Warszawa, dnia 9 kwietnia 2026 r.

Poz. 12

ZARZĄDZENIE NR 12/2026

GŁÓWNEGO INSPEKTORA TRANSPORTU DROGOWEGO

z dnia 9 kwietnia 2026 r.

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

Na podstawie art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160) w związku z § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 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 2024 r. poz. 773), 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), 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 2023 r. poz. 1206), art. 21-25 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) oraz art. 52 ust. 1 ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2025 r. poz. 1490, 1676, 1795 i 1843) zarządza się, co następuje:

§ 1. W załączniku do zarządzenia nr 17/2023 Głównego Inspektora Transportu Drogowego w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Głównym Inspektoracie Transportu Drogowego (Dz. Urz. GITD z 2023 r. poz. 17) wprowadza się następujące zmiany:

1) w § 30 w ust. 3 pkt 1 otrzymuje brzmienie:

„1) realizacja zadań określonych szczegółowo w PODO, w szczególności współpraca z Pełnomocnikiem do spraw bezpieczeństwa informacji przy prowadzeniu rejestrów czynności przetwarzania oraz kategorii czynności przetwarzania;”;

2) w załączniku nr 6 do Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego:

a) w § 1:

- w ust. 1 pkt 1 otrzymuje brzmienie:

„1) w przypadku naruszeń ochrony danych osobowych – Pełnomocnik do spraw bezpieczeństwa informacji;”,

- w ust. 2 pkt 1 otrzymuje brzmienie:

„1) Pełnomocnik do spraw bezpieczeństwa informacji – rejestr naruszeń ochrony danych osobowych;”,

b) w § 2 w ust. 2 pkt 1 otrzymuje brzmienie:

„1) W przypadku zidentyfikowania zagrożenia naruszenia ochrony danych osobowych ASI niezwłocznie informuje Pełnomocnika do spraw bezpieczeństwa informacji.”,

c) w § 3 w ust. 8 pkt 1 otrzymuje brzmienie:

„1) dla naruszeń ochrony danych osobowych Pełnomocnik do spraw bezpieczeństwa informacji dokonuje zgłoszenia do PUODO w terminie do 72 godzin od zaistnienia lub wykrycia naruszenia;”,

d) tytuł § 4 otrzymuje brzmienie:

„Działania Pełnomocnika do spraw bezpieczeństwa informacji w zakresie obsługi naruszeń ochrony danych osobowych”

e) § 4 otrzymuje brzmienie:

„§ 4. 1. Pełnomocnik do spraw bezpieczeństwa informacji dokonuje analizy informacji dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu Pełnomocnik do spraw bezpieczeństwa informacji może występować o wszelkie informacje, wyjaśnienia i opinie do komórek organizacyjnych, pracowników, w tym kierujących komórkami organizacyjnymi, którzy są zobowiązani do przekazania informacji, wyjaśnień lub opinii bez zbędnej zwłoki, w możliwie najkrótszym terminie.

2. Na podstawie dokonanej analizy Pełnomocnik do spraw bezpieczeństwa informacji ocenia, czy stwierdzone zdarzenie może skutkować ryzykiem naruszenia praw.

3. W przypadku stwierdzenia występowania ryzyka naruszenia praw i wolności osób fizycznych, w szczególności ryzyka wysokiego i potwierdzenia prawidłowości

kwalifikacji zdarzenia jako naruszenie ochrony danych osobowych Pełnomocnik do spraw bezpieczeństwa informacji informuje o tym Głównego Inspektora.

4. Pełnomocnik do spraw bezpieczeństwa informacji odpowiada za zgłoszenie stwierdzonego naruszenia ochrony danych osobowych do PUODO.

