WOJEWODA DOLNOŚLĄSKI

PNK-K.431.2.6.2026.BJ

Pan
Tomasz Resler
Dolnośląski Wojewódzki Inspektor
Inspekcji Handlowej we Wrocławiu

ul. Ofiar Oświęcimskich 15A
50-069 Wrocław

WYSTĄPIENIE POKONTROLNE

(Dolnośląski Wojewódzki Inspektor Inspekcji Handlowej we Wrocławiu
wniósł zastrzeżenia do projektu wystąpienia pokontrolnego
doręczonego w dniu 10 lipca 2026 r.
Zastrzeżenia zostały uwzględnione w części.
Wystąpienie pokontrolne sporządzone zostało na podstawie
projektu wystąpienia pokontrolnego oraz stanowiska w sprawie zastrzeżeń)

Wrocław, dnia 3 sierpnia 2026 r.

I. Informacje organizacyjne

Jednostka kontrolowana	Wojewódzki Inspektorat Inspekcji Handlowej we Wrocławiu, ul. Ofiar Oświęcimskich 15A, 50-069 Wrocław
Kierownik jednostki kontrolowanej	Tomasz Resler – Dolnośląski Wojewódzki Inspektor Inspekcji Handlowej we Wrocławiu (dalej jako: DWIIH). Do dnia 6 kwietnia 2024 r. funkcję piastował Pan Janusz Szydłowski.
Zakres kontroli	Bezpieczeństwo teleinformatyczne jednostki – działanie systemów teleinformatycznych oraz rejestrów publicznych używanych do realizacji zadań administracji rządowej na podstawie przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz. U. z 2025 r. poz. 1703, z późn. zm., dalej jako: ustawa o informatyzacji) oraz 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, dalej jako: r.k.r.i.).
Podstawa prawna kontroli	Art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie[1] oraz art. 1 pkt 1 i art. 6 ust. 4 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[2] w zw. z art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji oraz na podstawie zatwierdzonego w dniu 22 grudnia 2025 r. przez Wojewodę Dolnośląskiego planu kontroli na I półrocze 2026 r. (PNK-K.430.2.2025.TS), imienne upoważnienia Wojewody Dolnośląskiego z dnia 13 kwietnia 2026 r.
Data rozpoczęcia i zakończenia czynności kontrolnych	13 kwietnia 2026 r. – 12 czerwca 2026 r.
Kontrolerzy	1. Bartosz Jędrysiak, starszy inspektor wojewódzki z Wydziału Prawnego, Nadzoru i Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, upoważnienie nr 43 z dnia 13 kwietnia 2026 r., znak: PNK-K.0030.43.2026.BJ; 2. Klaudia Majewska, inspektor wojewódzki z Wydziału Prawnego, Nadzoru i Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, upoważnienie nr 44 z dnia 13 kwietnia 2026 r., znak: PNK-K.0030.44.2026.BJ; 3. Sebastian Mika, starszy informatyk z Zespołu Informatyki i Cyberbezpieczeństwa Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, upoważnienie nr 45 z dnia 13 kwietnia 2026 r., znak PNK-K.0030.45.2026.BJ; 4. Piotr Szagdaj, główny informatyk z Zespołu Informatyki i Cyberbezpieczeństwa Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, upoważnienie nr 46 z dnia 13 kwietnia 2026 r., znak PNK-K.0030.46.2026.BJ. [dowód: akta kontroli str.: 22-29]

[1] Tekst. jedn. Dz. U. z 2025 r., poz. 428.
[2] Tekst. jedn. Dz. U. z 2026 r., poz. 158.

II. Ocena kontrolowanej jednostki

Mając na uwadze poniższe ustalenia oraz przyjęte w programie kontroli zasady oceniania, sposób realizacji przez Dolnośląskiego Wojewódzkiego Inspektora Inspekcji Handlowej we Wrocławiu zadania stanowiącego przedmiot niniejszej kontroli oceniono **pozytywnie pomimo stwierdzonych nieprawidłowości.**

III. Ustalenia kontroli

Celem kontroli była ocena działalności jednostki kontrolowanej w zakresie bezpieczeństwa teleinformatycznego, dokonana na podstawie ustalonego stanu faktycznego przy zastosowaniu przyjętych kryteriów kontroli, a w przypadku stwierdzenia nieprawidłowości ustalenie ich zakresu, przyczyn i skutków, a także sformułowanie zaleceń pokontrolnych zmierzających do usunięcia nieprawidłowości.

Ocena działalności jednostki kontrolowanej w zakresie objętym kontrolą została dokonana na podstawie ustalonego stanu faktycznego, w oparciu o udostępnione w toku wykonywania czynności kontrolnych dokumenty, złożone przez kontrolowanego wyjaśnienia oraz protokoły z oględzin, przy zastosowaniu kryteriów kontroli wynikających z ustawy o kontroli w administracji rządowej, tj. legalności oraz rzetelności.

[dowód: akta kontroli str.: 53-81]

Obszar A dot. świadczenia usług drogą elektroniczną.

Do jednych z podstawowych celów funkcjonowania urzędu zalicza się realizowanie usług w sposób szybki, sprawny i możliwie jak najbardziej przyjazny dla obsługiwanego podmiotu. Realizację powyższych postulatów w praktyce można uzyskać świadcząc te usługi poprzez platformę elektroniczną dostępną za pośrednictwem sieci Internet. Taki sposób realizacji umożliwia załatwianie spraw w urzędzie bez wychodzenia z domu lub z dowolnego innego miejsca, w którym klient ma dostęp do Internetu. Ma to na celu ułatwienie, jak i usprawnienie obsługi podmiotów, a także eliminowanie korespondencji papierowej na rzecz elektronicznych formularzy i dokumentacji, wypełnianych i przesyłanych za pośrednictwem przewidzianych ustawowo form komunikacji.

Zgodnie z art. 16 ust. 1a ustawy o informatyzacji podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji oraz zapewnia jej obsługę. Ponadto, w myśl art. 147 ust. 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (tekst jedn. Dz. U. z 2026 r., poz. 3) korespondencja pomiędzy podmiotami publicznymi, do dnia 30 września 2029 r., jest równoważna w skutkach z korespondencją za pośrednictwem doręczeń elektronicznych. W wyniku kontroli ustalono, iż podmiot kontrolowany, na stronie podmiotowej Biuletynu Informacji Publicznej (dalej: „BIP") https://www.gov.pl/web/wiih-wroclaw udostępnia adres Elektronicznej Skrzynki Podawczej: /tig053vv26/SkrytkaESP. Stwierdzono również, iż jednostka kontrolowana zamieściła adres ESP prawidłowo w formie identyfikatora URI oraz zamieściła warunki doręczania do podmiotu dokumentów elektronicznych, co jest zgodne z przepisem § 3 ust. 1 Rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. *w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych* (tekst jedn. Dz. U. z 2018 poz. 180).

Ponadto, w myśl art. 8 ustawy o doręczeniach elektronicznych podmiot publiczny jest obowiązany do posiadania adresu do doręczeń elektronicznych wpisanego do bazy

adresów elektronicznych, powiązanego z publiczną usługą rejestrowanego doręczenia elektronicznego. W toku kontroli ustalono, iż na stronie BIP Kontrolowany udostępnia adres do doręczeń elektronicznych: AE:PL-72024-15247-AJRAE-30.

Co więcej, Kontrolowany udostępnia również na stronie BIP kontaktowy adres e-mail: sekretariat@wiih.wroclaw.pl.

Powyższe oceniono pozytywnie.

[dowód: akta kontroli str.: 466-518]

W toku kontroli przeprowadzono test wysyłkowy za pośrednictwem adresu e-mail, platformy ePUAP oraz doręczeń elektronicznych, polegający na przekazaniu na adresy elektroniczne kontrolowanej jednostki oraz przekazaniu przez Kontrolowanego na adresy elektroniczne Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, plików w trzech formatach danych: .doc, .pdf, .jpg, wskazanych w załączniku do Rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych oraz załącznikiem nr 2 do r.k.r.i. W wyniku przeprowadzonych testów stwierdzono, iż Wojewódzki Inspektorat Inspekcji Handlowej we Wrocławiu (dalej jako: WIIH) zapewnia możliwość świadczenia usług w postaci elektronicznej na rzecz klientów, co należy ocenić pozytywnie.

[dowód: akta kontroli str.: 427-429]

Zgodnie z § 5 ust. 2 pkt 1 i 4 r.k.r.i. interoperacyjność na poziomie organizacyjnym osiągana jest przez informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty oraz publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

W toku kontroli ustalono, że jednostka kontrolowana udostępnia na stronie podmiotowej BIP informacje o możliwym świadczeniu usług drogą elektroniczną oraz wskazuje procedury obowiązujące przy załatwianiu następujących spraw:

a) Złożenie wniosku o pozasądowe rozpatrzenie sporu konsumenckiego;
b) Złożenie wniosku o rozpatrzenie sprawy przed Stałym Sądem Polubownym;
c) Złożenie skargi lub wniosku;
d) Złożenie petycji;
e) Uzyskanie informacji publicznej;
f) Złożenie wniosku o wpis na listę rzeczoznawców;
g) Dokonanie zgłoszenia w trybie ustawy o ochronie sygnalistów;
h) Złożenie wniosku o zapewnienie dostępności;
i) Złożenie wniosku o ulgę dot. kar administracyjnych.

Analiza przedmiotowych opisów procedur[3] wskazuje, iż w odniesieniu do procedur wskazanych w literach a), b), c) oraz i) jako jedną z możliwych form złożenia pism wskazano platformę ePUAP, mimo iż obowiązującym sposobem doręczeń od 1 stycznia 2026 r. jest platforma eDoręczeń. Odnośnie procedur wskazanych w punktach d), e) i f) nie wskazano w ogóle możliwości wniesienia pism w postaci elektronicznej, natomiast w odniesieniu do procedury wskazanej w literze g), przy załatwianiu sprawy drogą elektroniczną ograniczono się jedynie do adresu e-mail.

[3] Analizy dokonano na podstawie dostępu do strony BIP Kontrolowanego w dniu 22 maja 2026 r. i utrwalono stan zastany poprzez dokonania zrzutów ekranu, wskazujących datę i godzinę dostępu do strony.

Powyższe nieprawidłowości stanowią naruszenie § 5 ust. 2 pkt 4 r.k.r.i.

[dowód: akta kontroli str.: 466-518]

Korespondencja w toku kontroli z jednostką kontrolowaną wykazała, że Elektroniczna Skrzynka Podawcza działająca w ramach platformy ePUAP oraz eDoręczeń jednostki kontrolowanej realizuje obowiązek automatycznego generowania poświadczenia przedłożenia, zgodnie z obowiązkiem wynikającym z art. 4 ustawy o doręczeniach elektronicznych oraz § 13 Rozporządzenia Prezesa Rady Ministrów *w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.*

W wyniku kontroli ustalono również, że Elektroniczna Skrzynka Podawcza działająca w ramach platformy ePUAP oraz eDoręczeń jednostki kontrolowanej udostępnia adresatowi dokumentu elektronicznego poświadczenie doręczenia w celu umożliwienia podpisania poświadczenia doręczenia, zgodnie z art. 4 ustawy o doręczeniach elektronicznych oraz § 14 - §16 Rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. *w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych.*

[dowód: akta kontroli str.: 427-429]

Mając na uwadze powyższe ustalenia, wskazany obszar należy ocenić **pozytywnie pomimo stwierdzonych nieprawidłowości.**

Obszar B dot. współpracy systemów teleinformatycznych z innymi systemami (interoperacyjność).

Realizując czynności kontrolne analizie poddano 3 użytkowane w Dolnośląskim Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu (dalej jako: WIIH) systemy teleinformatyczne wskazane w przekazanej przez Kontrolowanego informacji przedkontrolnej tj. EZD RP, Vulcan oraz Zabbix.

