Warszawa, dnia 22 listopada 2021 r.
Poz. 39

ZARZĄDZENIE NR 39/2021

GŁÓWNEGO INSPEKTORA TRANSPORTU DROGOWEGO

z dnia 22 listopada 2021 r.

zmieniające zarządzenie w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Głównym Inspektoracie Transportu Drogowego

Na podstawie art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[1)]), art. 32 ust. 3 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070) w związku z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) oraz art. 52 ust. 1 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2021 r. poz. 919 i 1005) zarządza się, co następuje:

§ 1. W zarządzeniu nr 43/2019 Głównego Inspektora Transportu Drogowego z dnia 19 września 2019 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Głównym Inspektoracie Transportu Drogowego (Dz. Urz. GITD z 2019 r. poz. 44 oraz z 2020 r. poz. 1, 17 i 25) w załączniku do zarządzenia wprowadza się następujące zmiany:

1) po § 5 dodaje się § 5a w brzmieniu:

„§ 5a. 1. Pracownicy GITD zobowiązani są do ochrony informacji powierzonych GITD na podstawie zawartych umów z podmiotami zewnętrznymi.

[1)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018 r., str. 2 i w Dz. Urz. UE L 74 z 04.03.2021 r., str. 35

2. Umowa z podmiotem zewnętrznym o powierzeniu informacji powinna w szczególności regulować następujące zagadnienia:

1) określenie i wymienienie informacji, jakie będą przetwarzane w GITD i będą uważane za wrażliwe, w szczególności: informacje dotyczące budowy i funkcjonowania Systemów Informatycznych, dane osobowe, dokumentacja techniczna, dokumentacja powykonawcza oraz informacje organizacyjne, finansowe, know-how i inne informacje o działalności Stron, które nie zostały ujawnione jak również informacje techniczne, technologiczne, organizacyjne lub inne, posiadające wartość gospodarczą, co do których Strony podjęły niezbędne działania w celu zachowania ich poufności lub przekazały je z zastrzeżeniem poufności;
2) określenie, w jaki sposób informacje, o których mowa w pkt 1 mają być chronione przez osoby, które zostały zobowiązane do poufności;
3) wskazanie, jakie działania osoby zobowiązanej będą stanowić naruszenie informacji, o których mowa w pkt 1, to jest (lub poprzez) określenie komu, kiedy i w jaki sposób takie informacje mogą być przekazywane, aby nie doszło do naruszenia;
4) określenie, że zobowiązanie do poufności trwa zarówno podczas obowiązywania umowy o pracę, współpracy, zlecenia, o dzieło, jak również po jej ustaniu przez określony czas wskazany w umowie o poufności oraz, że została przewidziana możliwość przedłużenia tego okresu;
5) skutki naruszenia zobowiązania do poufności, takie jak w szczególności odpowiedzialność dyscyplinarna oraz sankcje w sytuacji, gdy obowiązek poufności zostanie naruszony.

3. Nieuprawione ujawnienie, wykorzystanie lub pozyskanie informacji wrażliwej nie będzie miało miejsca, jeśli nastąpiło w jednym z następujących celów:

1) ochrony uzasadnionego interesu chronionego prawem;
2) w celu ujawnienia nieprawidłowości, uchybienia lub działania z naruszeniem prawa dla ochrony interesu publicznego;
3) gdy ujawnienie informacji stanowiących informację wrażliwą wobec przedstawicieli pracowników w związku z pełnieniem przez nich funkcji na podstawie przepisów prawa było niezbędne dla prawidłowego wykonywania tych funkcji.

