II

(Komunikaty)

KOMUNIKATY INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

KOMISJA EUROPEJSKA

ZAWIADOMIENIE KOMISJI

Wytyczne w sprawie rocznych sprawozdań z audytu, które należy przedłożyć zgodnie z art. 15 ust. 8 dyrektywy 2014/40/UE w kontekście unijnego systemu identyfikowalności wyrobów tytoniowych

(Tekst mający znaczenie dla EOG)

(2020/C 167/01)

ZASTRZEŻENIE PRAWNE: Celem niniejszego dokumentu jest przedstawienie zatwierdzonemu audytorowi wytycznych na temat zakresu audytu oraz procedury przedkładania rocznego sprawozdania z audytu. Nie jest on prawnie wiążący, lecz zawiera ogólne wytyczne i zalecenia oraz informacje na temat najlepszych praktyk. Niniejsze wytyczne pozostają bez uszczerbku dla przepisów krajowych.

1. **Wprowadzenie**

W art. 15 dyrektywy Parlamentu Europejskiego i Rady 2014/40/UE ([1]) przewidziano ustanowienie ogólnounijnego systemu identyfikowalności wyrobów tytoniowych w celu rozwiązania problemu nielegalnego handlu. System ten zaczął funkcjonować w dniu 20 maja 2019 r.

W ramach tego systemu art. 15 ust. 8 dyrektywy 2014/40/UE zobowiązuje państwa członkowskie do zapewnienia, aby producenci i importerzy wyrobów tytoniowych zawarli umowy w sprawie przechowywania danych z niezależną stroną trzecią („dostawca będący stroną trzecią") w celu ustanowienia ośrodka przechowywania danych dotyczących wyrobów tytoniowych poszczególnych producentów i importerów („repozytorium pierwotne").

W celu ochrony niezależnego funkcjonowania systemu identyfikowalności art. 15 ust. 8 dyrektywy 2014/40/UE stanowi, że audytor zewnętrzny monitoruje działalność repozytorium pierwotnego i jego dostawcy będącego stroną trzecią. Audytor jest proponowany i opłacany przez producenta tytoniu oraz zatwierdzany przez Komisję. Audytor zewnętrzny przedkłada swoją ocenę w formie rocznego sprawozdania właściwym organom krajowym i Komisji, oceniając zwłaszcza wszelkie naruszenia dotyczące dostępu.

Celem niniejszego dokumentu jest przedstawienie zatwierdzonemu audytorowi wytycznych na temat zakresu audytu oraz procedury przedkładania rocznego sprawozdania z audytu. Należy go odczytywać w związku z rozporządzeniem wykonawczym Komisji (UE) 2018/574 ([2]), w którym określono wymogi techniczne dotyczące ustanowienia i funkcjonowania systemu identyfikowalności, w tym dla repozytoriów pierwotnych, oraz rozporządzeniem delegowanym Komisji (UE) 2018/573 ([3]) określającym główne elementy umów w sprawie przechowywania danych zawieranych w ramach systemu identyfikowalności.

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2014/40/UE z dnia 3 kwietnia 2014 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich w sprawie produkcji, prezentowania i sprzedaży wyrobów tytoniowych i powiązanych wyrobów oraz uchylająca dyrektywę 2001/37/WE (Dz.U. L 127 z 29.4.2014, s. 1).

([2]) Rozporządzenie wykonawcze Komisji (UE) 2018/574 z dnia 15 grudnia 2017 r. w sprawie norm technicznych dotyczących ustanowienia i funkcjonowania systemu identyfikowalności wyrobów tytoniowych (Dz.U. L 96 z 16.4.2018, s. 7).

([3]) Rozporządzenie delegowane Komisji (UE) 2018/573 z dnia 15 grudnia 2017 r. w sprawie głównych elementów umów w sprawie przechowywania danych zawieranych w ramach systemu identyfikowalności wyrobów tytoniowych (Dz.U. L 96 z 16.4.2018, s. 1).