Zgodnie z brzmieniem § 18 ust. 1 r.k.r.i. systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia. Jednym z formatów danych jest format .xml *(Extensible Markup Language)*.

Czynności kontrolne wykazały, że systemy EZD RP, Vulcan, oraz Zabbix są systemami ogólnopolskimi, umożliwiającymi wymianę danych z innymi systemami – m. in. za pomocą pliku w formacie .xml, ze stroną kodową UTF-8. Dokonane ustalenia pokrywają się z oświadczeniami producentów systemów. Powyższe jest zgodne z § 18 ust. 1 r.k.r.i., a stosowanie standardu UTF-8 wypełnia dyspozycję § 17 ust. 1 r.k.r.i., co należy ocenić pozytywnie.

[dowód: akta kontroli str.: 139-187]

W wyniku przeprowadzonych testów wysyłkowych, o których wspomniano w części dotyczącej świadczenia usług drogą elektroniczną ustalono, że system Elektronicznego Zarządzania Dokumentacją umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu działania podmiotu w formatach danych określonych w załącznikach nr 2 i 3 do r.k.r.i., co jest zgodne z § 18 ust. 2 r.k.r.i.

[dowód: akta kontroli str.: 427-429]

Mając na uwadze powyższe ustalenia, wskazany obszar należy ocenić **pozytywnie.**

Obszar C dot. Systemu Zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych.

1. **Dokumenty z zakresu systemu bezpieczeństwa informacji.**

W myśl § 19 ust. 1 r.k.r.i., podmiot realizujący zadania publiczne zobowiązany jest do opracowania i ustanowienia, wdrożenia i eksploatowania, monitorowania i przeglądania, a także utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji[4] zapewniającego poufność, dostępność oraz integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Mając na uwadze powyższe, niezbędnym jest opracowanie kompleksowej dokumentacji SZBI, w tym również odpowiednich regulacji wewnętrznych, a także zapewnienia ich aktualizacji w zakresie dot. zmieniającego się otoczenia. Dokumentacja musi być sporządzona w sposób precyzyjny, nie może pozostawiać wątpliwości co do stosowania zawartych w niej reguł, ponieważ dotyczy wszystkich użytkowników mających dostęp oraz przetwarzających informacje. Opracowanie wszechstronnej dokumentacji SZBI umożliwia efektywne wykonywanie zadań w jednostce, a także właściwe zarządzanie bezpieczeństwem informacji oraz zabezpieczenie interesów jednostki. Kompleksowe podejście do omawianej tematyki powinno uwzględniać rozmaite kategorie informacji, odnosząc się do ich zabezpieczenia, z uwzględnieniem właściwej klasyfikacji, zależnej od profilu działalności podmiotu, m.in. bezpieczeństwo osobowe, informatyczne, fizyczne, prawne, czy technologie oraz tajemnice jednostki. Jednym z najważniejszych elementów, wchodzących w zakres dokumentacji SZBI jest Polityka Bezpieczeństwa Informacji, która powinna zostać zatwierdzona przez kierownictwo podmiotu, przekazana pracownikom do zapoznania, a następnie regularnie poddawana przeglądowi. Doskonalenie całego SZBI jest szczególnie istotne, ponieważ zapewnia aktualność wszystkich regulacji, co znacząco wpływa na zagwarantowanie właściwego poziomu bezpieczeństwa.

W toku kontroli ustalono, iż w WIIH opracowano następujące dokumenty z zakresu bezpieczeństwa informacji:

- Politykę Ochrony Danych Osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu wprowadzoną zarządzeniem nr 7/2026 z dnia 10 lutego 2026 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu[5];
- Instrukcję postępowania w przypadku naruszenia ochrony danych osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu (Załącznik nr 3 do Polityki Ochrony Danych Osobowych)[6];
- Instrukcję zarządzania systemem informatycznym w związku z koniecznością przetwarzania danych osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu (Załącznik nr 4 do Polityki Ochrony Danych Osobowych)[7].

[dowód: akta kontroli str.: 82-86, 87-108, 109-115, 116-124, 125-133, 325-345, 352-359]

W załączniku nr 3 do informacji przedkontrolnej z dnia 27 marca 2026 r. jako dokument obowiązujący w WIIH wskazywano *Politykę bezpieczeństwa informatycznego* oraz *politykę ochrony danych* wprowadzone zarządzeniem Nr 7/2026 z dnia 10 lutego

[4] Dalej jako: SZBI.
[5] Dalej jako: polityka.
[6] Dalej jako: instrukcja postepowania.
[7] Dalej jako: instrukcja zarządzania systemem informatycznym.

2026 r. W toku kontroli stwierdzono jednak, iż zarządzenie Nr 7/2026 z dnia 10 lutego 2026 r. dotyczy wprowadzenia Polityki Ochrony Danych Osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu (wraz z jej załącznikami tj.: Instrukcją postępowania w przypadku naruszenia ochrony danych osobowych w WIIH oraz Instrukcją zarządzania systemem informatycznym w związku z koniecznością przetwarzania danych osobowych w WIIH), nie zaś wprowadzenia Polityki bezpieczeństwa informatycznego, co potwierdza treść ww. zarządzenia.

Pismem z dnia 22 maja 2026 r. Kontrolowany wyjaśnił, iż: „(…) *polityka bezpieczeństwa informatycznego została opisana w załączniku nr 4 do Polityki Ochrony Danych Osobowych. (...)*''. W toku kontroli stwierdzono, iż w §1 Instrukcji zarządzania systemem informatycznym w związku z koniecznością przetwarzania danych osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu (załącznik nr 4 Polityki Ochrony Danych Osobowych) zawarte zostały uniwersalne rozwiązania dotyczące zarzadzaniem systemem informatycznym (sposób przydziału haseł dla użytkowników i osoby odpowiedzialne za te czynności; sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności; procedury rozpoczynania i kończenia pracy; metodę i częstotliwość tworzenia kopii zapasowych; metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania; sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków; sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych; sposób postępowania w zakresie komunikacji w sieci komputerowej), co należy ocenić pozytywnie.

Z treści ww. aktu jasno wynika, że dotyczy on jednak systemów do przetwarzania danych osobowych (dla przykładu, w § 2 ust. 1 określono, iż nadawanie dostępów dotyczy przyznawania uprawnień do systemu informatycznego służącego do przetwarzania danych osobowych), zatem dotyczy zarządzania systemem informatycznym przeznaczonym do przetwarzania konkretnej grupy informacji.

Mając na uwadze powyższe stwierdzono, iż obowiązujące w jednostce kontrolowanej dokumenty odnoszą się jedynie do bezpieczeństwa danych osobowych, czego skutkiem jest brak uregulowania wielu niezbędnych kwestii zapewniających poufność, dostępność oraz integralność pozostałych kategorii informacji. Pomimo, iż w piśmie z dnia 22 maja 2026 r. Kontrolowany wyjaśnił, iż: *„(...) w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu przetwarza się wyłącznie dane osobowe (...)”* oraz w piśmie z dnia 16 czerwca 2026 r. wyjaśniono, iż: *„(...) wobec systemów, w ramach których realizowane są postępowania kontrolne stosowane są regulacje zawarte w Instrukcji zarządzania systemem informatycznym w związku z koniecznością przetwarzania danych osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu, będącą załącznikiem nr 4 do Polityki Ochrony Danych Osobowych wprowadzonej zarządzeniem Nr 7/2026*”, zauważyć należy, iż jednostka nie dysponuje tylko i wyłącznie danymi osobowymi. Jako pracodawca jest w posiadaniu informacji m.in. o zdrowiu swoich pracowników (np. zwolnienia lekarskie) czy informacji wynikających ze stosunku pracy dot. swoich pracowników (np. dane dot. wynagrodzenia). Ponadto WIIH jako organ administracji publicznej uprawniony jest na podstawie przepisów szczególnych[8] do prowadzenia postępowań kontrolnych m. in. w zakresie działania przedsiębiorców prowadzących działalność gospodarczą w rozumieniu przepisów odrębnych w zakresie produkcji, handlu i usług. Zauważyć należy, iż dane osobowe stanowią bardzo istotny, ale tylko jeden z wielu obszarów informacji, które należy odpowiednio chronić i zabezpieczać. Zauważyć należy, iż pojęcie bezpieczeństwa informacji jest pojęciem szerszym, obejmującym różne kategorie informacji, jak stwierdzono w przypadku kontrolowanej jednostki.

[dowód: akta kontroli str.: 82-86, 87-108, 109-115, 116-124, 125-133, 238-242, 325-345, 352-359]

[8] Art. 3 Ustawy z dnia 15 grudnia 2000 r. o Inspekcji Handlowej (Tekst. jedn. Dz.U. z 2026 r. poz. 656).

W toku kontroli ustalono, iż zgodnie z § 5 Polityki Ochrony Danych Osobowych Administrator Danych Osobowych, realizuje zadania w zakresie bieżącego nadzoru nad systemem informatycznym (pkt 6) oraz zarządza zmianami wpływającymi na prywatność (privacy by desing), a wszystkie nowe procedury w inspektoracie uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) w fazie projektowania czy na początku procedury (pkt 7).

Ponadto zgodnie z § 6 ust. 1 polityki w celu monitorowania przestrzegania zasad bezpieczeństwa, obowiązujących przepisów prawa oraz prowadzenia kontroli przetwarzania danych osobowych, Administrator powołuje IOD. Realizację obowiązku potwierdza przekazana za zgodność z oryginałem kopia pisma z dnia 25 lipca 2025 r., na mocy którego funkcję IOD powierzono Pani Beacie Łyko- Kurowskiej. W myśl § 6 ust. 2 pkt 10 polityki, do zadań IOD należy w szczególności sporządzanie i przedkładanie Administratorowi do dnia 30 września każdego roku, rocznego sprawozdania o stanie ochrony danych w inspektoracie. W piśmie z dnia 22 maja 2026 r. DWIIH wyjaśnił jednak, iż ww. sprawozdanie zostało wprowadzone Zarządzeniem nr 7/2026 Dolnośląskiego Wojewódzkiego Inspektora Inspekcji Handlowej z dnia 10 lutego 2026 r., w związku z powyższym, pierwsze sprawozdanie o których mowa w § 6 ust. 2 pkt 10 ww. dokumentu, zostanie sporządzone do końca września 2026 r.

Powyższe wyjaśnienia uwzględniono w ustaleniach kontroli.

[dowód: akta kontroli str.: 87-108, 238-242, 325-345, 374-376]

W toku kontroli stwierdzono jednak, że żaden z dokumentów nie przewiduje zapisów dot. okresowych przeglądów SZBI, które powinny ustalać zasady i częstotliwość ich przeprowadzania, co jest konieczne do utrzymania odpowiedniego poziomu bezpieczeństwa informacji i wymagane § 19 ust. 1 r.k.r.i. Powyższe ustalenia potwierdził Kontrolowany, w wyjaśnieniach z dnia 16 czerwca 2026 r. informując, iż: *„(...) w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu nie opracowano regulacji dotyczących okresowych przeglądów SZBI.”*

Powyższe wyjaśnienia uwzględniono w ustaleniach kontroli.

[dowód: akta kontroli str.: 82-86, 87-108, 109-115, 116-124, 125-133, 325-345, 352-359, 437-465]

Mając na uwadze, iż dokumentacja musi być sporządzona w sposób precyzyjny, nie pozostawiający wątpliwości co do stosowania zawartych w niej reguł stwierdzono, iż w stosunku do regulacji wprowadzonych zarządzeniem nr 7 dnia 10 lutego 2026 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu (wraz z załącznikami do polityki) nie została sporządzona w sposób precyzyjny. Stosuje się w niej bowiem pojęcia takie jak „administrator danych osobowych (administrator)”, „administrator systemu informatycznego”, „administrator systemu”, „administrator bezpieczeństwa informacji”, „administrator danych” oraz „ administrator sieci”. Zauważyć jednak należy, iż wyjaśnienie definicji użyto jedynie w przypadku określenia „administrator danych osobowych (administrator)” oraz „administrator systemu informatycznego”. Powyższe oznacza, iż w przypadku konieczności zastosowania procedur określonych we wskazanych dokumentach może dojść do braku możliwości ustalenia osoby odpowiedzialnej za podjęcie działania lub podjęcie działania przez osobę nieuprawnioną. Brak sporządzenia ww. regulacji w sposób precyzyjny ocenia się negatywnie.