4. Po zapoznaniu z rodzajem i zakresem informacji o których mowa w ust. 1 pracownicy GITD podpisują oświadczenie, o którym mowa w załączniku 1.”;

2) w § 11 pkt 3 otrzymuje brzmienie:

„3) informacja wrażliwa (tajemnica GITD) – informacje wewnętrzne GITD, wytworzone w GITD lub na jego rzecz oraz informacje pozyskane przez GITD od podmiotów zewnętrznych, w szczególności organów administracji państwowej i samorządowej, w tym na postawie zawartych umów, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje dostępne wewnątrz GITD i przeznaczone do użytku wewnętrznego. Informacje te mogą być udostępniane stronom trzecim (osobom lub podmiotom) na zasadzie „wiedzy uzasadnionej", w szczególności w związku z realizacją usług na podstawie zawartych umów, porozumień. Dokumenty zawierające informacje sklasyfikowane jako tajemnica GITD, w szczególności te udostępniane stronom trzecim, powinno się oznaczać co najmniej na pierwszej stronie (np.: w nagłówku lub stopce dokumentu) w przypadku dokumentów papierowych, lub w nazwie pliku w przypadku dokumentów elektronicznych, informacją np.: „tajemnica GITD", „do użytku wewnętrznego";";

3) Załącznik nr 1 do Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego otrzymuje brzmienie określone w załączniku nr 1 do niniejszego zarządzenia;

4) Załącznik nr 4 do Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego otrzymuje brzmienie określone w załączniku nr 2 do niniejszego zarządzenia.

§ 2. 1. W przypadku umów o powierzeniu informacji, zawartych z podmiotami zewnętrznymi przed wejściem w życie niniejszego zarządzenia, Główny Inspektor może samodzielnie określić rodzaj i zakres informacji stanowiących informację wrażliwą, o której mowa w § 1 pkt 2, związanych z realizacją umowy, wobec pracowników GITD, z uwzględnieniem zapisów zawartych w § 1 pkt 1.

2. Po zapoznaniu z rodzajem i zakresem informacji o których mowa w ust. 1 pracownicy Głównego Inspektoratu Transportu Drogowego podpisują oświadczenie, o którym mowa w § 1 pkt 3.

§ 3. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Główny Inspektor Transportu Drogowego**:** *A. Gajadhur*

Załączniki do zarządzenia nr 39/2021 Głównego Inspektora Transportu Drogowego z dnia 22 listopada 2021 r. (poz. 39)

Załącznik nr 1

„Załącznik nr 1 do Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego

Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji

Głównego Inspektoratu Transportu Drogowego oraz o zachowaniu poufności

Niniejszym oświadczam, że zostałam/em* zapoznana/y* z Polityką Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego oraz przepisami i podstawowymi zasadami dotyczącymi ochrony danych osobowych i zobowiązuję się do ich przestrzegania.

Zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych, w tym danych osobowych oraz informacji wrażliwych, do których mam lub będę miał/a* dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych wykonywanych na rzecz Głównego Inspektoratu Transportu Drogowego na podstawie:

……

W szczególności zobowiązuję się do ochrony informacji prawnie chronionych oraz informacji wrażliwych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem, a także do nieujawniania sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania zadań, jak i po ich zakończeniu.

Oświadczam, że bez upoważnienia nie będę wykorzystywał/a* informacji, w tym danych osobowych oraz informacji wrażliwych ze zbiorów prowadzonych przez Głównego Inspektora Transportu Drogowego, jak i zbiorów powierzonych do przetwarzania Głównemu Inspektorowi Transportu Drogowego przez inne podmioty. Mam świadomość, że celem Polityki Bezpieczeństwa Informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji, w tym danych osobowych, przetwarzanych w Głównym Inspektoracie Transportu Drogowego, a naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną, porządkową lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia

21 listopada 2008 r. o służbie cywilnej (Dz. U. 2021 poz. 1233), ustawie z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. 2020 poz. 1320), ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

* niepotrzebne skreślić

……. …….
miejsce i data złożenia oświadczenia czytelny podpis”