5. Pełnomocnik do spraw bezpieczeństwa informacji sprawuje nadzór nad prawidłową realizacją obowiązku poinformowania osób, których dane osobowe zostały naruszone, przez komórki organizacyjne, w których naruszenie wystąpiło. Komórki te przygotowują i wysyłają zawiadomienia podpisywane przez kierującego komórką organizacyjną po uprzedniej konsultacji treści z Pełnomocnikiem do spraw bezpieczeństwa informacji oraz IOD.

6. Informację o zrealizowaniu czynności poinformowania Pełnomocnik do spraw bezpieczeństwa informacji umieszcza w rejestrze naruszeń ochrony danych osobowych oraz przekazuje do PUODO.

7. Pełnomocnik do spraw bezpieczeństwa informacji pełni nadzór nad obsługą incydentu przez właściwe komórki organizacyjne.”;

3) w załączniku nr 7 do Polityki Bezpieczeństwa Informacji Głównego Inspektoratu Transportu Drogowego:

a) w § 16 ust. 2 otrzymuje brzmienie:

„2. Każdy przypadek naruszenia lub podejrzenia wystąpienia naruszenia ochrony danych osobowych należy zgłosić niezwłocznie na ogólny adres e-mail dedykowany do zgłaszania naruszeń ochrony danych osobowych, incydentów bezpieczeństwa informacji oraz incydentów dotyczących cyberbezpieczeństwa: incydent@gitd.gov.pl.”,

b) w § 17 ust. 9 otrzymuje brzmienie:

„9. Pracownicy, o których mowa w ust. 5 mają obowiązek informowania bez zbędnej zwłoki Pełnomocnika do spraw bezpieczeństwa informacji o danych podmiotu przetwarzającego po zawarciu umowy powierzenia oraz o czasie jej obowiązywania, celem aktualizacji rejestru czynności przetwarzania. Pełnomocnik do spraw bezpieczeństwa informacji musi być również bez zbędnej zwłoki poinformowany o zakończeniu obowiązywania umowy powierzenia, nie później jednak niż przed terminem jej wygaśnięcia.”,

c) w § 18 ust. 3 otrzymuje brzmienie:

„3. Właściciel informacji, której dotyczy powierzenie przetwarzania danych osobowych, zapewnia realizację obowiązków określonych w umowie powierzenia przetwarzania danych osobowych, w szczególności:

1) określanie i wdrażanie zabezpieczeń, udzielanie upoważnień do przetwarzania danych osobowych;
2) realizowanie obowiązków informacyjnych;
3) przeprowadzanie ocen skutków dla ochrony danych;
4) prowadzenie pozostałej wymaganej dokumentacji dotyczącej przetwarzania powierzonych danych osobowych

– z zastrzeżeniem czynności przypisanych do realizacji przez Pełnomocnika do spraw bezpieczeństwa informacji oraz IOD.”,

d) w § 21:

- ust. 1-3 otrzymują brzmienie:

„§ 21. 1. Pełnomocnik do spraw bezpieczeństwa informacji prowadzi rejestr czynności przetwarzania i wykaz kategorii czynności przetwarzania oraz rejestr wszystkich kategorii czynności przetwarzania w przypadku, gdy to Główny Inspektor jest podmiotem przetwarzającym.

2. Rejestry, o których mowa w ust. 1 są prowadzone w postaci elektronicznej.

3. Pełnomocnik do spraw bezpieczeństwa informacji ma obowiązek:

1) zapewnić integralność rejestrów i wykazów, o których mowa w ust. 1, a w odniesieniu do opisu zabezpieczeń – również poufność;
2) okresowo – nie rzadziej niż raz w roku – dokonywać weryfikacji, przy udziale właścicieli informacji, czy czynności przetwarzania opisane w rejestrach i wykazach o których mowa w ust. 1, są aktualne oraz jeżeli to wymagane – dokonać aktualizacji rejestru na podstawie informacji przekazanych przez właścicieli informacji;
3) zapewnić dostępność rejestrów i wykazów, o których mowa w ust. 1.”