Niniejszy dokument jest dostępny jako narzędzie dla zatwierdzonych audytorów; zawiera niewiążące wytyczne i nie powoduje żadnych nowych zobowiązań prawnych. W zakresie, w jakim niniejsze wytyczne mogą zawierać wykładnię przepisów, stanowisko Komisji pozostaje bez uszczerbku dla jakiejkolwiek wykładni przedmiotowej dyrektywy, której może dokonać Trybunał Sprawiedliwości Unii Europejskiej.

2. **Ogólny kontekst audytów**

Każde repozytorium pierwotne zakontraktowane przez producenta podlega corocznemu procesowi audytu. W przypadku gdy ten sam dostawca będący stroną trzecią prowadzi dwa lub większą liczbę repozytoriów pierwotnych, dla każdego repozytorium powinno się przeprowadzić oddzielny audyt i przedłożyć odrębne sprawozdanie z audytu.

Należy przeprowadzić audyt w odniesieniu do repozytorium pierwotnego i powiązanych z nim usług, w tym pod kątem oceny, czy dany dostawca będący stroną trzecią oraz – w stosownych przypadkach – jego podwykonawcy spełniają odpowiednie wymogi prawne określone w dyrektywie 2014/40/UE, rozporządzeniu wykonawczym (UE) 2018/574 i rozporządzeniu delegowanym (UE) 2018/573.

Każdy producent lub importer musi powiadomić Komisję o proponowanym przez siebie audytorze, który ma przeprowadzić audyt jego repozytorium pierwotnego, i odpowiednim dostawcy będącym stroną trzecią. Wszyscy proponowani audytorzy podlegają zatwierdzeniu przez Komisję.

3. **Zakres audytu**

Zakres i cel

Należy przedłożyć sprawozdania z audytu w celu poinformowania właściwych organów krajowych i Komisji o ustaleniach audytorów, w szczególności w odniesieniu do wszelkich naruszeń dotyczących dostępu do danych przechowywanych przez repozytoria pierwotne.

Sprawozdania z audytu powinny zawierać oddzielne rozdziały dla każdej z sześciu wymienionych poniżej dziedzin. Każdy rozdział powinien dotyczyć punktów kontrolnych danej dziedziny, wymienionych w liście kontrolnej znajdującej się w załączniku.

Audyty należy przeprowadzać zgodnie ze wspomnianą listą kontrolną określającą wymagane dziedziny i punkty kontrolne zgodnie z normą ISO/IEC 27001:2013 dotyczącą systemów zarządzania bezpieczeństwem informacji ([4]). W tym celu audytorzy powinni mieć na uwadze, że art. 10 rozporządzenia delegowanego Komisji (UE) 2018/573 odnosi się do ISO/IEC 27001:2013 jako do preferowanej normy zarządzania bezpieczeństwem informacji w kontekście prowadzenia repozytoriów pierwotnych.

Dziedzina	Cele
Bezpieczeństwo organizacyjne i fizyczne	Ustanowienie ram zarządzania bezpieczeństwem informacji w ramach organizacji. Zapewnienie, aby pracownicy i wykonawcy rozumieli swoje obowiązki i byli odpowiednimi kandydatami do wypełniania ról, do których są przewidziani. Zapobieganie nieuprawnionemu fizycznemu dostępowi, szkodom lub zakłóceniom w organizacji, w tym w odniesieniu do informacji i środków przetwarzania informacji. Zapobieganie utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.
Bezpieczeństwo eksploatacji	Zapewnienie poprawnej i bezpiecznej eksploatacji środków przetwarzania informacji. Ochrona przed utratą danych. Rejestrowanie zdarzeń i zbieranie materiałów dowodowych. Zapewnienie integralności systemów operacyjnych. Zapobieganie wykorzystywaniu podatności technicznych.
Kontrola dostępu (użytkownicy i aplikacje)	Ograniczenie dostępu do informacji i do środków przetwarzania informacji. Zapewnienie dostępu uprawnionym użytkownikom oraz zapobieganie nieuprawnionemu dostępowi do systemu i usług. Zapewnienie rozliczalności użytkowników za zabezpieczenie ich informacji uwierzytelniających. Zapobieganie nieuprawnionemu dostępowi do systemów i aplikacji. Zapewnienie projektowania i wdrażania bezpieczeństwa informacji w ramach cyklu życia systemów informacyjnych.