Załącznik nr 2

„Załącznik nr 4 do Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego

Bezpieczeństwo osobowe

§ 1. Przed zatrudnieniem

1. W ramach procesu zatrudniania i zmiany dotychczasowego zatrudnienia prowadzona jest weryfikacja osób planowanych do zatrudnienia.
2. Wobec osób, których dotyczy zmiana dotychczasowego zatrudnienia, weryfikacja prowadzona jest w zakresie zależnym od nowego stanowiska i jego wpływu na bezpieczeństwo informacji.
3. Jeżeli zmiana dotychczasowego zatrudnienia nie wiąże się m.in. z większymi uprawnieniami w systemach informatycznych, nie wiąże się z dostępem do szerszego zakresu danych i nie wpływa na bezpieczeństwo informacji, weryfikacja może zostać zaniechana.
4. Weryfikację należy prowadzić zgodnie z odpowiednimi przepisami prawa, regulacjami i zasadami w zakresie ochrony prywatności, danych osobowych i zatrudnienia, przyjętymi w GITD, uwzględniając zidentyfikowane ryzyka oraz klasyfikację informacji, do których przyszły pracownik będzie miał dostęp.
5. Informacje o wszystkich kandydatach gromadzone i przetwarzane są zgodnie z przepisami prawa w zakresie zatrudnienia i ochrony danych osobowych.
6. Za weryfikację oraz ochronę danych osobowych kandydatów odpowiadają w szczególności pracownicy komórki organizacyjnej właściwej do spraw kadrowych oraz członkowie komisji rekrutacyjnych. Nadzór nad ochroną danych osobowych kandydatów w zakresie uprawnień określonych w przepisach prawa sprawuje IOD.
7. W ramach prowadzonej rekrutacji należy weryfikować:
    1) tożsamość kandydata oraz poprawność podanych przez niego danych;
    2) wykształcenie i kwalifikacje zawodowe, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku, na podstawie złożonych dokumentów oraz np. rozmowy kwalifikacyjnej, testu kompetencji;
    3) przebieg dotychczasowego zatrudnienia, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku;
    4) korzystanie z pełni praw publicznych oraz karalność za umyślne przestępstwo lub umyślne przestępstwo skarbowe, na podstawie złożonego oświadczenia;
    5) gotowość do poddania się procedurze weryfikacji zgodnie z zasadami określonymi w ustawie o ochronie informacji niejawnych, w przypadku, gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku, na podstawie złożonego oświadczenia;
    6) przebieg dotychczasowego zatrudnienia w GITD, w przypadku zmiany zakresu obowiązków lub zmiany stanowiska / komórki organizacyjnej;

7) inne uzasadnione zakresem obowiązków i zadań na danym stanowisku, w granicach i na podstawie obowiązującego prawa.

8. Dokumentacja z procesu rekrutacji winna być przechowywana i chroniona zgodnie z obowiązującymi przepisami prawa w zakresie zatrudnienia oraz ochrony danych osobowych. Za właściwe przechowywanie dokumentacji odpowiadają pracownicy komórki organizacyjnej właściwej do spraw kadrowych.

§ 2. W trakcie zatrudnienia

1. Osoba zatrudniona jest do przestrzegania postanowień m.in.:
   1) obowiązującego Regulaminu pracy w GITD;
   2) obowiązujących PBI, PBT i PODO;
   3) obowiązujących w GITD innych, niż wskazane powyżej, polityk, planów, procedur, instrukcji oraz innych dokumentów odnoszących się do któregokolwiek z obszarów bezpieczeństwa: organizacyjnego, technicznego i technologicznego, osobowego, fizycznego;
   4) obowiązujących dokumentacji bezpieczeństwa systemów informatycznych, których jest użytkownikiem.
2. Osoba zatrudniona może uzyskać dostęp do zasobów informacyjnych GITD (dokumentów, nośników z danymi, systemów informatycznych, obiektów, stref dostępu, pomieszczeń itp.) w tym również urządzeń (komputerów, telefonów itp.), po podpisaniu oświadczenia o zobowiązaniu do zachowania poufności, o którym mowa w PODO.
3. Przed podjęciem przez osobę zatrudnioną zadań i obowiązków wymagających dostępu do informacji niejawnych, konieczne jest spełnienie wymagań prawnych związanych z dostępem do tych informacji wynikających z właściwych przepisów prawa i regulacji wewnętrznych w zakresie ochrony informacji niejawnych. Nadzór nad tym sprawuje Pełnomocnik ds. ochrony informacji niejawnych.
4. Bezpośredni przełożony osoby zatrudnionej jest zobowiązany:
   1) określić wymagania w zakresie dostępu do informacji oraz uprawnień do systemów informatycznych, niezbędne do wykonania powierzonych tej osobie obowiązków i zadań i złożyć wymagane w tym zakresie wnioski do właściwych merytorycznie komórek organizacyjnych;
   2) określić wymagania w zakresie dostępu do obiektów, stref, pomieszczeń itp. i wymagane w tym zakresie wnioski do właściwej dla danego obiektu, strefy, pomieszczenia itp. komórki organizacyjnej;
   3) wprowadzić taką osobę w obowiązki i odpowiedzialność związane z bezpieczeństwem informacji na danych stanowisku pracy;
   4) udzielać takiej osobie wytycznych określających wymagania w zakresie bezpieczeństwa informacji związanych z ich obowiązkami na danym stanowisku pracy;
   5) nadzorować stosowanie przez taką osobę postanowień PBI, PBT i PODO;
   6) umożliwiać udział w szkoleniach wewnętrznych z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony danych osobowych.