- ust. 6 otrzymuje brzmienie:

„6. Właściciele informacji mają obowiązek:

1) współpracować z Pełnomocnikiem do spraw bezpieczeństwa informacji przy prowadzeniu rejestrów i wykazów, o których mowa w ust. 1, w szczególności poprzez przekazywanie informacji niezbędnych do ich prawidłowego prowadzenia i zapewnienie poprawności danych w nich zawartych;
2) zapewniać aktualność zapisów w rejestrach i wykazach, o których mowa w ust. 1 oraz przekazywać bez zbędnej zwłoki Pełnomocnikowi do spraw bezpieczeństwa informacji dane niezbędne do ich aktualizacji, w tym w przypadku zmian czynności przetwarzania w szczególności zmian celów przetwarzania, kategorii osób, zakresu danych, odbiorców danych, podmiotów przetwarzających.”,

e) § 23 otrzymuje brzmienie:

„§ 23. 1. Pełnomocnik do spraw bezpieczeństwa informacji, przy wsparciu Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni oraz IOD ustala, czy:

1) naruszenia ochrony danych osobowych stanowią incydent w podmiocie publicznym i wymagają zgłoszenia do CSIRT w ciągu 24 godzin od ich wykrycia – kryterium klasyfikacji określa ustawa o krajowym systemie cyberbezpieczeństwa oraz procedura zgłaszania incydentów określona w załączniku nr 6 do PBI;
2) incydenty cyberbezpieczeństwa stanowią naruszenie ochrony danych osobowych i wymagają zgłoszenia do PUODO w ciągu 72 godzin od ich wykrycia, ewentualnie powiadomienia osób, których dane są objęte naruszeniem – kryterium klasyfikacji określa RODO, ustawa oraz procedura zgłaszania incydentów określona w załączniku nr 6 do PBI;
3) incydenty bezpieczeństwa informacji stanowią naruszenie ochrony danych osobowych i wymagają zgłoszenia do PUODO w ciągu 72 godzin od ich wykrycia, ewentualnie powiadomienia osób, których dane są objęte naruszeniem – kryterium klasyfikacji określa RODO, ustawa oraz procedura zgłaszania incydentów określona w załączniku nr 6 do PBI.

2. Obsługę i wyjaśnianie naruszeń ochrony danych osobowych koordynuje Pełnomocnik do spraw bezpieczeństwa informacji. W ramach tych czynności Pełnomocnik do spraw bezpieczeństwa informacji jest uprawniony do żądania od wszystkich pracowników udzielenia wyjaśnień w związku z obsługiwanym naruszeniem, w tym do uzyskiwania materiałów mogących stanowić dowód w postępowaniu. Do przekazywania informacji wrażliwych lub informacji prawnie chronionych należy stosować wymagania i wytyczne dotyczące zapewnienia poufności informacji, m.in. dostępne mechanizmy szyfrowania.

3. Pełnomocnik do spraw bezpieczeństwa informacji rejestruje wszystkie naruszenia ochrony danych osobowych w rejestrze naruszeń ochrony danych osobowych oraz przechowuje uwierzytelnione przez siebie kopie zgłoszeń naruszeń do PUODO.

4. Rejestr naruszeń ochrony danych osobowych prowadzony przez Pełnomocnika do spraw bezpieczeństwa informacji obejmuje następujące informacje:

1) datę i godzinę zgłoszenia faktu naruszenia ochrony danych osobowych;
2) imię i nazwisko osoby zgłaszającej naruszenie;
3) opis lub symptomy naruszenia zabezpieczenia, opis charakteru naruszenia i okoliczności jego wystąpienia, w tym w miarę możliwości wskazanie kategorii

i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów (wykazów) danych osobowych, których dotyczy naruszenie;

4) opis możliwych konsekwencji naruszenia;

5) opis podjętych działań i decyzji, opis środków zastosowanych lub proponowanych przez administratora i podjętych działań naprawczych i zapobiegawczych w celu zaradzenia naruszeniu (usunięcia naruszenia), w tym zminimalizowania jego ewentualnych negatywnych skutków oraz uniknięcia podobnych naruszeń w przyszłości;

6) przebieg wyjaśniania naruszeń, w tym wskazanie, czy informację o wystąpieniu naruszenia przekazywano do osób, których dane są danym naruszeniem objęte.

