmuje odpowiednie do potrzeb działania, a w szczególności:

   1) dokonuje rozpoznania zdarzenia;

   2) ocenia wagę problemu;

   3) lokalizuje źródło problemu

2. Dyrektor BFG informuje ABI o rozpoznaniu sytuacji naruszenia pomieszczeń.
3. Jeżeli zdarzenie dotyczy delegatury terenowej GITD, lokalny Koordynator ds. ochrony danych osobowych przekazuje ABI informacje na temat zdarzenia. Przekazana informacja powinna być zgodna z poniższym wzorem:

Imię i nazwisko osoby zgłaszającej naruszenie/podejrzenie naruszenia zasad ochrony danych osobowych	Delegatura	Data i godzina pozyskania informacji o naruszeniu/podejrzeniu naruszenia zasad ochrony danych osobowych	Opis lub symptomy naruszenia zabezpieczenia (z uwzględnieniem informacji o których mowa w § 2 pkt 5 – pkt 7 niniejszej procedury)

§ 4

1. W sytuacji naruszenia ochrony przetwarzania danych osobowych w systemie informatycznym ABSI lub ASI ocenia sytuację i podejmuje odpowiednie do potrzeb działania, a w szczególności:

   1) dokonuje rozpoznania zdarzenia;

   2) ocenia wagę problemu;

   3) ocenia możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania systemu;

   4) lokalizuje źródło problemu (przeprowadza analizę posiadanych danych);

   5) podejmuje decyzję o wstrzymaniu lub dalszej pracy systemu;

6) informuje ABI o rozpoznaniu sytuacji naruszenia w systemie informatycznym.

§ 5

W przypadku stwierdzenia zasadności podejrzeń o naruszeniu ochrony danych osobowych ABI powiadamia o tym Głównego Inspektora, który podejmuje działania, zmierzające do wyjaśnienia sprawy i poinformowania odpowiednich organów o zaistniałej sytuacji.

§ 6

ABI nadzoruje rozwiązanie problemu przez ABSI i ASI w sytuacji naruszenia ochrony danych osobowych w systemie informatycznym oraz podejmuje działania, celem wyeliminowania, bądź zminimalizowania wystąpienia podobnej sytuacji w przyszłości.

§ 7

W sytuacji naruszenia bezpieczeństwa danych osobowych, przetwarzanych w systemie informatycznym, każda interwencja ABSI lub ASI kończy się analizą postępowania i sporządzeniem notatki, która jest przekazywana do ABI.

§ 8

Po stwierdzeniu naruszenia bezpieczeństwa danych osobowych ABI sporządza notatkę, którą przekazuje Głównemu Inspektorowi.

§ 9

ABI prowadzi rejestr wszystkich zdarzeń, dotyczących naruszenia ochrony danych osobowych w GITD zgodnie z poniższym wzorem:

Lp.	Data i godzina zgłoszenia ABI faktu naruszenia ochrony danych osobowych	Imię i nazwisko osoby zgłaszającej zdarzenie	Opis lub symptomy naruszenia zabezpieczenia	Opis podjętych działań i decyzji
1.				
2.				
3.				
4.				
5.				

Załącznik nr 12 do Polityki Bezpieczeństwa Danych Osobowych

Wzór oświadczenia o zachowaniu poufności informacji dla osób przebywających w obszarze przetwarzania danych osobowych w Głównym Inspektoracie Transportu Drogowego

OŚWIADCZENIE

Imię i nazwisko……..……..

Nazwa firmy ……...…….

Stanowisko ……..……

Nr dowodu osobistego …….……..

W związku z przebywaniem w pomieszczeniach Głównego Inspektoratu Transportu Drogowego, zobowiązuję się do zachowania w tajemnicy informacji, do których mam lub będę mógł (a) mieć dostęp, jak również sposobów zabezpieczenia informacji i pomieszczeń. Przyjmuję do wiadomości, że obowiązek ten istnieje do czasu ustania tajemnicy (upublicznienia informacji).