([4]) ISO/IEC 27001:2013. Information technology — security techniques – information security management systems – requirements [Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania] Wymagania określone w normie ISO/IEC 27001:2013 mają charakter ogólny i mają zastosowanie do wszystkich organizacji, bez względu na rodzaj, wielkość lub charakter.

Dziedzina	Cele
Bezpieczeństwo komunikacji	Zapewnienie właściwego i skutecznego wykorzystania kryptografii w celu ochrony poufności, autentyczności lub integralności informacji. Zapewnienie ochrony informacji w sieciach oraz wspomagających je środkach przetwarzania informacji. Utrzymanie bezpieczeństwa informacji przekazywanych w ramach organizacji i w ramach podmiotów zewnętrznych.
Ciągłość działania	Zapewnienie spójnego i skutecznego podejścia do zarządzania incydentami związanymi z bezpieczeństwem informacji, w tym informowania o zdarzeniach związanych z bezpieczeństwem i słabościach systemu bezpieczeństwa. Ciągłość bezpieczeństwa informacji musi być uwzględniona w systemach zarządzania ciągłością działania organizacji. Zapewnienie dostępności środków przetwarzania informacji. Unikanie naruszeń zobowiązań prawnych, obowiązków ustawowych i regulacyjnych lub zobowiązań umownych związanych z bezpieczeństwem informacji oraz wszelkich wymagań w zakresie bezpieczeństwa.
Aktywa i integralność danych	Identyfikacja aktywów organizacyjnych i określenie odpowiednich obowiązków w zakresie ochrony. Zapewnienie, by informacjom przypisano odpowiedni poziom ochrony. Zapobieganie nieuprawnionemu ujawnianiu, zmienianiu, usuwaniu lub niszczeniu informacji przechowywanych na nośnikach.

Wnioski i zalecenia

Wnioski z audytu należy przedstawić dla każdego punktu kontrolnego wymienionego w liście kontrolnej.

W sprawozdaniu z audytu należy jedynie podkreślać i szczegółowo przedstawiać ustalenia dotyczące kwestii niezgodności lub innych zidentyfikowanych rodzajów ryzyka. Ustaleniom powinny również towarzyszyć odpowiednie zalecenia określające działania niezbędne do usunięcia problemów i niedociągnięć stwierdzonych w trakcie audytu.

4. **Aspekty proceduralne**

Częstotliwość

Audytorzy są zobowiązani do składania sprawozdań z audytu w ujęciu rocznym. Ponieważ system identyfikowalności zaczął funkcjonować w dniu 20 maja 2019 r., audytorzy proszeni są o przedstawienie do dnia 30 listopada 2020 r. pierwszych rocznych sprawozdań z audytu, obejmujących pierwszy rok funkcjonowania systemu identyfikowalności (tj. od dnia 20 maja 2019 r. do dnia 19 maja 2020 r.). Następnie audytorzy są proszeni o składanie sprawozdań rocznych za kolejne lata funkcjonowania do końca października każdego roku kalendarzowego.

Czynności po przeprowadzeniu audytu

W przypadku przeprowadzenia działań następczych w celu oceny, czy dany dostawca będący stroną trzecią odpowiednio wprowadził zalecenia do rocznego sprawozdania z audytu, audytor jest w miarę możliwości proszony o przedłożenie wyników Komisji i właściwym organom krajowym w terminie trzech miesięcy od przedłożenia rocznego sprawozdania z audytu.

5. **Aspekty proceduralne sprawozdań z audytu**

Informacje dotyczące audytorów

We wprowadzeniu do sprawozdania z audytu powinny być wskazane nazwiska audytorów oraz w stosownych przypadkach powiązane firmy audytorskie.