5. Kopie zgłoszeń naruszeń do PUODO, które stanowią dopełnienie rejestru naruszeń ochrony danych osobowych zawierają informacje, o których mowa w ust. 4 pkt 1-6 – w takiej sytuacji informacji w rejestrze nie powtarza się. Zakres informacyjny rejestru naruszeń ochrony danych osobowych może być rozszerzony o dodatkowe informacje, jeżeli Pełnomocnik do spraw bezpieczeństwa informacji lub administrator danych identyfikują taką potrzebę.

6. Pełnomocnik do spraw bezpieczeństwa informacji prowadzi rejestr naruszeń ochrony danych osobowych w formie elektronicznej i zapewnia jego poufność, integralność oraz dostępność.

7. Zgłoszenia naruszenia ochrony danych osobowych do PUODO dokonuje Pełnomocnik do spraw bezpieczeństwa informacji w imieniu Głównego Inspektora, bez zbędnej zwłoki, ale nie później niż w ciągu 72 godzin od jego wykrycia, przekazując w zgłoszeniu co najmniej (jeżeli są dostępne w chwili zgłoszenia) informacje określone w art. 33 ust. 3 RODO lub art. 44 ust. 4 ustawy – w zależności, którego przetwarzania naruszenie dotyczy.

8. Pełnomocnik do spraw bezpieczeństwa informacji dokonuje zgłoszenia jednym ze sposobów wskazanych przez UODO. Dokonując zgłoszenia, Pełnomocnik do spraw bezpieczeństwa informacji może korzystać z interaktywnych formularzy dostępnych na stronie UODO lub innych formularzy udostępnionych tam przez Urząd.

9. Jeżeli w chwili zgłoszenia do PUODO nie są dostępne wszystkie wymagane informacje, Pełnomocnik do spraw bezpieczeństwa informacji uzupełnia zgłoszenie niezwłocznie po ich uzyskaniu od pracowników zaangażowanych w wyjaśnianie zdarzenia i minimalizowanie jego skutków.

10. W przypadku, gdy źródłem informacji o naruszeniu ochrony danych jest osoba lub podmiot zewnętrzny, Pełnomocnik do spraw bezpieczeństwa informacji informuje o naruszeniu Głównego Inspektora, bez zbędnej zwłoki, najpóźniej z chwilą wysyłania zgłoszenia naruszenia do PUODO.

11. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Główny Inspektor bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Czynności tej w imieniu Głównego Inspektora dokonuje właściciel informacji, której dotyczy naruszenie, po uprzedniej konsultacji powiadomienia z Pełnomocnikiem do spraw bezpieczeństwa informacji oraz IOD.

12. Do przypadków, w których poinformowanie jest obowiązkowe należą sytuacje, w których naruszenie prowadzi do dyskryminacji, kradzieży tożsamości, oszustwa, straty finansowej lub uszczerbku na reputacji. Jeżeli naruszenie dotyczy danych osobowych szczególnej kategorii, przyjmuje się, że, takie naruszenie może prowadzić do wskazanych wyżej szkód. Nie jest konieczne, aby wysokie ryzyko zmaterializowało się, czyli faktycznie doszło do naruszenia praw lub wolności osoby fizycznej.

13. Obowiązek zawiadomienia należy zrealizować tak szybko, jak pozwalają na to okoliczności danej sprawy. Należy przyjąć, że im poważniejsze jest ryzyko naruszenia praw lub wolności podmiotu danych, tym szybciej powinno nastąpić zawiadomienie.