……., dn. .....
miejscowość, data i podpis

.....
podpis osoby odbierającej oświadczenie w imieniu GITD

Załącznik nr 2

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W GŁÓWNYM INSPEKTORACIE TRANSPORTU DROGOWEGO

§ 1. W Głównym Inspektoracie Transportu Drogowego wprowadza się Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Głównym Inspektoracie Transportu Drogowego zawiera następujące zagadnienia:

§ 1. Postanowienia ogólne 42

§ 2. Definicje i skróty 42

§ 3. Cel i zakres Instrukcji 43

§ 4. Zabezpieczenie danych osobowych 43

§ 5. Obowiązki użytkowników systemu 44

§ 6. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności 44

§ 7. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem 45

§ 8. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu 46

§ 9. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania 47

§ 10. Sposób, miejsce i czas przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych 48

§ 11. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego 48

§ 12. Sposób odnotowywania w systemie informatycznym/aplikacji danych o jakich mowa w § 7 Rozporządzenia 49

§ 13. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych 49

§ 14. Postanowienia końcowe 49

§ 1. Postanowienia ogólne

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Głównym Inspektoracie Transportu Drogowego, zwana dalej „Instrukcją", została opracowana zgodnie z wymogami § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

§ 2. Definicje i skróty

Użyte w niniejszej Instrukcji definicje i skróty oznaczają:

1) Administrator danych – Głównego Inspektora Transportu Drogowego , który decyduje o środkach i celach przetwarzania danych osobowych;
2) Administrator Bezpieczeństwa Informacji (ABI) – osobę wyznaczoną przez Głównego Inspektora Transportu Drogowego na podstawie art. 36 ust. 3 u.o.d.o., która nadzoruje przestrzeganie zasad ochrony danych osobowych w GITD;
3) Administrator Systemu Informatycznego (ASI) – osobę wyznaczoną przez Dyrektora Generalnego GITD zarządzającą systemami operacyjnymi, bazodanowymi, sieciowymi lub systemami bezpieczeństwa;
4) GITD – Główny Inspektorat Transportu Drogowego;
5) BIŁ – Biuro Informatyki i Łączności;
6) dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
7) DIT – dyrektora Biura Informatyki i Łączności;
8) KKO – kierującego komórką organizacyjną GITD;
9) osoba upoważniona – osobę posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora danych;
10) przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;

11) rozporządzenie - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
12) u.o.d.o. – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662);
13) użytkownik – osobę upoważnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym;
14) zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

§ 3. Cel i zakres Instrukcji

1. Celem Instrukcji jest określenie podstawowych zasad właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w którym są przetwarzane dane osobowe ze zbioru danych osobowych oraz podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład, urządzenia, odpowiednio do zagrożeń i kategorii danych objętych ochroną.

2. Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem informatycznym. W przypadku wystąpienia potrzeb wprowadzenia nowych lub modyfikacji istniejących zasad bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, wnioski o ich uwzględnienie i wdrożenie powinni składać właściwi przedstawiciele komórek organizacyjnych, w których przetwarzane są dane osobowe, bezpośrednio do DIT.

§ 4. Zabezpieczenie danych osobowych

1. Podstawowym celem zabezpieczeń systemu informatycznego jest zapewnienie jak najwyższego poziomu bezpieczeństwa danych osobowych, które są w nim przetwarzane.

2. W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, dostęp do systemu informatycznego powinien być możliwy wyłącznie po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła lub innego elementu uwierzytelniającego.

3. Prawidłowy poziom zabezpieczenia systemu informatycznego i danych w nim przetwarzanych zostaje zapewniony poprzez przestrzeganie następujących zasad:

1) uniemożliwienie osobom postronnym uzyskiwania nieupoważnionego dostępu do systemu;

2) instalowanie nowego lub aktualizowanie już zainstalowanego oprogramowania wyłącznie przez uprawnionych użytkowników;
3) niepodejmowanie przez użytkowników prób testowania, modyfikacji i naruszenia zabezpieczeń systemu lub jakichkolwiek działań noszących takie znamiona.