[dowód: akta kontroli str.: 82-86, 87-108, 109-115, 116-124, 125-133, 325-345, 352-359]

W toku kontroli ustalono, iż zgodnie z § 22 ust. 1 i ust. 2 Instrukcji zarządzania systemem informatycznym użytkownikom pracującym na komputerach zabrania się przekazywania danych osobowych oraz plików wytworzonych wewnątrz systemu

informatycznego inspektoratu do narzędzi sztucznej inteligencji korzystając z darmowych jak i dedykowanych kont firmowych, a jedyną dozwoloną do wykorzystania sztuczną inteligencją jest PLLuM w zakresie zgodnym z poniższymi punktami. W § 22 ust. 3 zawarto natomiast katalog danych, które podlegają szczególnej ochronie przed przekazaniem sztucznej inteligencji. Mając na uwadze obecnie dostępne narzędzia obowiązywanie w WIIH ww. regulacji należy uznać za działania zmierzające do zapewnienia aktualizacji regulacji wewnętrznych w zakresie dot. zmieniającego się otoczenia.

[dowód: akta kontroli str.: 116-124, 352-359]

Wraz z wyjaśnieniami z dnia 22 maja 2026 r. przekazano potwierdzone za zgodność z oryginałem kopie wybranych w ramach kontroli przykładowych oświadczeń o zapoznaniu się z zasadami ochrony danych osobowych w WIIH, składanych przez pracowników WIIH. Stwierdzono, iż oświadczenia były zgodne ze wzorem określonym w załączniku nr 2 do Polityki Ochrony Danych Osobowych.

[dowód: akta kontroli str.: 437-465]

W toku kontroli stwierdzono, iż wszystkie wskazane dokumenty zostały formalnie zatwierdzone przez kierownictwo jednostki.

Mając na uwadze powyższe obszar dotyczący dokumentacji z zakresu systemu bezpieczeństwa informacji oceniono **pozytywnie pomimo stwierdzonych nieprawidłowości.**

2. Analiza zagrożeń związanych z przetwarzaniem informacji.

Regulacja zawarta w przepisie § 19 ust. 2 pkt. 3 r.k.r.i. wskazuje na konieczność przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzone analizy.

W informacji przedkontrolnej z dnia 27 marca 2026 r., w Ankiecie dotyczącej działania systemów teleinformatycznych używanych do realizacji zadań podmiotu, w pkt 2.2. wskazano, iż niniejszy obszar został uregulowany w Polityce Ochrony Danych Osobowych wprowadzonej zarządzeniem Nr 7/2026 z dnia 10 lutego 2026 r. oraz wyjaśniono, iż: „*Ryzyko jest analizowane na bieżąco w trakcie pracy systemu. Monitorowany jest log serwera poczty elektronicznej, programu antywirusowego oraz aktualne informacje w internecie zagrożeniach Podejmowane są kroki w zależności od zagrożenia (blokada adresów IP na firewalu, blokada stron WWW lub blokada wiadomości e-mail lub załączników). Brane są także pod uwagę informacje płynące ze zgłoszeń użytkowników. Brak dokumentacji.*"

Stwierdzono, iż w rozdziale V, VI i VII Polityki Ochrony Danych Osobowych określono zadania i obowiązki: Administratora (Dolnośląski Wojewódzki Inspektor Inspekcji Handlowej), Inspektora Ochrony Danych (IOD) oraz osób upoważnionych do przetwarzania danych osobowych. Zgodnie § 5 ww. dokumentu Administrator Danych Osobowych, realizuje zadania w zakresie ochrony danych osobowych, w tym upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków, a także, m. in.: przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii (pkt 2) oraz przeprowadza oceny skutków dla ochronnych danych, tam gdzie ryzyko naruszenia praw i wolności osób jest wysokie (pkt 3).

Pozytywnie należy ocenić fakt wskazania w Polityce Ochrony Danych Osobowych kto w ramach instytucji jest odpowiedzialny za kwestię przeprowadzania analizy ryzyka dla czynności przetwarzania danych lub ich kategorii, zauważyć jednak należy, iż nie określono procedury analizy ryzyka, co Kontrolowany potwierdził w pkt 4 wyjaśnień z dnia 16 czerwca

2026 r.[9]. Podkreślić należy, że analiza zagrożeń związanych z przetwarzaniem informacji jest istotnym czynnikiem wpływającym na zachowanie bezpieczeństwa informacji. Poprzez szacowanie potencjalnego ryzyka możliwa jest identyfikacja zagrożeń, a także ocena prawdopodobieństwa ich wystąpienia, czy ewentualnych skutków. Forma bieżącej analizy ryzyka bez dokumentowania jej ogranicza możliwości zabezpieczenia jednostki przed utratą integralności, dostępności lub poufności informacji, gdyż dokumentacja z jej przeprowadzenia umożliwia opracowanie kompleksowych regulacji z zakresu SZBI, a także stanowi podstawę do ich aktualizacji w zakresie dot. zmieniającego się otoczenia.

Mając na uwadze powyższe należy wskazać, iż kontrolowana jednostka nie przeprowadzała wymaganej § 19 ust. 2 pkt. 3 r.k.r.i. okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji, tym samym nie identyfikowano w kompleksowy sposób potencjalnych zagrożeń oraz nie ustalono poziomu ryzyka, czy ewentualnych skutków ich wystąpienia. Należy podkreślić, że analiza ryzyka jest istotnym elementem SZBI, umożliwia wskazanie zagrożeń związanych z przetwarzaniem informacji, a także ustalenie prawdopodobieństwa ich wystąpienia, czy stopnia akceptacji ryzyka.

[dowód: akta kontroli str.: 53-81, 87-108, 325-345, 437-465]

Mając na uwadze powyższe obszar dotyczący analizy zagrożeń związanych z przetwarzaniem informacji oceniono **negatywnie.**

3. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji.

Zgodnie z § 19 ust. 2 pkt 13 r.k.r.i., kierownictwo podmiotu powinno zapewnić warunki umożliwiające realizację oraz egzekwowanie bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

W toku kontroli stwierdzono, iż nie sporządzono dokumentacji dot. zgłaszania incydentów naruszenia bezpieczeństwa wszystkich kategorii informacji. Kwestie dot. zgłaszania incydentów naruszenia ochrony danych osobowych uregulowano jednak w przyjętej Zarządzeniem Nr 7/2026 z dnia 10 lutego 2026 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w WIIH we Wrocławiu *Instrukcji Postępowania w Przypadku Naruszenia Ochrony Danych Osobowych w WIIH We Wrocławiu* (zał. nr 3 do Polityki Ochrony Danych Osobowych).

[dowód: akta kontroli str.: 109-115]

W instrukcji zdefiniowano, czym jest naruszenie bezpieczeństwa informacji[10], osoby zobowiązane do jej przestrzegania, tj.: Administrator, wszyscy Pracownicy Administratora oraz osoby współpracujące z Administratorem na podstawie innego stosunku prawnego (§ 1 ust. 3 instrukcji). W wypadku podejrzenia naruszenia ochrony danych osobowych lub stwierdzenia naruszenia ochrony danych osobowych każdy ma obowiązek niezwłocznego powiadomienia Administratora lub IOD (§ 1 ust. 4 instrukcji). W treści ww. instrukcji określono również przypadki naruszenia ochrony danych, które każdy obowiązany jest zgłosić. Ponadto ww. dokument określa działania, jakie obowiązany jest podjąć Administrator oraz IOD. Zauważyć jednak należy, iż o ile w instrukcji postępowania w przypadku naruszenia ochrony danych osobowych określono jakie kroki mają zostać podjęte przez Administratora lub IOD po powiadomieniu o podejrzeniu naruszenia lub o naruszeniu ochrony danych osobowych, nie określono jednak w jaki sposób takie powiadomienie miałoby nastąpić.

[9] BA.1611.1.2026.GK.

[10] § 2 ust. 1 instrukcji postępowania.

Nie określono procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji przez osoby zgłaszające, tj. nie określono w jaki sposób ma być dokonywane zgłoszenie (osobiście, za pośrednictwem e-mail czy telefonicznie itp.).

[dowód: akta kontroli str.: 109-115]

Ponadto, w wyniku kontroli stwierdzono, iż w WIIH został opracowany Rejestr incydentów cyberbezpieczeństwa (przekazany wraz z dokumentacją SZBI w dniu 13 kwietnia 2026 r.). W treści ww. rejestru wskazywano datę zgłoszenia, zadanie publiczne, którego dotyczy zgłoszenie, opis zdarzenia, kategorię incydentu, podjęte działania zapobiegawcze oraz podjęte działania naprawcze. Nie wskazano jednak daty kiedy miały miejsce incydenty, kto dokonał ich zgłoszenia oraz kto podjął działania. Brak powyższych informacji nie dokumentuje w sposób wyczerpujący przebiegu zdarzenia, jakim jest wystąpienie incydentu oraz nie obrazuje w pełni kwestii dot. podjętych działań. W toku kontroli stwierdzono również, iż w żadnym z obowiązujących w WIIH dokumencie z zakresu SZBI nie uregulowano kwestii samego Rejestru incydentów, co potwierdzają wyjaśnienia Kontrolowanego przedstawione w piśmie z dnia 16 czerwca 2026 r., cyt.: *„w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu nie uregulowano w formie dokumentu pojęcia ani kategorii incydentu”*. W ww. piśmie wyjaśniono również, że: *w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu nie odnotowano dotychczas żadnego incydentu; odpowiedzialność za prowadzenie tego typu rejestru spoczywa na Administratorze, który powierzył to zadanie do wykonania IOD. Ponieważ nie miało dotychczas miejsce żadne zdarzenie, które można zakwalifikować jako incydent taki rejestr nie został jeszcze opracowany.”*

Powyższych wyjaśnień nie uwzględniono. W dniu 13 kwietnia 2026 r. Kontrolowany przekazał w ramach kontroli Rejestr incydentów cyberbezpieczeństwa, w którym odnotowywano incydenty z lat 2016-2026 dot. połączenia z podsieci adresu IP do serwera oraz prób odgadnięcia hasła do poczty elektronicznej. Powyższe oznacza, iż taki rejestr był prowadzony, a kwestie dotyczące jego prowadzenia oraz treści nie zostały uregulowane. Fakt bieżącego dokonywania zgłoszeń i prowadzenia rejestru incydentów potwierdza również treść pkt 2.3. dot. procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji ankiety[11], z uwagi na to, że Kontrolowany wskazał, iż: „*Podejrzane sytuacje są na bieżąco zgłaszane do przełożonych oraz informatyków skutkując szybką reakcją. Monitorowane są zgłoszenia o zagrożeniach co pozwala z góry powiadomić i uczulić użytkowników na nowe zagrożenia oraz podjąć działania prewencyjne”*, co oceniono pozytywnie.

[dowód: akta kontroli str.: 125-133, 437-465]

Zgodnie z § 3 ust. 2 i ust. 5 Instrukcji Postępowania w Przypadku Naruszenia Ochrony Danych Osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu, IOD dokumentuje zdarzenie oraz niezwłocznie przygotowuje raport naruszenia ochrony danych osobowych, który stanowi podstawę dokumentacji naruszeń ochrony danych osobowych prowadzonej przez Administratora. Powyższy zapis nakłada na upoważnione do tego osoby obowiązek dokumentacyjny w toku zgłaszania incydentów, co należy ocenić pozytywnie. Niemniej jednak w piśmie z dnia 22 maja 2026 r. wyjaśniono, iż: „*W Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu nie zdiagnozowano dotychczas incydentów w zakresie naruszenia ochrony danych osobowych, a w konsekwencji żaden raport w tej sprawie nie został jeszcze sporządzony.*”. Powyższe wyjaśnienia uwzględniono w ustaleniach kontroli.