5. Właściciel systemu, którego użytkownikiem jest osoba zatrudniona, zobowiązany jest zapewnić:
    1) wprowadzenie tej osoby w obowiązki i odpowiedzialność w zakresie bezpieczeństwa tego systemu i informacji w nim przetwarzanych;
    2) udzielać tej osobie wytycznych w zakresie wymagań bezpieczeństwa systemu informatycznego;
    3) monitorowanie działań użytkownika w systemie informatycznym w odniesieniu do poufności, integralności i dostępności informacji z zapewnieniem atrybutów takich, jak rozliczalność, niezaprzeczalność, autentyczność i niezawodność.
6. IOD jest zobowiązany zapewnić osobie zatrudnionej:
    1) informację o obowiązkach spoczywających na tej osobie w związku z przetwarzaniem przez nią danych osobowych oraz doradzać jej w tej sprawie;
    2) działania zwiększające świadomość w zakresie ochrony danych osobowych;
    3) szkolenia z zakresu ochrony danych osobowych, na zasadach określonych w PODO;
    4) wykonywanie wobec tej osoby roli punktu kontaktowego we wszystkich sprawach związanych z przetwarzaniem jej danych osobowych oraz z wykonywaniem przysługujących jej praw na mocy RODO, na zasadach opisanych w PODO.
7. Pełnomocnik ds. bezpieczeństwa informacji zobowiązany zapewnić osobie zatrudnionej:
    1) szkolenia z zakresu bezpieczeństwa informacji;
    2) działania zwiększające świadomość w zakresie bezpieczeństwa informacji.

§ 3. Zmiana zatrudnienia

1. W przypadku zmiany, przez osobę zatrudnioną, stanowiska w obrębie tej samej komórki organizacyjnej lub przeniesieniem do innej komórki organizacyjnej, dotychczasowy bezpośredni przełożony tej osoby zobowiązany jest zapewnić:
    1) przejęcie akt spraw przez nią prowadzonych;
    2) złożenie wniosków o odebranie uprawnień do systemów informatycznych, z których osoba ta nie będzie korzystała wykonując zadania na nowym stanowisku;
    3) złożenie wniosku o odebranie specyficznych (innych niż dostęp do strefy tej komórki organizacyjnej lub przestrzeni wspólnej) uprawnień do obiektów, stref, pomieszczeń itp. do właściwej dla danego obiektu, strefy, pomieszczenia itp. komórki organizacyjnej.
2. W przypadku zmiany, przez osobę zatrudnioną, stanowiska w obrębie tej samej komórki organizacyjnej lub przeniesieniem do innej komórki organizacyjnej, nowy bezpośredni przełożony tej osoby zobowiązany jest zapewnić:
    1) złożenie wniosków o nadanie uprawnień do systemów informatycznych, z których osoba ta będzie korzystała wykonując zadania na nowym stanowisku;
    2) złożenie wniosku o nadanie innych, niż wskazane poniżej, uprawnień dostępu do obiektów, stref, pomieszczeń itp. do właściwej dla danego obiektu, strefy, pomieszczenia itp. komórki organizacyjnej.
3. W przypadku zmiany komórki organizacyjnej uprawnienia do systemów informatycznych powinny zostać całkowicie odebrane i nadane ponownie w nowej komórce organizacyjnej,

zgodnie z właściwym wnioskiem, na zasadach określonych w PBT. Powyższe nie dotyczy podstawowych uprawnień takich, jak dostęp do konta domenowego, poczty elektronicznej, zasobów wspólnych GITD.