§ 5. Obowiązki użytkowników systemu

1. Do podstawowych obowiązków użytkowników należy przetwarzanie danych osobowych wyłącznie w celu i zakresie wynikającym z obowiązków służbowych lub określonym przez swoich przełożonych.

2. Osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym są zobowiązane do podejmowania współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.

3. Użytkownicy systemu informatycznego zobowiązani są do:
1) przestrzegania opracowanych dla systemu zasad przetwarzania danych osobowych oraz procedur i instrukcji;
2) uniemożliwienia dostępu lub podglądu danych osobom nieupoważnionym;
3) informowania ASI o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych,
4) wykonywania bez zbędnej zwłoki poleceń ASI w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§ 6. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności

1. Dostęp do systemu informatycznego przetwarzającego dane osobowe (rozumiany również jako nadanie, odebranie lub zmiana uprawnień) może być przyznany jedynie osobom, które uzyskały upoważnienia do przetwarzania danych osobowych zgodnie z dokumentem „Polityka Bezpieczeństwa Danych Osobowych w GITD”.

2. Po spełnieniu wymagań określonych w punkcie powyższym rejestrowanie użytkowników i nadawanie uprawnień w systemie informatycznym realizowane jest na podstawie wniosku o nadanie lub odebranie uprawnień do systemów informatycznych.

3. Uprawnienia do systemu informatycznego mogą być nadawane, odbierane lub modyfikowane wyłącznie na podstawie wypełnionego wniosku w postaci elektronicznej lub papierowej skierowanego do BIŁ i zaakceptowanego przez właściwego KKO.

4. KKO akceptujący wniosek, jest zobowiązany do jego weryfikacji pod kątem zgodności wnioskowanych uprawnień z zakresem obowiązków podległego pracownika lub pracownika podmiotu zewnętrznego.

5. Wniosek który wpłynął do BIŁ jest akceptowany przez DIT i przekazywany do realizacji właściwym ASI.

6. ASI realizują wniosek oraz prowadzą rejestr identyfikatorów przyznanych użytkownikom w poszczególnych systemach informatycznych.

7. Wnioski o nadanie lub odebranie uprawnień do systemów informatycznych są archiwizowane przez BIŁ.

8. BIŁ przekazuje informacje o przyznanych identyfikatorach i hasłach bezpośrednio użytkownikowi.

9. Zmiana i odbieranie uprawnień do systemów informatycznych odbywa się na podstawie wypełnionego wniosku o nadanie lub odebranie uprawnień, zaakceptowanego przez właściwego KKO i skierowanego do BIŁ.

10. Zmiana uprawnień polega na odebraniu uprawnień przyznanych wcześniej i nadaniu nowych uprawnień zgodnie z nowym wnioskiem i procedurą opisaną powyżej.

11. DIT we wniosku o nadanie lub odebranie uprawnień do systemów informatycznych określa, które z uprawnień mogą nie być odbierane w przypadku gdy zmiana uprawnień wiąże się ze zmianą stanowiska lub zakresu obowiązków pracownika.

12. Jeżeli zmiana uprawnień użytkownika wiąże się ze zmianą komórki organizacyjnej, KKO, z której użytkownik odchodzi, ma obowiązek wnioskować o odebranie uprawnień użytkownika zaznaczając, że użytkownik przechodzi do innej komórki organizacyjnej.

13. W przypadku zakończenia zatrudnienia KKO, któremu podlegał pracownik, ma obowiązek wnioskować o całkowite odebranie uprawnień użytkownika do systemów informatycznych.

14. Postępowanie z zasobami sieciowymi (zgromadzonymi plikami, wiadomościami poczty elektronicznej) użytkownika, którego zatrudnienie w GITD ustało, jest każdorazowo uzgadniane pomiędzy DIT a właściwym KKO.