Format

Sprawozdanie z audytu powinno być przedstawione w formacie elektronicznym (niezabezpieczony plik w formacie PDF z funkcją wyszukiwania).

Audytorzy są proszeni o przedłożenie Komisji sprawozdań rocznych w miarę możliwości w języku angielskim.

Procedura składania wniosków

Roczne sprawozdanie z audytu i ewentualne sprawozdanie uzupełniające należy przesyłać drogą elektroniczną na adres: SANTE-TT-SW@ec.europa.eu, wpisując w temacie wiadomości następujące informacje: „Audit report [follow-up to the audit report] for [rok] – [Nazwa producenta, który zawarł umowę] – [Nazwa dostawcy będącego stroną trzecią poddanego audytowi]”

Przejrzystość

W celu zwiększania ogólnej przejrzystości i rozliczalności systemu identyfikowalności wyrobów tytoniowych Komisja zwraca się do producentów, aby na zasadzie dobrowolności porozumieli się ze swoimi audytorami w sprawie przesłania Komisji również publicznej wersji sprawozdania z audytu, z wyłączeniem wszelkich danych osobowych i szczególnie chronionych danych handlowych.

Takie publiczne wersje sprawozdań z audytu zostaną opublikowane na specjalnej stronie internetowej Komisji.

ZAŁĄCZNIK

Lista kontrolna dotycząca audytów repozytoriów pierwotnych

Dziedzina	Punkty kontrolne ([1])	Wytyczne regulacyjne	Wytyczne dotyczące dowodów
Bezpieczeństwo organizacyjne i fizyczne	**A.6 Organizacja bezpieczeństwa informacji** — A.6.1 Organizacja wewnętrzna — A.6.2 Urządzenia mobilne i telepraca **A.7 Bezpieczeństwo zasobów ludzkich** — A7.1 Przed zatrudnieniem — A7.2 Podczas zatrudnienia — A7.3 Zakończenie i zmiana zatrudnienia **A.11 Bezpieczeństwo fizyczne i środowiskowe** — A.11.1 Obszary bezpieczne — A.11.2 Sprzęt	Uwagi do pkt A.6 i A.11: Repozytorium musi fizycznie znajdować się na terytorium UE. Dane nie mogą być przechowywane w państwie trzecim ani przekazywane do państwa trzeciego. (art. 15 ust. 8 dyrektywy 2014/40/UE) Repozytorium musi być chronione przez procedury i systemy bezpieczeństwa zapewniające, aby dostęp do repozytorium był zarezerwowany dla właściwych organów państw członkowskich, Komisji i audytorów zewnętrznych. Uwagi do pkt A.7: Dostawca repozytorium oraz jego podwykonawcy muszą być niezależni i wykonywać swoje funkcje w sposób bezstronny. Zastosowanie mają wymogi dotyczące niezależności prawnej, niezależności finansowej i braku konfliktu interesów (art. 35 rozporządzenia wykonawczego (UE) 2018/574)	Schemat organizacyjny organizacji, opisy stanowisk pracy podpisane przez personel kluczowy, udział w odpowiednich szkoleniach dotyczących pełnionych ról. Wykaz nominacji (CISO, IOD itp.) oraz opis obowiązków i zadań w ramach ról pełnionych w zakresie bezpieczeństwa. Dowód uczestnictwa personelu w szkoleniach (np. przyjęte zaproszenie, data i program szkoleń, podpisana lista uczestników warsztatów informacyjnych itp.). Polityka/procedury dotyczące bezpieczeństwa zasobów ludzkich regularnie poddawane przeglądowi i aktualizowane (ewidencja wykonania procedur). Podstawowe wdrożenie środków bezpieczeństwa fizycznego i kontroli otoczenia, takich jak zamki w drzwiach i szafkach, alarmy przeciwwłamaniowe i przeciwpożarowe, gaśnice, telewizja przemysłowa itp. Wykaz personelu z uprawnionym dostępem i upoważnieniami. Udokumentowana polityka dotycząca środków bezpieczeństwa fizycznego i kontroli otoczenia, w tym opis odpowiednich obiektów i systemów. Szczegółowy wykaz obejmujący sprzęt używany do celów administracyjnych.
Bezpieczeństwo eksploatacji	**A.12 Bezpieczeństwo eksploatacji** — A.12.1 Procedury i obowiązki w zakresie eksploatacji — A.12.3 Kopie zapasowe — A.12.4 Rejestrowanie i monitorowanie — A.12.5 Nadzór nad oprogramowaniem operacyjnym — A.12.6 Zarządzanie podatnościami technicznymi	Uwagi do pkt A.12.3: Wszystkie składniki i usługi repozytorium muszą posiadać wystarczający mechanizm zabezpieczający (art. 25 ust. 1 lit. i) rozporządzenia wykonawczego (UE) 2018/574) Uwagi do pkt A.12.4: Repozytorium musi zawierać pełną ścieżkę audytu wszystkich operacji dotyczących przechowywanych danych oraz użytkowników wykonujących powiązane operacje, w tym	Procedura konserwacji systemu bezpieczeństwa odpowiednio udokumentowana i zatwierdzona przez kadrę kierowniczą wyższego szczebla. Jasno zdefiniowany proces utrzymywania minimalnego poziomu bezpieczeństwa. Wykaz wszystkich umów ze stronami trzecimi ([2]). Wymogi w zakresie bezpieczeństwa wyraźnie określone w umowach zawieranych ze stronami trzecimi dostarczającymi produkty informatyczne, usługi informatyczne, zlecane na zewnątrz procesy biznesowe, pomoc techniczną itp.