4. W przypadku zmiany komórki organizacyjnej, jeżeli jest to konieczne ze względu na ograniczenia dostępu do poszczególnych stref i pomieszczeń, podstawowe uprawnienia do stref i pomieszczeń są modyfikowane na podstawie informacji kadrowej przekazywanej przez BDG–WKR.

§ 4. Nieobecność osoby zatrudnionej

1. W przypadkach dotyczących nieobecności osoby zatrudnionej wynikających np. z urlopu wypoczynkowego, urlopu bezpłatnego, zwolnienia lekarskiego lub innych sytuacjach losowych skutkujących dłuższą nieobecnością pracownika w pracy, kierujący komórką organizacyjną, w której osoba jest zatrudniona może zadecydować o czasowym zawieszeniu praw dostępu tej osoby do wewnętrznych zasobów i systemów informatycznych oraz stref i pomieszczeń podlegających szczególnej ochronie. Zawieszenie uprawnień jest realizowane na podstawie wniosku kierowanego przez tego kierującego komórką organizacyjną do Właściciela danego systemu, na zasadach opisanych w PBT lub obowiązujących w danym systemie (lub innym zasobie), lub do właściwej dla danej strefy lub pomieszczenia komórki organizacyjnej.
2. Jeżeli nieobecność pracownika wynosi 30 i więcej dni, w przypadku systemów informatycznych administrowanych przez BT, ASI tych systemów mogą dokonać zablokowania do nich dostępów na podstawie informacji przekazanej przez BDG – WKR.

§ 5. Zakończenie zatrudnienia

1. W przypadku zakończenia zatrudnienia przez osobę zatrudnioną, bezpośredni przełożony tej osoby jest zobowiązany zapewnić:
   1) wnioskowanie o odebranie uprawnień w systemach informatycznych, do których ta osoba posiadała dostęp;
   2) wnioskowanie o odebranie uprawnień dostępu do obiektów, stref, pomieszczeń, w szczególności nadanych w elektronicznych systemach kontroli dostępu;
   3) rozliczenie pracownika z udostępnionego wyposażenia związanego z przetwarzaniem informacji (komputerów, telefonów, nośników danych itp.);
   4) przejęcie akt spraw przez nią prowadzonych.
2. Odebranie uprawnień w systemach informatycznych, oraz uprawnień dostępu do obiektów, stref, pomieszczeń itp., w tym w elektronicznych systemach kontroli dostępu, jest realizowane zgodnie z zasadami opisanymi w PBT lub dokumentacji danego systemu informatycznego lub na podstawie wniosku do właściwej dla danego obiektu, strefy, pomieszczenia itp. komórki organizacyjnej.
3. Uprawnienia w systemach informatycznych, w tym elektronicznych systemach kontroli dostępu należy odbierać niezwłocznie z chwilą ustania zatrudnienia, z wyjątkiem sytuacji, gdy osoba kończąca zatrudnienie nie świadczy pracy przed ustaniem zatrudnienia. W takim

przypadku, uprawnienia powinny być odebrane już z chwilą ustania obowiązku świadczenia pracy (w tym również w przypadku rozpoczęcia urlopu (np. wykorzystanie zaległego urlopu)).