§ 7. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Podstawowym mechanizmem uwierzytelnienia użytkownika w systemie informatycznym są indywidualne identyfikatory i hasła. Otrzymane przez pracownika identyfikatory i hasła dostępowe do systemu informatycznego są poufne oraz zostały przekazane wyłącznie na jego użytek. Nie wolno ich użyczać lub przekazywać innym osobom, zapisywać lub pozostawiać w miejscu, w którym mogłyby być odkryte przez osobę nieupoważnioną (krawędź biurka, spód klawiatury itp.).

2. Pracownicy muszą stosować hasła zgodne z polityką tworzenia haseł przyjętą w GITD.

3. Jeżeli system informatyczny z powodów technologicznych nie ma możliwości wymuszenia odpowiednio silnego hasła lub wymuszenia jego zmiany co 30 dni, pracownicy zobowiązani są do:

1) ustanowienia indywidualnego hasła dostępu składającego się z minimum 8 znaków, zawierającego co najmniej jedną wielka i jedną małą literę oraz cyfrę lub znak specjalny;
2) zmiany hasła co 30 dni i nie używania starego hasła lub hasła o strukturze zbliżonej do starego hasła;
3) niezwłocznej zmiany hasła, gdy istnieje uzasadnione podejrzenie naruszenia bezpieczeństwa systemu lub ujawnienia hasła, zmiany hasła tymczasowego przy pierwszym logowaniu.

4. Zabrania się wprowadzania haseł na stałe do systemów informatycznych oferujących możliwość ich zapamiętania i ponownego logowania bez potrzeby podawania hasła.

§ 8. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Przed przystąpieniem do pracy z systemem, użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie ASI za pomocą systemu QDesk.

3. Rozpoczynając pracę na komputerze, pracownik musi podać wszystkie wymagane, własne identyfikatory i hasła, w sposób uniemożliwiający ich ujawnienie innym osobom.

4. Pracownik zobowiązany jest uwierzytelniać się w systemie informatycznym, wyłącznie na podstawie własnego identyfikatora i hasła. Uwierzytelnienie lub próby uwierzytelniania przy pomocy identyfikatorów i haseł innych pracowników będą traktowane jako świadome naruszenie zasad bezpieczeństwa systemów informatycznych.

5. Każdy z pracowników posiada dostęp tylko do tych funkcji aplikacji, które są mu niezbędne w codziennej pracy. Próby nieautoryzowanego dostępu do innych funkcji aplikacji lub jakichkolwiek zasobów informatycznych będą traktowane jako świadome naruszenie zasad bezpieczeństwa systemów informatycznych.

6. W przypadku braku możliwości zalogowania się pracownika do działającego systemu informatycznego lub dostępu do funkcjonalności systemu, niezbędnych do realizacji zadań służbowych, należy poinformować ASI za pomocą systemu QDesk.

7. Opuszczając stanowisko pracy należy wylogować się z systemu.

8. Przy krótkotrwałych przerwach w pracy należy zablokować stację roboczą (przyciski Ctr+Alt+Del Zablokuj ten komputer lub klawisz ⊞ + L).

9. Kończąc pracę, użytkownik obowiązany jest do:

1) wylogowania się z systemu, a następnie wyłączenia sprzętu komputerowego;
2) zabezpieczenia stanowiska pracy, w szczególności schowania do zamykanych szaf, szuflad itp. wszelkiej dokumentacji oraz nośników magnetycznych, optycznych i papierowych (zasada „czystego biurka").

§ 9. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. DIT ustala w porozumieniu z właściwymi KKO sposób wykonywania kopii bezpieczeństwa poszczególnych systemów informatycznych z uwzględnieniem potrzeb biznesowych oraz możliwości technicznych.

2. Dla każdego systemu informatycznego należy określić i udokumentować:

1) zakres danych podlegających zabezpieczeniu;
2) częstotliwość wykonywania kopii bezpieczeństwa;
3) czas i miejsce przechowywania kopii bezpieczeństwa;
4) nośnik wykorzystywany do przechowywania kopii zapasowych.