[dowód: akta kontroli str.: 109-115, 238-242]

[11] Ankieta dotycząca działania systemów teleinformatycznych używanych do realizacji zadań podmiotu, przekazana w ramach informacji przedkontrolnej z dnia 27 marca 2026 r.

Mając na uwadze powyższe, obszar dotyczący procedur zgłaszania incydentów naruszenia bezpieczeństwa informacji należy ocenić **pozytywnie pomimo stwierdzonych nieprawidłowości.**

4. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Mając na uwadze § 19 ust. 2 pkt 14 r.k.r.i. podmiot realizujący zadania publiczne zobowiązany jest do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Audyt jest jednym z istotnych elementów wpływających na utrzymanie oraz doskonalenie całego SZBI. Pozwala na wskazanie mocnych i słabych stron przyjętych rozwiązań, a następnie ich analizę i podjęcie odpowiednich działań korygujących. Brak audytów uniemożliwia optymalne szacowanie istniejących ryzyk, jak również wyeliminowanie potencjalnych słabości, dlatego też tak ważne jest jego uregulowanie w dokumentach z zakresu bezpieczeństwa informacji. Ponadto, audyt stanowi kluczowe narzędzie, które pozwala na regularny przegląd SZBI. Niezapewnienie przeprowadzania audytów wewnętrznych jest sprzeczne z § 19 ust. 1 r.k.r.i., który zobowiązuje podmiot realizujący zadania publiczne do monitorowania oraz przeglądania i doskonalenia SZBI. Aktualizacja regulacji wewnętrznych opiera się w znaczącym stopniu na przeprowadzanych audytach oraz realizacji zaleceń poaudytowych, a ich brak może skutkować pominięciem istotnych czynników wymagających zmiany.

W piśmie z dnia 16 czerwca 2026 r. Kontrolowany wskazał, iż: „(…) *w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu nie uregulowano w formie dokumentu kwestii audytów wewnętrznych z zakresu Bezpieczeństwa Informacji*". Tym samym pismem wyjaśniono jednocześnie, że: „*(...) w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu nie posiadamy dokumentacji audytów wewnętrznych w zakresie Bezpieczeństwa Informacji (BI). Przegląd BI w Delegaturach jest wykonywany co najmniej raz na pół roku podczas wizyt w delegaturach przy okazji prowadzonych planowanych prac. We Wrocławiu przegląd BI jest wykonywany przy każdej zmianie uprawnień użytkowników oraz podczas wizyt w poszczególnych wydziałach, minimum raz w roku*".

Powyższe wyjaśnienia uwzględniono w ustaleniach kontroli. Zauważyć jednak należy, iż brak regulacji dotyczącej kwestii audytu wewnętrznego w zakresie BI należy uznać za niezgodny z § 19 ust. 2 pkt 14 r.k.r.i.

[dowód: akta kontroli str.: 437-465]

Podsumowując, powyższy obszar dotyczący audytu wewnętrznego z zakresu bezpieczeństwa informacji oceniono **negatywnie.**

5. Zarządzanie uprawnieniami do pracy w systemach informatycznych.

Istotnym elementem bezpieczeństwa informacji jest zarządzanie uprawnieniami. Proces ten ma zapewnić, że osoby zaangażowane w przetwarzanie informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych zadań oraz obowiązków, a w przypadku zmiany lub nierealizowania zadań następuje również zmiana lub cofnięcie tych uprawnień. W toku kontroli sprawdzono, czy osoby zaangażowane w proces przetwarzania informacji w WIIH posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, zgodnie z § 19 ust. 2 pkt 4 r.k.r.i.

Zagadnienia dotyczące zarządzania uprawnieniami w systemach informatycznych zostały określone w Polityce Ochrony Danych Osobowych oraz Instrukcji zarządzania systemem informatycznym w związku z koniecznością przetwarzania danych osobowych

w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu, stanowiącym załącznik nr 4 do ww. Polityki.

W myśl § 7 ust. 1 Polityki, do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora lub podmiot przetwarzający, które zostały zapoznane z przepisami o ochronie danych osobowych i złożyły stosowne oświadczenie dotyczącej właściwej realizacji przepisów RODO.

Zgodnie z § 2 ust. 1 ww. Instrukcji dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba zarejestrowana w tym systemie przez Administratora Systemu (dalej: ASI) na wniosek pracownika odpowiedzialnego za sprawy kadrowe, natomiast w myśl § 5 ust. 1 ww. Instrukcji wyrejestrowania użytkownika z systemu informatycznego dokonuje ASI na wniosek pracownika odpowiedzialnego za sprawy kadrowe.

[dowód: akta kontroli str. 87-108, 116-124, 325-345, 352-359]

W toku kontroli, celem ustalenia kwestii związanych z nadawaniem uprawnień w systemach, dokonano sprawdzenia trzech pracowników zatrudnionych w WIIH: ASI, Pani E.R. i Pani M.W., a także dwóch byłych pracowników WIIH: Pani B.S. oraz Pana J.P.[12].

Poprzez konsolę Active Directory dokonano weryfikacji statusu byłych pracowników WIIH, w wyniku której ustalono, iż konta Pani B.S. oraz Pana J.P. zostały usunięte - nie było możliwym znalezienie ich kont, mimo, iż osoby te widnieją w wykazie byłych pracowników (pozycja 15 i 29). Konta wskazanych osób nie widnieją również w systemie EZD RP. W odniesieniu do systemu Vulcan Pani B.S. widnieje w systemie jako nieaktywne, Panu J.P. nie utworzono konta w systemie Vulcan. W systemie Zabbix konta posiadają tylko informatycy.

W odniesieniu do obecnie zatrudnionych pracowników WIIH dokonano sprawdzenia kont lokalnych i ich uprawnień na stacjach roboczych. Z uwagi na zajmowane stanowisko, ASI posiadał uprawnienia administratora stacji roboczej, natomiast Pani E.R. oraz Pani M.W. posiadała uprawnienia użytkownika stacji lokalnej, co należy ocenić pozytywnie. W toku czynności kontrolnych dokonano również sprawdzenia uprawnień w systemie EZD oraz Vulcan, na podstawie którego ustalono, iż ASI posiada dwa konta w ww. systemach – użytkownika oraz administratora, natomiast Pani E.R. oraz Pani M.W. posiadają tylko po jednym koncie z podstawowymi uprawnieniami użytkownika.

[dowód: akta kontroli str.: 139-187, 188-201]

Mając na uwadze powyższe ustalenia obszar zarządzania uprawnieniami do pracy w systemach teleinformatycznych oceniono **pozytywnie.**

6. Praca na odległość i mobilne przetwarzanie danych.

Kontrola wykazała, iż w jednostce kontrolowanej ustanowiono Regulamin Pracy Zdalnej Wojewódzkiego Inspektoratu Inspekcji Handlowej we Wrocławiu, stanowiący załącznik nr 6 do Regulaminu Pracy Wojewódzkiego Inspektoratu Inspekcji Handlowej we Wrocławiu, a także Informację o zasadach bhp przy pracy zdalnej oraz Procedurę ochrony danych osobowych w pracy zdalnej, stanowiące odpowiednio załącznik nr 7 i 8 do ww. regulaminu pracy zdalnej. Regulacje te określają podstawowe zasady zapewniające bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, zgodnie z § 19 ust. 2 pkt 8 r.k.r.i.

[12] Pełne personalia pracowników w aktach kontroli.

W toku czynności kontrolnych ASI wyjaśnił, iż przy przetwarzaniu danych na odległość na laptopach zainstalowany jest open VPN który pozwala łączyć się z serwerami WIIH. Ponadto, w Active Directory utworzone są grupy pracowników, które mogą się łączyć zdalnie z serwerami DUW. Wskazano też określone dni i godziny (od poniedziałku do piątku, w godzinach 6:45 do 17:00), w których mogą pracować zdalnie. Poza tymi godzinami dostęp do komputerów jest niemożliwy (automatyczne wyłączenie urządzenia) – zarządzane przez ASI za pośrednictwem Active Directory. Ponadto, istnieje osobny VPN w przypadkach nagłych, do którego dostęp mają tylko informatycy WIIH – rozwiązanie to jest stosowane w przypadku wystąpienia sytuacji nagłych. Służbowy sprzęt, dyski i nośniki danych są szyfrowane. Ustalono również, iż WIIH nie posiada ustanowionych blokad dla urządzeń nienależących do WIIH. Ponadto, ASI zarządza globalnie zabezpieczeniami antywirusowymi i zaporą wszystkich użytkowników w WIIH oraz otrzymuje monity dot. ewentualnych naruszeń.

[dowód: akta kontroli str. 139-187, 243-275, 292-321]

Wskazane powyżej regulacje oraz działania faktyczne należy uznać za wystarczające, a powyższe zagadnienie ocenia się **pozytywnie.**

7. Zabezpieczenia techniczno - organizacyjne dostępu do informacji.

Zgodnie z § 19 ust. 2 pkt 7 r.k.r.i. zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez monitorowanie dostępu do informacji, poprzez czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji oraz poprzez zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

W wyniku kontroli ustalono, iż kwestie zabezpieczeń techniczno – organizacyjnych dostępu do informacji uregulowano w:

- Polityce ochrony danych wprowadzonej zarządzeniem Nr 7/2026 z dnia 10 lutego 2026 r.;
- Instrukcji zarządzania systemem informatycznym w związku z koniecznością przetwarzania danych osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu (załącznik nr 4 do polityki);
- Regulaminie pracy Wojewódzkiego Inspektoratu Inspekcji Handlowej we Wrocławiu wprowadzonym Zarządzeniem Nr 24 z dnia 17 czerwca 2025 r. w sprawie wprowadzenia regulaminu pracy Wojewódzkiego Inspektoratu Inspekcji Handlowej we Wrocławiu;

Analiza treści ww. dokumentów wykazała co następuje:

- <u>W zakresie działań związanych z monitorowaniem dostępu do informacji oraz w zakresie czynności mających na celu wykrycie nieautoryzowanych działań związanych z przetwarzaniem informacji:</u>

W wyjaśnieniach z dnia 22 maja 2026 r. wskazano, iż: „*Monitorowanie dostępu odbywa się za pośrednictwem upoważnień do przetwarzania danych osobowych, które są nadawane pracownikom zgodnie z procedurą opisaną w § 7 Polityki Ochrony Danych Osobowych; Rejestr osób upoważnionych do przetwarzania danych osobowych jest prowadzony w formie elektronicznej w systemie EZD. Od strony informatycznej monitorowanie dostępu do informacji odbywa się poprzez zapisywanie w logach serwerów np. plikowych oraz pocztowych dostępu oraz wykonanych operacji na informacjach zawartych na serwerach”.*

Zgodnie z treścią ww. przepisu, upoważnienia wydawane są przez Administratora (Dolnośląskiego Wojewódzkiego Inspektora Inspekcji Handlowej) na wniosek kierującego komórką organizacyjną, w której osoba upoważniona ma zostać zatrudniona na podstawie umowy o pracę lub z którą ma współpracować na innej podstawie. Inspektor Ochrony Danych przyjmuje od osoby, która ma zostać zatrudniona w inspektoracie oświadczenie o zapoznaniu z zasadami ochrony danych osobowych, a następnie przygotowuje upoważnienie. Zgodnie z treścią § 7 ust. 4 pkt 3 Polityki upoważnienia udzielane przez Administratora podlegają zewidencjowaniu w rejestrze upoważnień prowadzonym przez IOD.