4. W przypadku zwolnienia pracownika z obowiązku świadczenia pracy (wypowiedzenie umowy o pracę z jednoczesnym zwolnieniem pracownika z obowiązku świadczenia pracy lub porozumienie pomiędzy pracodawcą i pracownikiem zwalniające czasowo tego drugiego z obowiązku świadczenia pracy), takiemu pracownikowi są odbierane prawa dostępu do zasobów wewnętrznych GITD i systemów informatycznych oraz innych, niż ogólne uprawnień dostępu (wypowiedzenie umowy o pracę) lub zawieszane (porozumienie w sprawie czasowego zwolnienia z obowiązku świadczenia pracy) na okres określony pomiędzy pracodawcą i pracownikiem. Odebranie lub zawieszenie praw dostępu jest realizowane na podstawie wniosku kierowanego przez kierującego komórką organizacyjną do Właściciela danego systemu, komórki organizacyjnej właściwej dla danego obiektu, strefy, pomieszczenia itp., na standardowych zasadach obowiązujących PBT lub w tym systemie (lub innym zasobie) lub na podstawie informacji z BDG – WKR.
5. Potwierdzenie zwrotu wyposażenia udostępnionego osobie kończącej zatrudnienie, w tym kart dostępu w elektronicznych systemach kontroli dostępu, kart mikroprocesorowych umożliwiających dostęp do systemów informatycznych, odbywa się zgodnie z wewnętrznymi procedurami obowiązującymi w GITD, w szczególności dotyczącymi zarządzania mieniem.

§ 6. Naruszenia bezpieczeństwa

1. Postępowanie wyjaśniające wobec osoby zatrudnionej naruszającej bezpieczeństwo informacji jest prowadzone na podstawie obowiązujących przepisów prawa i regulacji obowiązujących w GITD w zakresie odpowiedzialności służbowej i dyscyplinarnej.
2. Postępowanie wyjaśniające powinno być prowadzone po skutecznej weryfikacji i potwierdzeniu, że faktycznie nastąpiło naruszenie bezpieczeństwa informacji, na podstawie zgromadzonego i zabezpieczonego materiału dowodowego.
3. W sytuacji wystąpienia incydentu bezpieczeństwa związanego z kontami osoby zatrudnionej w systemach informatycznych i innych zasobach, do których ma dostęp, w tym elektronicznych systemach kontroli dostępu, może być wprowadzone zawieszenie lub odebranie praw dostępu, jeżeli zachodzi podejrzenie, że dane konto zostało wykorzystane lub jest wykorzystywane do wykonywania działań niezgodnych z obowiązującymi przepisami prawa, w szczególności określonymi w art. 267 – 269b Kodeksu Karnego. Decyzję o zawieszeniu lub odebraniu praw dostępu podejmuje Właściciel danego systemu, Dyrektor Generalny, Główny Inspektor lub jego zastępcy, w tym na podstawie rekomendacji i wniosków z analizy incydentu m.in. Dyrektora BT w odniesieniu do systemów informatycznych, Dyrektora BDG w odniesieniu do ochrony fizycznej, IOD, Pełnomocnika ds. bezpieczeństwa informacji lub Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni.
4. Zawieszenie lub odebranie praw dostępu osoby zatrudnionej może być również wynikiem realizacji polecenia wydanego przez właściwe organy śledcze uprawnione do wydania takiej dyspozycji m.in. w związku z prowadzonymi czynnościami śledczymi.

§ 7. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

1. Pełnomocnik ds. bezpieczeństwa informacji przy wsparciu BDG – WDZ organizuje szkolenia wstępne i okresowe z zakresu bezpieczeństwa informacji dla wszystkich osób zatrudnionych.
2. Szkolenia są prowadzone w formule e-learning z wykorzystaniem funkcjonującej w GITD wewnętrznej platformy szkoleniowej. Szkolenia kończą się testem.
3. Każda osoba zatrudniona jest zobowiązana do odbycia szkolenia wstępnego – w ciągu 2 miesięcy od rozpoczęcia zatrudnienia lub innej formy współpracy.
4. Każda osoba zatrudniona jest zobowiązana do odbycia szkolenia okresowego. Szkolenia okresowe są organizowane co najmniej raz na 2 lata, w formule e-learning.
5. Dopuszcza się organizowanie szkoleń stacjonarnych, o ile warunki epidemiczne, lokalowe lub techniczne pozwalają na taką formę szkolenia.
6. Szkolenia wewnętrzne z zakresu bezpieczeństwa informacji inne, niż wskazane w pkt. 1, mogą być zorganizowane na podstawie zapotrzebowania kierujących komórkami organizacyjnymi zgłoszonego do BDG – WDZ.”.