3. Wymagane jest przechowywanie kopii bezpieczeństwa poza lokalizacją, w której znajduje się system informatyczny dla którego wykonuje się kopię bezpieczeństwa.

4. Zatwierdzone podpisem właściwego KKO zasady wykonywania kopii bezpieczeństwa dla systemu informatycznego są przechowywane przez BIŁ.

5. ASI przed dokonywaniem istotnych zmian konfiguracyjnych w systemie informatycznym mogących skutkować niestabilnym działaniem systemu (np. wgranie nowej wersji oprogramowania kluczowych komponentów systemu) jest zobowiązany do wykonania dodatkowej kopii bezpieczeństwa niezależnie od przyjętego harmonogramu wykonywania kopii zapasowych.

6. Nie wykonuje się kopii bezpieczeństwa stacji roboczych. Dane ze stacji roboczych które są istotne dla działalności GITD muszą być zapisywane przez użytkowników na dedykowanych zasobach sieciowych wskazanych przez DIT.

7. Odtwarzanie kopii bezpieczeństwa następuje w wyniku:

1) działań realizowanych przez BIŁ związanych z obsługą awarii lub rekonfiguracją systemu informatycznego;
2) okresowego sprawdzania możliwości odtworzenia kopii bezpieczeństwa przez BIŁ;
3) na wniosek KKO skierowany do BIŁ.

8. BIŁ prowadzi w formie elektronicznej rejestr, w którym odnotowywane są błędy wykonania kopii bezpieczeństwa oraz awaryjne i okresowe odtworzenia kopii bezpieczeństwa.

§ 10. Sposób, miejsce i czas przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Dane osobowe mogą być przechowywane:

1) na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych;
2) na wymiennych nośnikach elektronicznych.

2. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafach lub sejfach w obszarach zapewniających kontrolę dostępu.

3. Nośniki elektroniczne zawierające dane osobowe, dla których cel przetwarzania ustał powinny być pozbawiane zapisu tych danych, a w przypadku gdy nie jest to możliwe, należy je zniszczyć poprzez złamanie, pocięcie, przedziurawienie lub poprzez przekazanie na podstawie umowy do specjalistycznej firmy dokonującej likwidacji nośników danych.

§ 11. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.

2. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.

3. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

4. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują wyznaczone osoby niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.

5. Administratorzy systemu mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

6. Innymi środkami ochrony przed szkodliwym oprogramowaniem, umożliwiającym uzyskanie nieuprawnionego dostępu do systemu informatycznego, są zapory oraz systemy wykrywania i prewencji przed włamaniami.

§ 12. Sposób odnotowywania w systemie informatycznym/aplikacji danych o jakich mowa w § 7 rozporządzenia

1. System informatyczny powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.

2. Odnotowanie pozostałych informacji, tj.:

1) źródła pochodzenia danych osobowych, jeśli dane mogą pochodzić z różnych źródeł;
2) informacji o odbiorcach danych osobowych oraz o dacie i zakresie udostępnienia danych;
3) sprzeciwu wobec dalszego przetwarzania danych osobowych, określonego w art. 32 ust. 1 pkt 7 i 8 u.o.d.o.

- jest zależne od sytuacji dotyczącej przetwarzania danych osobowych.

3. ABI podejmuje decyzję o odnotowywaniu wymienionych w ust. 2 informacji po analizie, czy w danym systemie informatycznym/aplikacji jest to wymagane.

§ 13. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemie informatycznym odpowiadają ASI.

2. Przeglądu, konserwacji i napraw mogą dokonywać ASI lub podmioty zewnętrzne pod nadzorem ASI, na podstawie odrębnych umów.

3. Osoby nie będące pracownikami GITD, które prowadzą prace serwisowe na rzecz Administratora danych, przed rozpoczęciem prac powinny być poddane weryfikacji tożsamości przez ASI. Prace powinny być prowadzone w miarę możliwości bez dostępu do danych osobowych.