Wraz z wyjaśnieniami z dnia 16 czerwca 2026 r. przekazano kopię rejestru upoważnień nadawanych w kontrolowanej jednostce. W toku kontroli stwierdzono, iż zbadane w ramach próby kontroli upoważnienia sporządzone zostały na wzorze określonym w załączniku nr 1 do Polityki Ochrony Danych Osobowych. Ponadto ustalono, iż wpisy w rejestrze wprowadzane były przez osobę wyznaczoną do pełnienia funkcji IOD, co jest zgodne z obowiązującymi regulacjami wewnętrznymi. Stwierdzono jednak, iż 1 z 5 badanych upoważnień (upoważnienie Pani M.W.) nie zostało uwzględnione (zarówno jako przyznane upoważnienie jak i upoważnienie, które wygasło) w prowadzonym rejestrze upoważnień, choć, jak wskazano w załączniku nr 4 do informacji przedkontrolnej z dnia 23 marca 2026 r, pracownik, któremu nadano upoważnienie nadal jest zatrudniony w WIIH i ma dostęp do systemów takich jak EZD RP, Vulcan, Kerio Connect. Ponadto w przypadku innego upoważnienia (Pana K. Ż.) w rejestrze jako datę wydania upoważnienia wskazano dzień 29.10.2025 r., choć data widniejąca na upoważnieniu to 30.10.2025 r. Stwierdzono również, iż mimo że w rejestrze zamieszczono rubrykę o nazwie „nazwa zbioru", to nie została ona uzupełniona w przypadku żadnego z upoważnień. Powyższe oznacza, iż rejestr upoważnień prowadzonym przez IOD prowadzony jest w sposób nierzetelny, co należy ocenić negatywnie.

[dowód: akta kontroli str.: 53-81, 87-108, 116-124, 238-242, 243-275, 325-345, 352-359, 437-465]

W § 4 ust. 2 pkt 2 Regulaminu Pracy Zdalnej Wojewódzkiego Inspektoratu Inspekcji Handlowej we Wrocławiu, stanowiącego załącznik nr 6 do Regulaminu pracy Wojewódzkiego Inspektoratu Inspekcji Handlowej we Wrocławiu, pracownik wykonujący pracę zdalną jest zobowiązany potwierdzać rozpoczęcie pracy zdalnej w danym dniu poprzez wysłanie wiadomości e-mail, ze wskazaniem godziny rozpoczęcia pracy do bezpośredniego przełożonego oraz do wiadomości pracownika odpowiedzialnego za sprawy kadrowe i w taki sam sposób informować o zakończeniu pracy zdalnej.

Ponadto zgodnie z wyjaśnieniami udzielonymi przez Pana M. T. podczas oględzin w dniu 22 kwietnia 2026 r. przy przetwarzaniu danych na odległość (np. praca zdalna) – na laptopach zainstalowany jest open VPN, który pozwala łączyć się z serwerami WIIH. Ponadto, w AD utworzone są grupy pracowników, które mogą się łączyć zdalnie z serwerami WIIH. Określono też dni i godziny (od poniedziałku do piątku, w godzinach 6:45 do 17:00), w których mogą pracować zdalnie. Poza tymi godzinami dostęp do komputerów jest niemożliwy (automatyczne wyłączenie urządzenia) – zarządzane przez AD. Ponadto wyjaśniono, iż istnieje osobny VPN w przypadkach nagłych, do którego dostęp mają tylko informatycy. Powyższe wyjaśnienia uwzględniono.

Zgodnie z § 10 ust. 1 Polityki Ochrony Danych Osobowych w inspektoracie prowadzi się wspólny Rejestr Czynności Przetwarzania i wspólny Rejestr Kategorii Czynności Przetwarzania dla wszystkich jednostek organizacyjnych. Rejestry stanowią formę dokumentowania czynności przetwarzania danych i umożliwiają realizację zasady rozliczalności. Wraz z pismem z dnia 22 maja 2026 r. przekazano rejestr czynności przetwarzania, w którym wskazane zostały m. in.: nazwa czynności przetwarzania, cel przetwarzania, kategorie osób, kategorie danych, źródło danych, podstawa prawna, planowany termin usunięcia kategorii danych, nazwa współadministratora, nazwa podmiotu

przetwarzającego, kategorie odbiorców (innych niż podmiot przetwarzający), nazwa systemu przetwarzania lub oprogramowania, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Wyżej wymienionym pismem wyjaśniono jednocześnie, iż: „(…) rejestr kategorii czynności przetwarzania nie został uzupełniony".

Mając na uwadze powyższe działania związane z monitorowaniem dostępu do informacji oraz czynności mające na celu wykrycie nieautoryzowanych działań związanych z przetwarzaniem informacji oceniono pozytywnie.

[dowód: akta kontroli str.: 87-108, 139-187, 238-242, 292-321, 325-345]

- W zakresie działań związanych z monitorowaniem ruchu osobowego w kontrolowanym podmiocie:

Kontrola wykazała, że wejście do budynku WIIH we Wrocławiu jest zabezpieczone poprzez elektrozamek (domofon) oraz alarm. Osoby chcące wejść do budynku muszą poprzez domofon połączyć się z sekretariatem w celu otworzenia drzwi.

W piśmie z dnia 22 maja 2026 r. wyjaśniono, iż: „ *W WIIH we Wrocławiu realizowane są działania mające na celu wykrywanie oraz ograniczanie ryzyka nieautoryzowanego dostępu do informacji i pomieszczeń, w których informacje są przetwarzane. Nie jest prowadzony formalny rejestr wejść i wyjść. Dostęp do pomieszczeń zabezpieczony jest jednak poprzez system domofonowy. Osoby zewnętrzne wpuszczane są do siedziby po wcześniejszym kontakcie z sekretariatem oraz weryfikacji celu wizyty. Po wejściu do siedziby osoby zewnętrzne poruszają się po obiekcie wyłącznie w obecności lub pod nadzorem powiadomionego pracownika. Dodatkowo dostęp do informacji oraz systemów informatycznych posiadają wyłącznie osoby upoważnione, zgodnie z zakresem wykonywanych obowiązków. Stosowane są indywidualne konta użytkowników oraz mechanizmy uwierzytelniania dostępu do systemów".*

Powyższe wyjaśnienia uwzględniono. Należy jednak zauważyć, iż brak formalnego rejestru wejść i wyjść nie zapewnia zgodności działań z atrybutem rozliczalności, wynikającym z § 19 ust. 1 r.k.r.i.. Mając jednak na uwadze podejmowane działania związane z monitorowaniem ruchu osobowego, działania te oceniono pozytywnie pomimo stwierdzonych nieprawidłowości.

[dowód: akta kontroli str.: 238-242]

- W zakresie działań związanych z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji WIIH.

W § 4 Instrukcji zarządzania systemem informatycznym określono zasady tworzenia haseł do systemu informatycznego służącego do przetwarzania danych osobowych. Zgodnie z treścią ww. przepisu hasło powinno składać się z co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne (ust. 1). Hasło nie może być identyczne z identyfikatorem użytkownika (ust. 2). Ponadto zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom. Dotyczy to także identyfikatorów i haseł użytkownika do innych systemów informatycznych używanych przy wykonywaniu czynności służbowych (ust. 3), a identyfikator i hasło jest używane do zabezpieczenia dostępu do komputera, poczty elektronicznej, komunikatora czasu rzeczywistego oraz dostępu zdalnego (ust. 4).

W piśmie z dnia 22 maja 2026 r. wyjaśniono również, iż: „ *W celu uzyskania dostępu do sieci wewnętrznej należy zalogować się na komputerze służbowym z użyciem loginu i hasła, które jest przydzielane na wniosek pracownika odpowiedzialnego za sprawy kadrowe zgodnie*

z § 2. 1. instrukcji zarządzania systemem informatycznym. Odebranie uprawnień, czyli wyrejestrowanie użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek pracownika odpowiedzialnego za sprawy kadrowe zgodnie z § 5. 1. instrukcji zarządzania systemem informatycznym. Wyrejestrowanie użytkownika z systemu informatycznego może mieć charakter czasowy lub trwały w zależności od przyczyny uzasadniającej blokadę. Konta tworzone dla użytkowników systemu nie mają uprawnień do zmiany ustawień systemowych ani do instalowania oprogramowania. W zależności od przynależności do grupy zabezpieczeń użytkownik ma ograniczony dostęp do informacji zgromadzonych na serwerach urzędu. By chronić dane zgromadzone na dyskach twardych komputerów użytkowników są one zaszyfrowane z użyciem wbudowanego w system operacyjny mechanizmu Bitlocker". Powyższe wyjaśnienia uwzględniono.

Działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji oceniono pozytywnie.

[dowód: akta kontroli str.: 116-124, 238-242, 352-359]

- W zakresie fizycznej ochrony informacji, uniemożliwiającej nieuprawnionemu ich ujawnienia, modyfikacji, usunięcia lub zniszczenia:

W toku kontroli ustalono, iż budynek znajdujący się przy ul. Ofiar Oświęcimskich 15a, we Wrocławiu, w której znajduje się siedziba WIIH we Wrocławiu przekazany został na mocy decyzji nr 24/2000 z 10 kwietnia 2000 r. w trwały zarząd WIIH.

Ustalono również, iż od 1 stycznia 2011 r. siedziba WIIH we Wrocławiu podlega ochronie firmy SOLID GROUP Sp. z o.o. Sp. k., która świadczy usługę monitorowania sygnałów lokalnego systemu alarmowego oraz podejmowania interwencji. W piśmie z dnia 22 maja 2026 r. wyjaśniono, iż: *„(...) w budynku zamontowano system kamer. Materiał wideo z kamer jest zapisywany na rejestratorze znajdującym się w serwerowni i jest przechowywany przez 30 dni. Po tym czasie najstarsze nagrania zostają nadpisane*.". Ponadto tym samym pismem wyjaśniono, iż: „ *Informacje przetwarzane w WIIH we Wrocławiu są zabezpieczone w sposób ograniczający możliwość ich nieuprawnionego ujawnienia, modyfikacji, usunięcia lub zniszczenia. Pomieszczenia biurowe po zakończeniu pracy są zamykane przez pracowników firmy sprzątającej. Klucze pozostawiane są w zamkach drzwi zgodnie z przyjętą procedurą wewnętrzną. Po zakończeniu prac porządkowych pracownicy firmy sprzątającej uruchamiają system alarmowy w budynku, co uniemożliwia dostęp osobom trzecim poza godzinami pracy. Dodatkowo w organizacji obowiązuje zasada „czystego biurka", zgodnie z którą pracownicy są zobowiązani do zabezpieczania i usuwania dokumentów oraz nośników informacji z biurek po zakończeniu pracy, tak aby nie były one dostępne dla osób nieuprawnionych.*'' W piśmie z dnia 16 czerwca 2026 r. poinformowano jednak, że: „(…) *w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu nie opracowano pisemnej procedury wewnętrznej, regulującej kwestie kluczy do pomieszczeń oraz uruchamiania alarmu po zakończeniu prac porządkowych przez pracowników firmy sprzątającej; (...) Wojewódzki Inspektorat Inspekcji Handlowej we Wrocławiu potwierdza, że kod do alarmu, który posiadają pracownicy firmy sprzątającej jest odrębnym kodem niż ten, który stosowany jest wobec alarmu do pomieszczenia serwerowni;(...).* Ponadto poinformowano, iż: *(...)Wojewódzki Inspektorat Inspekcji Handlowej we Wrocławiu informuje, ze prowadzi wykaz osób posiadających kody do alarmu".*

Mając na uwadze powyższe wyjaśnienia z dnia 22 maja 2026 r. uwzględniono jedynie w części. Pozytywnie należy ocenić fakt, iż po wykonanej usłudze sprzątania uruchamiany jest system alarmowy w budynku, co uniemożliwia dostęp osobom trzecim poza godzinami pracy, oraz fakt, iż kod ten jest odrębnym kodem niż ten, który zabezpiecza pomieszczenie serwerowni Pozytywnie należy ocenić również fakt, iż prowadzony jest wykaz osób

posiadających kody do alarmu oraz to, że obowiązuje zasada zasadę „czystego biurka”[13], zgodnie z którą pracownicy są zobowiązani do zabezpieczania i usuwania dokumentów oraz nośników informacji z biurek po zakończeniu pracy, tak aby nie były one dostępne dla osób nieuprawnionych. Negatywnie należy jednak ocenić brak regulacji dot. zamykania pomieszczeń, w których przetwarzane są informacje, jak i uruchamiania alarmu po zakończeniu prac porządkowych przez pracowników firmy sprzątającej.