14. Gdy jest to uzasadnione oraz zgodne z zaleceniami organów ścigania wysłanie zawiadomienia o naruszeniu do osób fizycznych, na które wywiera ono wpływ może być opóźnione do momentu, w którym takie zawiadomienie nie zaszkodzi takim postępowaniom, zgodnie z art. 45 ust. 6 ustawy. Jeżeli zawiadomienie o naruszeniu danych osobowych zostało wysłane z opóźnieniem, właściciel informacji ma obowiązek poinformować Pełnomocnika do spraw bezpieczeństwa informacji oraz IOD o powodach tego opóźnienia celem udokumentowania w rejestrze naruszeń ochrony danych osobowych.

15. W przypadku, o którym mowa w art. 26 ust. 1 ustawy zawiadomienie można również ograniczyć lub pominąć (obowiązek poinformowania Pełnomocnika do spraw bezpieczeństwa informacji oraz IOD w celu udokumentowania powodu ograniczenia lub pominięcia zawiadomienia, w rejestrze naruszeń ochrony danych osobowych).

16. Zawiadomienie musi zawierać wymagane prawem elementy wskazane poniżej:

1) charakter naruszenia ochrony danych osobowych;

2) imię i nazwisko oraz dane kontaktowe IOD lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
4) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

17. Do zawiadomienia stosuje się zasady przejrzystości, prostoty i zrozumiałości informacji.

18. Wybierając środek komunikacji należy pamiętać, że zawiadomienie musi zostać dostarczone adresatowi w możliwie najkrótszym czasie, przy czym wybór środka komunikacji musi uwzględniać informacje teleadresowe o danej osobie, które administrator posiada.

19. Jeżeli właściciel informacji nie jest w stanie zawiadomić danej osoby fizycznej o naruszeniu, ponieważ posiadane dane są niewystarczające do skontaktowania się z tą osobą, w takim szczególnym przypadku właściciel informacji informuje taką osobę tak szybko, jak jest to rozsądnie wykonalne (np. gdy osoba fizyczna skorzysta z przewidzianego w art. 15 RODO prawa do uzyskania dostępu do swoich danych osobowych i dostarczy dodatkowe informacje wymagane do skontaktowania się z nią).

20. Właściciel informacji nie wysyła zawiadomienia, jeżeli:

1) zastosowane zostały, przed wystąpieniem naruszenia odpowiednie techniczne i organizacyjne środki w celu ochrony danych osobowych, w szczególności środki uniemożliwiające odczyt danych osobom, które nie są uprawnione do dostępu do tych danych;
2) natychmiast po wystąpieniu naruszenia zostały podjęte działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej;
3) skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku, z zastrzeżeniem ust. 15.

21. W przypadku, gdy skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku, Główny Inspektor w porozumieniu z Pełnomocnikiem do spraw bezpieczeństwa informacji oraz właścicielem informacji, po konsultacji z IOD wydaje publiczny komunikat lub stosuje podobny środek, aby w równie skuteczny sposób poinformować osoby o naruszeniu dotyczących ich danych osobowych.

22. Do naruszeń danych osobowych, których przetwarzanie zostało powierzone Głównemu Inspektorowi, zastosowanie mają powyższe zasady, ale przede wszystkim wymagania szczegółowo określone w umowach lub porozumieniach z administratorami tych danych osobowych dotyczących danego powierzenia.”.

§ 2. Osobę zastępującą Pełnomocnika do spraw bezpieczeństwa informacji w czasie jego nieobecności Główny Inspektor wyznacza w drodze decyzji, na wniosek Pełnomocnika do spraw bezpieczeństwa informacji, oraz za zgodą kierującego komórką organizacyjną, w której ta osoba jest zatrudniona.

§ 3. Zarządzenie wchodzi w życie z dniem ogłoszenia.

p.o. Głównego Inspektora Transportu Drogowego**:** *Robert Koźlak*