4. W wypadku konieczności dostępu pracowników firm zewnętrznych do danych osobowych, podpisują oni oświadczenie o zachowaniu poufności informacji pozyskanych w trakcie wykonywania prac oraz sposobów zabezpieczeń tych danych - zgodnie ze wzorem zawartym w „Polityce Bezpieczeństwa Danych Osobowych w GITD”.

5. W przypadku konieczności przekazania sprzętu do naprawy lub konserwacji poza strefę obejmującą obiekty użytkowane przez GITD nośniki z danymi osobowymi są z urządzeń demontowane i pozostają w siedzibie GITD w strefie kontrolowanego dostępu.

§ 14. Postanowienia końcowe

1. Każdy użytkownik obowiązany jest zapoznać się przed dopuszczeniem do pracy z niniejszą Instrukcją.

2. Za nieprzestrzeganie zasad określonych w Instrukcji użytkownik ponosi odpowiedzialność karną na podstawie art. 51 – 52 u.o.d.o. oraz art. 266-269 i art. 287 ustawy z dnia 1997 r. – Kodeks Karny (Dz. U. Nr 88, poz. 553, z późn. zm.[2)]).

3. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 2, naruszenie zasad zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych w GITD, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

4. W sprawach nieuregulowanych w niniejszej Instrukcji, mają zastosowanie przepisy u.o.d.o. oraz przepisy aktów wykonawczych, wydanych na jej podstawie.

2) Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1997 r. Nr 128, poz. 840, z 1999 r. Nr 64, poz. 729 i Nr 83, poz. 931, z 2000 r. Nr 48, poz. 548, Nr 93, poz. 1027 i Nr 116, poz. 1216, z 2001 r. Nr 98, poz. 1071, z 2003 r. Nr 111, poz. 1061, Nr 121, poz. 1142, Nr 179, poz. 1750, Nr 199, poz. 1935 i Nr 228, poz. 2255, z 2004 r. Nr 25, poz. 219, Nr 69, poz. 626, Nr 93, poz. 889 i Nr 243, poz. 2426, z 2005 r. Nr 86, poz. 732, Nr 90, poz. 757, Nr 132, poz. 1109, Nr 163, poz. 1363, Nr 178, poz. 1479 i Nr 180, poz. 1493, z 2006 r. Nr 190, poz. 1409, Nr 218, poz. 1592 i Nr 226, poz. 1648, z 2007 r. Nr 89, poz. 589, Nr 123, poz. 850, Nr 124, poz. 859 i Nr 192, poz. 1378, z 2008 r. Nr 90, poz. 560, Nr 122, poz. 782, Nr 171, poz. 1056, Nr 173, poz. 1080 i Nr 214, poz. 1344, z 2009 r. Nr 62, poz. 504, Nr 63, poz. 533, Nr 166, poz. 1317, Nr 168, poz. 1323, Nr 190, poz. 1474, Nr 201, poz. 1540 i Nr 206, poz. 1589, z 2010 r. Nr 7, poz. 46, Nr 40, poz. 227 i 229, Nr 98, poz. 625 i 626, Nr 125, poz. 842, Nr 127, poz. 857, Nr 152, poz. 1018 i 1021, Nr 182, poz. 1228, Nr 225, poz. 1474 i Nr 240, poz. 1602, z 2011 r. Nr 17, poz. 78, Nr 24, poz. 130, Nr 39, poz. 202, Nr 48, poz. 245, Nr 72, poz. 381, Nr 94, poz. 549, Nr 117, poz. 678, Nr 133, poz. 767, Nr 160, poz. 964, Nr 191, poz. 1135, Nr 217, poz. 1280, Nr 233, poz. 1381 i Nr 240, poz. 1431, z 2012 r. poz. 611, z 2013 r. poz. 849, 905, 1036 i 1247 oraz z 2014 r. poz. 538.