[dowód: akta kontroli str.: 238-242, 365-366, 367-369]

W toku kontroli stwierdzono również, iż zapewniono fizyczną ochronę informacji, uniemożliwiającą ich nieuprawnione ujawnienie, modyfikację, usunięcie lub zniszczenie poprzez zawarcie w umowie z wykonawcą usług sprzątających zapisów[14] dotyczących:

- zakazu wpuszczania na teren biura osób trzecich bez uprzedniej, pisemnej zgody DWIH;
- zobowiązania do zachowania jako poufnych wszelkich informacji – bez względu na ich nośniki jakie od siebie uzyskają;
- zachowanie w tajemnicy wszystkich informacji i danych, które mogą zostać uzyskane w trakcie świadczenia usług, a które mogą mieć wpływ na stan bezpieczeństwa ludzi i mienia, a także na działalność prowadzoną przez WIIH, zarówno w czasie trwania umowy, jak i po jej rozwiązaniu.

Powyższe czynności oceniono pozytywnie.

[dowód: akta kontroli str.: 437-465]

W toku kontroli stwierdzono również, iż w § 12 ust. 6 polityki zobowiązano pracowników w szczególności do: pozostawiania na biurkach jedynie dokumentów i nośników niezbędnych do bieżącego wykonywania obowiązków służbowych; zabezpieczenia dokumentów zawierających dane osobowe (w szczególności po zakończonym dniu pracy lub dłuższej nieobecności przy stanowisku pracy) w zamykanych szafach, szufladach czy innych schowkach; niepozostawiania nośników danych, w szczególności pendrivów, płyt CD, DVD, dysków zewnętrznych i innych urządzeń służbowych w miejscach ogólnodostępnych i widocznych dla osób trzecich; zamykania ekranu komputera (blokady) przy każdorazowym odejściu od stanowiska pracy; ochrony haseł i dostępów do urządzeń służbowych.

Ponadto w § 19 ust. 1 instrukcji zarządzania systemem informatycznym uregulowano kwestie przechowywania nośników informatycznych oraz kwestie faktycznego ustawienia oraz blokady monitorów stanowiskowych w taki sposób, aby uniemożliwić tym osobom wgląd w dane. Treścią § 20 instrukcji zarządzania systemem informatycznym obowiązano osoby użytkujące przenośny komputer, służący do przetwarzania danych osobowych do zachowania szczególnej ostrożności podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej. Wskazano również, iż wszelkie nośniki danych podłączane do komputera muszą być zaszyfrowane i zabezpieczone hasłem w celu uniemożliwienia dostępu do danych osobom nieuprawnionym. W § 21 uregulowano również kwestię obowiązków użytkowników sporządzających wydruki, które zawierają dane osobowe do zachowania szczególnej ostrożności przy korzystaniu z nich, oraz zabezpieczeniu ich przed dostępem osób nieposiadających imiennego upoważnienia oraz nieuprawnionych do wglądu na podstawie indywidualnego zakresu czynności. Uregulowano również kwestie niszczenia takich wydruków, tj. w stopniu uniemożliwiającym ich odczytanie.

[dowód: akta kontroli str.: 87-108, 116-124, 325-345, 352-359]

[13] Zgodnie z § 12 ust. 5 polityki Środki bezpieczeństwa fizycznego obejmują zobowiązanie Pracowników do stosowania tzw. polityki czystego biurka i czystego ekranu. Ponadto zgodnie z § 12 ust. 6 polityki

[14] § 6 pkt. 3, pkt 5 oraz pkt 6 umowy nr 12/BA/2025 z firmą sprzątającą.

W toku kontroli oględzinom poddano również pomieszczenia serwerowni znajdującej się w budynku WIIH we Wrocławiu przy ul. Ofiar Oświęcimskich 15a, 50-069 Wrocław. W ich wyniku stwierdzono, co następuje:

- Serwerownia znajduje się na 2 piętrze budynku, jest pomieszczeniem odrębnym, zamykanym na klucz tradycyjny, który znajduje się w pomieszczeniu informatyków oraz dysponuje nim Pan M.T. W toku oględzin wyjaśniono, iż w razie nieobecności klucz przekazywany jest zastępcy. Ponadto wskazano, iż klucz zapasowy jest w posiadaniu Kierownika jednostki kontrolowanej.
- Wejście do serwerowni zabezpieczone zostało alarmem, a w celu dostania się do jej wnętrza konieczne jest jego rozbrojenie.
- Konsola alarmu znajduje się na parterze budynku na korytarzu,
- Kod do alarmu posiadają informatycy WIIH (Pan M.T. oraz Pan K.S.) oraz dodatkowo kod w wersji wydrukowanej umieszczono w sejfie, do którego dostęp posiada Kierownik jednostki kontrolowanej.
- W toku oględzin stwierdzono, iż konsola alarmu nie jest widoczna z zewnątrz (wejście do budynku) oraz nie znajduje się w świetle kamer.
- Dla serwerowni nie prowadzi się rejestru wejść i wyjść. Nie stworzono również rejestru pobierania klucza do serwerowni.
- W przypadku kodu do alarmu system odnotowuje datę i godzinę wpisania kodu, niemniej jednak nie ma możliwości sprawdzenia kto wpisał kod do alarmu.
- Serwerownia zabezpieczona została poprzez:
  - czujkę ruchu,
  - czujkę dymu,
  - kamerę wewnątrz serwerowni, zapewniającą bieżący monitoring, zapewniającą bieżący monitoring serwerowni w razie wykrycia ruchu albo hałasu,
  - klimatyzator ustawiony na 17 stopni, bez możliwości zdalnego ustawienia temperatury,
  - UPS podłączone serwerów głównych i zapasowych, a także do urządzeń sieciowych typu switch i router,
  - bieżące monitorowanie serwerów przez Zabbix w zakresie temperatury urządzenia,
  - dwie gaśnice CO_2 do urządzeń elektronicznych znajdujące się w serwerowni,
- Przed pomieszczeniem serwerowni, na korytarzu, znajduje się skrzynka z bezpiecznikami zarządzającymi m. in. klimatyzacją serwerowni. W trakcie prowadzonych oględzin skrzynka nie była zabezpieczona przed dostępem osób trzecich.
- Ściany pomieszczenia serwerowni zrobione są w cienkiego materiału, który nie daje gwarancji zatrzymania próby dostania przy użyciu siły,
- Brak czujnika wilgoci,
- Brak czujnika wilgotności i temperatury pomieszczenia,
- Brak czujnika zalania pomieszczenia,
- Serwerownia wyposażona została w:
  - 4 serwery : 2 główne i 2 zapasowe (jeden serwer do maszyn wirtualnych i jeden do plików, a także po jednym serwerze zapasowym dla każdego),
  - 2 UPSy podtrzymujące serwery WIIH, 1 UPS podtrzymujący switche oraz anteny do bezprzewodowej telefonii VOIP oraz 1 UPS do podtrzymywania urządzenia brzegowego firewall. Piąty UPS podtrzymuje napięcie w urządzeniu przechowującym kopie zapasowe danych,
  - 2 skrzynie ze switchami sieciowymi,

  - 3 szafy, w których przechowywane nośniki instalacyjne systemów wraz z licencjami będącymi w posiadaniu WIIH,
  - 2 gaśnice ręczne CO_2,
- Serwerownia posiada zasilanie awaryjnie z UPS-a znajdującego się w pomieszczaniu serwerowni. Nie ma UPS-ów podtrzymujących serwery jednostki w innych pomieszczeniach (w sekretariacie WIIH znajduje się UPS podtrzymujący napięcie w systemie centrali telefonicznej),

Na podstawie dokonanych ustaleń zauważyć należy, iż po rozbrojeniu alarmu należy udać się na 2 piętro budynku i otworzyć pomieszczenie serwerowni przy użyciu klucza tradycyjnego. Powyższe oznacza, iż od momentu rozbrojenia alarmu do momentu dotarcia do serwerowni osoby do tego uprawnionej, serwerownia może pozostawać bez nadzoru, co nie powinno mieć miejsca.

W dniu prowadzenia oględzin stwierdzono, iż dla serwerowni nie prowadzono ewidencji wejść i wyjść, która pozwalałaby ustalić datę, godzinę, imię i nazwisko, podmiot/instytucję/jednostkę, cel wejścia, itp. Również system właściwy dla konsoli alarmu, mimo że odnotowywał datę i godzinę wpisania kodu, nie umożliwiał sprawdzenia kto wpisał dany kod do alarmu. Zauważyć jednak należy, iż w pismem z dnia 6 maja 2026 r. DWIIH poinformował, iż zmieniono ustawienia centrali alarmowej w taki sposób, aby możliwe było sprawdzenie kto wpisał kod do alarmu.

W toku oględzin stwierdzono, iż serwery są na bieżąco monitorowane przez program Zabbix w zakresie temperatury urządzenia. Zauważyć należy jednak, iż program Zabbix jest narzędziem monitoringu dystrybuowanym w oparciu o licencję open source, a jego kod źródłowy jest dostępny do użytku publicznego[15]. Zauważyć należy, że używanie programu open source nie zabezpiecza w stu procentach przed ingerencją zewnętrzną lub wystąpieniem awarii, która może nie zostać stwierdzona w odpowiednim momencie. Ponadto, brak czujnika wilgoci, czujnika wilgotności i temperatury pomieszczenia oraz czujnika zalania pomieszczenia może powodować wydłużenie czasu reakcji na sytuacje awaryjne, przez co może dojść do uszkodzenia urządzeń znajdujących się w serwerowni. Mając na uwadze powyższe, istnieje ryzyko paraliżu w funkcjonowaniu jednostki, w szczególności, iż stwierdzono brak UPS-ów podtrzymujących serwery jednostki w innych pomieszczeniach (zasilanie awaryjnie z UPS-a znajduje się w pomieszczaniu serwerowni).

Powyższe ryzyko odnosi się również do przechowywania kopii zapasowych serwera maszyn wirtualnych i plików w pomieszczeniu serwerowni.

Co więcej, ściany pomieszczenia serwerowni zrobione są w cienkiego materiału, który nie daje gwarancji zatrzymania próby dostania przy użyciu siły, co może nie zapewniać należytej ochrony pomieszczenia w sytuacji obecności w na drugim piętrze osób trzecich bez nadzoru lub bez zezwolenia.

W dniu przeprowadzania oględzin stwierdzono, iż przed pomieszczeniem serwerowni, na korytarzu, znajdowała się niezabezpieczona skrzynka z bezpiecznikami zarządzającymi m. in. klimatyzacją serwerowni. W ww. piśmie z dnia 6 maja 2026 r. DWIIH poinformował również, że znajdująca się na korytarzu skrzynka z bezpiecznikami została zabezpieczona przed dostępem osób trzecich (w drzwiach skrzynki zamontowano zamek).

[dowód: akta kontroli str.: 202-215]

Podsumowując, powyższy obszar dotyczący zabezpieczeń techniczno - organizacyjnych dostępu do informacji oceniono **pozytywnie pomimo stwierdzonych nieprawidłowości.**

[15] https://www.zabbix.com/documentation/6.0/pl/manual/introduction/about.

8. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.

Zgodnie z przepisem § 19 ust. 2 pkt 12 r.k.r.i. zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych. Powyższy obowiązek wskazuje otwarty katalog kwestii, mających istotne znaczenie przy tworzeniu odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych:

a) dbałości o aktualizację oprogramowania,
b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnieniu bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

W toku czynności kontrolnych dokonano weryfikacji powyższych kwestii.

Jak już wspomniano w części dotyczącej zarządzania uprawnieniami do pracy w systemach informatycznych, w trakcie prowadzenia czynności kontrolnych dokonano sprawdzenia trzech stacji roboczych pracowników WIIH, ASI, Pani E.R. oraz Pani M.W., na podstawie których ustalono co następuje.

Wskazani powyżej pracownicy posiadali adekwatne do wykonywanych zadań uprawnienia na swoich stacjach roboczych, co należy ocenić pozytywnie.

[dowód: akta kontroli str.: 139-187, 188-201]

Zgodnie z § 4 Instrukcji zarządzania systemem informatycznym hasło do systemu informatycznego powinno składać się z co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne. Ponadto, hasło nie może być identyczne z identyfikatorem użytkownika. W SZBI nie określono wymogów w zakresie częstotliwości zmian hasła (rotacji haseł) ani historii haseł (recykling haseł).

Zgodnie z wyjaśnieniami ASI, polityka globalna w WIIH przewiduje hasło złożone z 8 znaków przy złożoności uwzględniającej znak szczególny, dużą i małą literę, cyfrę, a hasło nie może być elementem nazwy użytkownika. Zasada ta wynika z domyślnie wbudowanych reguł Windows. Hasło jest niewygasające, a historia haseł zapamiętuje do jednego hasła wstecz. Zasadą wprowadzono również konieczność wprowadzenia hasła ponownie po nastąpieniu stanu wstrzymania urządzenia. W toku kontroli ustalono również, iż zgodnie z wyciągiem z globalnych polityk WIIH nie ustawiono progów blokady kont przy nieudanych próbach logowania, co umożliwia ataki typu brute-force.

Weryfikacja polityki haseł na stacjach roboczych wskazanych pracowników wykazała, iż komputery Pani E.R. oraz Pani M.W. są podpięte pod globalne polityki ochrony WIIH a użytkownicy nie posiadają uprawnień administratora na swoich stacjach roboczych, natomiast urządzenie ASI jest wyjęte z globalnych polityk ochrony WIIH.

Ponadto, poddane kontroli systemy (EZD, Vulcan, Zabbix) nie zostały zsynchronizowane z domeną WIIH, zatem ich polityki haseł narzucane są przez producenta i nie ma możliwości weryfikacji przez ASI, czy użytkownicy stosują hasła zgodne z § 4 Instrukcji zarządzania systemem informatycznym.

Mając na uwadze powyższe zauważyć należy, iż w SZBI powinny zostać określone kwestie rotacji i recyklingu haseł, nawet jeżeli hasło jest niewygasające, gdyż SZBI winno określać główne zasady bezpieczeństwa, które następnie realizowane są w praktyce przez wdrożenie odpowiednich reguł w systemach informatycznych. Polityka haseł określona w SZBI powinna obowiązywać każdego pracownika, podczas gdy stacja robocza ASI jest wyjęta z globalnych polityk ochrony. Ponadto nie podjęto działań zmierzających do wdrożenia polityki haseł określonej w SZBI w poddanych kontroli systemach. Wskazane powyżej kwestie ocenia się negatywnie.

[dowód: akta kontroli str.: 116-124, 139-187, 202-215, 352-359]

Zasady ochrony systemów informatycznych przed szkodliwym oprogramowaniem określono w § 11 Instrukcji zarządzania systemem informatycznym.

W toku kontroli ustalono, iż na stacjach roboczych Pani E.R. oraz Pani M.W. system antywirusowy, jak i zapora sieciowa, były uruchomione w najnowszej wersji wraz z aktualizacjami bazy danych. W toku kontroli ustalono również, iż stacja robocza ASI nie posiadała włączonej zapory sieciowej.

Zgodnie z wyjaśnieniami, ASI zarządza globalnie zabezpieczeniami antywirusowymi i zaporą wszystkich użytkowników w WIIH oraz otrzymuje monity dot. ewentualnych naruszeń.

Mając na uwadze powyższe należy negatywnie ocenić brak uruchomionej zapory sieciowej na stacji roboczej ASI. Pozostałe kwestie ocenia się pozytywnie.

[dowód: akta kontroli str.: 116-124, 139-187, 202-215, 352-359]

Polityka wygaszacza ekranu nie została określona w SZBI. Zgodnie z globalną polityką ochrony WIIH w Active Directory wygaszacz ekranu powinien być na 300 sekund.

W wyniku sprawdzenia stacji roboczych wybranych pracowników ustalono, iż na stacjach roboczych Pani E.R. oraz Pani M.W. wygaszacz ekranu uruchamia się po 300 sekundach (5 minutach), natomiast na stacji roboczej ASI po 600 sekundach (10 minutach). Ponadto, z wyjaśnień ASI wynika, iż gdy komputer jest podłączony do zasilania, wtedy nie funkcjonuje automatyczne wygaszanie ekranu. Gdy komputer korzysta z baterii, wygaszanie ekranu ustawione jest po upływie 15 minut, natomiast wyłączenie dysku twardego następuje po 30 minutach.

Mając na uwadze powyższe, brak regulacji SZBI we wskazanym zakresie oraz niezgodność ustawień na koncie ASI z globalną polityką ocenia się negatywnie.

[dowód: akta kontroli str.: 139-187, 202-215]

Kwestie dotyczące zabezpieczeń w ramach pracy na odległość i mobilnego przetwarzania danych zostały opisane w obszarze C pkt 6 niniejszego dokumentu i oceniono je pozytywnie.

W odniesieniu do zabezpieczeń systemów informatycznych poddanych kontroli stwierdzono, iż połączenie z systemem EZD oraz Vulcan jest szyfrowane za pomocą protokołu SSL/TLS, zapewniając ochronę informacji. Zgodnie z wyjaśnieniami ASI, połączenie z systemem Zabbix przez przeglądarkę internetową nie jest szyfrowane. W systemie Zabbix monitorowane są zdarzenia w innych systemach wykorzystywanych przez WIIH, przykładowo w EZD, poczcie służbowej i na stacjach roboczych pracowników. Połączenie webowe z Zabbix, mimo iż domyślnie nie jest szyfrowane, jest możliwe do samodzielnego wdrożenia.

Powyższe należy ocenić pozytywnie pomimo stwierdzonych nieprawidłowości.

[dowód: akta kontroli str.: 139-187]

Kwestie dotyczące zabezpieczeń w ramach sporządzania kopii zapasowych zostały opisane w obszarze C pkt 10 niniejszego dokumentu i oceniono je pozytywnie.

W odniesieniu do zapewnienia ciągłości działania systemów ustalono, iż zgodnie z § 12 Instrukcji zarządzania systemem informatycznym, system i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, a przedmiotowe zabezpieczenie realizuje się przez polega na wyposażeniu serwerów, zapór sieciowych oraz sprzętu sieciowego w zasilacze awaryjne UPS. W wyniku kontroli ustalono, iż wskazane zasilacze znajdują się w pomieszczeniu serwerowni, natomiast w sekretariacie WIIH znajduje się UPS podtrzymujący napięcie w systemie centrali telefonicznej.

Powyższe oceniono pozytywnie.

[dowód: akta kontroli str.: 116-124, 202-215, 352-359]

Odnosząc się do ustalonego powyżej stanu faktycznego stwierdzono, iż kontrolowany zasadniczo zapewnia ochronę przetwarzanych informacji zgodnie z przepisem § 19 ust. 2 pkt 12 r.k.r.i., mając jednak na względzie stwierdzone nieprawidłowości zagadnienie oceniono **pozytywnie pomimo stwierdzonych nieprawidłowości.**

9. Rozliczalność działań w systemach teleinformatycznych.

Rozliczalność jest właściwością systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie. Z tego względu zapewnienie rozliczalności działań polega na gromadzeniu informacji o tym, kto, kiedy i jakie czynności wykonał w systemie. Obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi) wszystkie działania dostępu do systemu z uprawnieniami administracyjnymi, w zakresie konfiguracji systemu i zabezpieczeń, a także działania, gdy przetwarzanie danych podlega prawnej ochronie.

Zgodnie z § 20 ust. 2 r.k.r.i. w dziennikach systemowych należy odnotowywać działania użytkowników lub obiektów systemowych polegające na dostępie do systemu z uprawnieniami administracyjnymi, konfiguracji systemu, w tym konfiguracji zabezpieczeń, przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

W wyniku kontroli stwierdzono że rozliczalność występuje we wszystkich systemach poddanych kontroli – zarówno w systemie EZD, Vulcan jak i Zabbix . Powyższe należy ocenić **pozytywnie.**

[dowód: akta kontroli str.: 139-187]

10. Kopie zapasowe.

Zgodnie z § 19 ust. 2 pkt 12 lit. b r.k.r.i. podmiot publiczny obowiązany jest do zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych poprzez minimalizowanie ryzyka utraty informacji w wyniku awarii. Do realizacji owego obowiązku niezbędne jest opracowanie odpowiednich procedur i podjęcie określonych w nich działań polegających na zabezpieczaniu przetwarzanych przez jednostkę danych, poprzez tworzenie kopii zapasowych zbiorów danych przetwarzanych w niej przetwarzanych.

Kwestie dotyczące tworzenia kopii zapasowych systemów teleinformatycznych opisane zostały w Instrukcji zarządzania systemem informatycznym w związku z koniecznością

przetwarzania danych osobowych w Wojewódzkim Inspektoracie Inspekcji Handlowej we Wrocławiu. We wskazanym dokumencie, w treści § 10 wskazano częstotliwość wykonywania kopii zapasowych, tj. raz dziennie na serwerze kopii zapasowych[16], informację, iż raz w miesiącu przedmiotowe kopie zostają zgrane na nośnik zewnętrzny i przechowywane są w pomieszczeniu informatyków, a także odpowiedzialność ASI za okresowy przegląd i ocenę przydatności kopii awaryjnych. Treść SZBI nie określa jednak długości przechowywania rzeczonych kopii ani kryteriów ani cykliczności dokonywania wskazanych przeglądów i ocen.
[dowód: akta kontroli str.: 116-124, 352-359]

Zgodnie z wyjaśnieniami udzielonymi w toku prowadzonych oględzin serwerowni kopie zapasowe serwera maszyn wirtualnych i plików znajdują się w pomieszczeniu serwerowni. Kopia zapasowa danych WIIH jest robiona raz dziennie, natomiast raz w miesiącu jest ona zgrywana na zabezpieczony nośnik zewnętrzny i przechowywana w pomieszczeniu informatyków na parterze budynku. Powyższe wyjaśnienia pokrywają się z zapisami SZBI.
[dowód: akta kontroli str.: 202-215]

Na podstawie powyższych stwierdzono, iż jednostka kontrolowana minimalizuje ryzyko utraty informacji w wyniku awarii tworząc kopie zapasowe, czym zapewnia odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, zgodnie z § 19 ust. 2 pkt 12 lit. b r.k.r.i., a zagadnienie należy ocenić **pozytywnie.**

11. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Zgodnie z § 19 ust. 2 pkt 2 r.k.r.i. podmiot publiczny zobowiązany jest do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Posiadanie takich informacji jest niezbędne przy wprowadzaniu wszelkich zmian w środowisku informatycznym. Jednocześnie należy podkreślić, że ww. baza nie jest tożsama z zapisami księgi inwentarzowej. Zawiera ona bowiem, w szczególności informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku.

W toku kontroli ustalono, iż w dokumentacji SZBI jedyna wzmianka o inwentaryzacji sprzętu i oprogramowania znajduje się w § 5 Regulaminu pracy zdalnej, stanowiącego załącznik nr 6 do Regulaminu pracy w WIIH. Wskazano tam, iż pracodawca na swój koszt zapewnia instalację, inwentaryzację, konserwację, aktualizację oprogramowania oraz serwis narzędzi pracy przekazanych pracownikowi i w tym celu pracownik uzgadnia terminy konkretnych czynności związanych z instalacją, inwentaryzacją, konserwacją, aktualizacją oprogramowania i serwisem z bezpośrednim przełożonym. Żaden z dokumentów SZBI nie określa kto przeprowadza inwentaryzację, kiedy, jak często dokonywana jest weryfikacja informacji w niej zawarta, ani jakie dane gromadzone są w ramach inwentaryzacji.

Zgodnie z treścią wyjaśnień z dnia 27 maja 2026 r. w WIIH, do inwentaryzacji sprzętu i oprogramowania, stosuje się moduł SysInspector programu antywirusowego ESET. Moduł na bieżąco, przy każdym połączeniu zarządzanego komputera, zbiera informacje o parametrach sprzętowych i zainstalowanym oprogramowaniu. Moduł umożliwia weryfikacją sprzętu i oprogramowania pojedynczych komputerów. Dodanie nowego sprzętu do inwentaryzacji jest

[16] Z wyłączeniem systemu kadrowo-płacowego i finansowo-księgowego, gdzie zgodnie z umową kopie danych tworzy dostawca systemu w formie chmury danych.

dokonywane podczas instalacji programu antywirusowego na komputerze przy wprowadzaniu danego komputera do użytku w WIIH. Zarówno w regulacjach SZBI jak i w przedmiotowych wyjaśnieniach brak jest informacji na temat inwentaryzacji pozostałego sprzętu i oprogramowania stosowanych w WIIH, np. systemów webowych, nośników danych typu pendrive itp.

[dowód: akta kontroli str.: 292-321, 377-381]

Wobec dokonanych ustaleń należy uznać, iż kontrolowany podmiot podejmował pewne działania w celu wypełnienia dyspozycji przepisu § 19 ust. 2 pkt 2 r.k.r.i., jednakże brak stosownych regulacji i brak posiadania pełnej inwentaryzacji posiadanego sprzętu w WIIH należy ocenić **negatywnie.**

12. Serwis sprzętu informatycznego i oprogramowania.

Przepis § 19 ust. 2 pkt 10 r.k.r.i. przewiduje, że umowy serwisowe podpisane ze stronami trzecimi powinny zawierać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. W odniesieniu do systemów teleinformatycznych i oprogramowania o znaczeniu krytycznym dla funkcjonowania jednostki niezbędne jest objęcie ich (w zakresie zarówno oprogramowania użytkowego i systemowego, jak i sprzętu) stosownymi umowami serwisowymi, aby zapewnić gwarancję odpowiednio szybkiego wznowienia pracy systemów w przypadku wystąpienia awarii. Umowy takie, zgodnie z § 19 ust. 2 pkt 10 r.k.r.i. powinny posiadać zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, w przypadku wejścia w ich posiadanie przez podmioty serwisujące.

Kwestie dotyczące zasad konserwacji i serwisowania sprzętu teleinformatycznego, opisane zostały w § 13 i § 14 Instrukcji zarządzania systemem informatycznym w związku z koniecznością przetwarzania danych osobowych. W treści wskazanych przepisów określono, iż urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy po uprzednim pozbawieniu zapisu danych albo naprawa może nastąpić w obecności osoby upoważnionej przez administratora danych osobowych, jeżeli nie ma możliwości by pozbawić sprzęt zapisu danych. W odniesieniu do przeglądu i konserwacji systemów, dokonywana jest ona doraźnie przez ASI, w tym przez codzienny przegląd logów systemu.

Z wyjaśnień udzielonych pismem z dnia 27 maja 2026 r. wynika, iż WIIH nie ma podpisanych żadnych umów na serwisowanie sprzętu i oprogramowania informatycznego. Powyższe wyjaśnienia są sprzeczne z pkt 2.10.1 informacji przedkontrolnej z dnia 27 marca 2026 r. gdzie wskazano, iż WIIH posiada umowę z firmą Vulcan oraz porozumienia zawarte z NASK oraz GOV.PL. W ramach zastrzeżeń do projektu wystąpienia pokontrolnego, Kontrolowany przedstawił umowy dotyczące serwisu sprzętu i oprogramowania. Analiza przedmiotowych umów wykazała, iż:

a) umowa powierzenia danych z NASK nie posiada podpisu ani fizycznego ani elektronicznego, zatem nie można uznać jej jako obowiązującej w WIIH,
b) umowa z Polską Telefonią Cyfrową nie jest umową serwisową. Z przekazanych dokumentów nie wynika na jakich warunkach i w jakim zakresie świadczony jest serwis sprzętu czy oprogramowania,
c) umowy z Polkomtel sp. z o.o. (telekomunikacja i Internet) oraz umowa z T-Mobile Polska s.a. zostały podpisane przez ASI, mimo iż ustawowo uprawnionym do reprezentowania jednostki kontrolowanej na zewnątrz jest DWIIH. W przekazanej dokumentacji nie znajdowały się upoważnienia do podjęcia wskazanych czynności przez ASI.
d) umowy z VULCAN Sp. z o. o. nie są umowami serwisowymi. Z przekazanych dokumentów nie wynika na jakich warunkach i w jakim zakresie świadczony jest serwis oprogramowania.

e) umowy z Ogólnopolską Grupą IT Danuta Walczak, CEZAR" Cezary Machnio i Piotr Gębka Sp. z o.o., EXTRATEL s.c., Oxylion s.a., Korbank s.a. oraz INFUS Katarzyna Fuśnik ocenia się prawidłowo.

W treści § 5 ust. 2 Regulaminu pracy zdalnej wskazano, iż pracodawca na swój koszt zapewnia instalację, inwentaryzację, konserwację, aktualizację oprogramowania oraz serwis narzędzi pracy przekazanych pracownikowi i w tym celu pracownik uzgadnia terminy konkretnych czynności związanych z instalacją, inwentaryzacją, konserwacją, aktualizacją oprogramowania i serwisem z bezpośrednim przełożonym.

Mając na uwadze przekazaną dokumentację stwierdzono, iż brak posiadania stosownych umów serwisowych, zawarcie ich przez osoby nieuprawnione oraz niezłożenie wymaganych podpisów stanowi zagrożenie dla dostępności i ciągłości działania sprzętu i systemów.

[dowód: akta kontroli str.: 292-321, 377-381]

Mając na uwadze powyższe, wskazany obszar ocenia się **negatywnie.**

13. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.

Treść § 19 ust. 2 pkt 6 r.k.r.i. nakłada wymóg zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, a także stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Kwestie szkoleń dla osób zaangażowanych w proces przetwarzania informacji wspominane zostały w dwóch dokumentach z zakresu SZBI: § 5 ust. 1 pkt 3 Regulaminu pracy zdalnej oraz w § 6 ust. 2 pkt 3 Polityki Ochrony Danych Osobowych. Przedmiotowe zapisy wskazują jedynie obowiązek Pracodawcy oraz Inspektora Ochrony Danych Osobowych do przeprowadzania szkoleń w zakresie pracy zdalnej oraz ochrony danych osobowych, nie wskazując jednak częstotliwości takich szkoleń.

[dowód: akta kontroli str.: 87-108, 243-275, 325-345]

Z przekazanej przez kontrolowanego informacji wynika, iż w 2024 roku nie były przeprowadzane żadne szkolenia dotyczące bezpieczeństwa informacji, natomiast w szkoleniach przeprowadzanych w latach 2025-2026 udział brało tylko część pracowników WIIH – na 70 pracowników Inspektoratu, wskazanych w informacji przedkontrolnej, w najliczniejszym pod względem osób szkoleniu pn. „Cyberbezpieczeństwo w organizacji: Skąd przestępcy mają nasze dane? - Prywatność w sieci”, które odbyło się dnia 18 marca 2025 r. w formie webinaru, wzięło udział 15 pracowników. Ponadto Kontrolowany wyjaśnił, iż każdy z nowo zatrudnionych pracowników WIIH nowi pracownicy przechodzą szkolenie z zakresu cyberbezpieczeństwa i wprowadzenia do zasad pracy z komputerem w WIIH. Proces ten prowadzi ASI z użyciem komputera i systemów, których pracownik będzie używał w pracy.

Powyższe nie jest wystarczające by stwierdzić, że w WIIH realizowany jest wymóg wynikający z § 19 ust. 2 pkt 6 lit. a-c r.k.r.i. w stosunku do wszystkich pracowników zaangażowanych w proces przetwarzania informacji. Zagadnienie ocenione zostało zatem **pozytywnie pomimo stwierdzonych nieprawidłowości.**

[dowód: akta kontroli str.: 382-426]

IV. Pozostałe informacje i zalecenia pokontrolne

Wystąpienie pokontrolne sporządzono w postaci dokumentu elektronicznego.

Na podstawie ustaleń kontroli, w celu dalszego usprawnienia realizacji kontrolowanego zadania należy:

1. Aktualizować w BIP procedury obowiązujące klientów WIIH przy załatwianiu spraw, w szczególności w zakresie świadczenia usług drogą elektroniczną.
2. Zapewnić ochronę pozostałych kategorii danych przetwarzanych w WIIH poprzez uwzględnienie ich w regulacjach z zakresu SZBI.
3. W dokumentacji z zakresu SZBI stosować terminologię spójną i precyzyjną dla całego zakresu regulacji.
4. Przeprowadzać cykliczne analizy ryzyka utraty integralności, dostępności lub poufności informacji, zgodnie z § 19 ust. 2 pkt 3 r.k.r.i.
5. Uregulować procedurę zgłaszania incydentów w WIIH uwzględniającą wszystkie czynności i osoby ich dokonujące od momentu wystąpienia incydentu do momentu reakcji na incydent.
6. Przeprowadzać i dokumentować czynności audytowe, mając na uwadze obowiązek wynikający z § 19 ust. 2 pkt 14 r.k.r.i.
7. Prowadzić rejestr upoważnień udzielonych w WIIH w sposób rzetelny.
8. Uwzględnić w dokumentacji z zakresu SZBI kwestie związane z bezpieczeństwem pomieszczeń, w których przetwarzane są informacje oraz kwestie dotyczące uruchamiania alarmu po zakończeniu prac porządkowych.
9. W miarę możliwości zwiększyć zabezpieczenia serwerów i serwerowni zgodnie z uwagami poczynionymi w obszarze C pkt 7 niniejszego dokumentu.
10. Ujednolicić wymagania określone w SZBI, w zakresie wygaszaczy ekranu, ze stosowanymi globalnymi politykami ochrony na stacjach roboczych oraz zapewnić, by każda stacja robocza WIIH podlegała przedmiotowym politykom.
11. Wdrożyć odpowiednie szyfrowanie informacji przetwarzanych przez system Zabbix.
12. Dokonywać inwentaryzacji zarówno sprzętu jak i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację, zgodnie z § 19 ust. 2 pkt 2 r.k.r.i.
13. Przy zawieraniu umów serwisowych dbać o kompletność zawieranych umów, odpowiednią reprezentację podmiotu oraz prawidłowość składanych podpisów.
14. Zapewnić szkolenia z zakresu bezpieczeństwa informacji wszystkim pracownikom przetwarzającym dane w WIIH, a także w sposób rzetelny dokumentować ich udział w rzeczonych szkoleniach.

Mając na uwadze art. 49 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej proszę o poinformowanie o sposobie wykonania powyższych zaleceń lub o przyczynach ich niewykonania, w terminie **do 31 sierpnia 2026 r.**

Z up. WOJEWODY DOLNOŚLĄSKIEGO
Damian Domusiewicz
Z-CA DYREKTORA WYDZIAŁU
Prawnego, Nadzoru i Kontroli
/podpisano kwalifikowanym podpisem elektronicznym/