Dziedzina	Punkty kontrolne ([1])	Wytyczne regulacyjne	Wytyczne dotyczące dowodów
		charakteru tych operacji oraz historii dostępu użytkowników (art. 25 ust. 1 lit. m) rozporządzenia wykonawczego (UE) 2018/574) Wytyczne dotyczące dowodów w odniesieniu do zdarzeń i rejestrowania: — próby logowania i wylogowania (zarówno udane, jak i nieudane) — ponowne uruchamianie serwera bazy danych — polecenia wydawane przez użytkowników z uprawnieniami administratora systemu — próby naruszenia integralności (w przypadku gdy zmienione lub wprowadzone dane nie odpowiadają wartościom więzów spójności referencyjnej, więzów klucza jednoznacznego (*unique*) i więzów *check*) — operacje wyboru, wstawiania, aktualizacji i usunięcia — wykonywanie procedur składowanych — nieudane próby uzyskania dostępu do bazy danych lub tabeli (brak uprawnień) — zmiany w tabelach katalogu systemowego	Udokumentowana polityka bezpieczeństwa w odniesieniu do umów ze stronami trzecimi Udokumentowane uwagi lub dzienniki zmian dotyczące polityki. Wprowadzona i utrzymywana procedura lub polityka oceny ryzyka w zakresie sprzedawcy/zarządzania ryzykiem w zakresie sprzedawcy. Udokumentowane zmiany lub zakończenie relacji ze stronami trzecimi. Sprawozdania z powiązanych działań w zakresie podnoszenia świadomości i szkoleń. Systemy, narzędzia i procedury wykrywania i analizy incydentów. Udokumentowana polityka wykrywania i analizy incydentów uwzględniająca cel, zakres, role i obowiązki oraz koordynację między wszystkimi powiązanymi podmiotami, w tym klientami. Istnienie sprawozdań dotyczących wykrywania i eskalacji minionych incydentów związanych z bezpieczeństwem. Aktualna dokumentacja dotycząca polityki wykrywania incydentów oraz powiązanych procedur i systemów. Wykaz wykrytych i eskalowanych poważnych incydentów mających miejsce w przeszłości, w tym wszystkich powiązanych informacji (przyczyna, skutki, kolejność podjętych działań). Dowody wcześniejszych ćwiczeń w dziedzinie cyberbezpieczeństwa, w tym daty ich przeprowadzenia.
Kontrola dostępu (użytkownicy i aplikacje)	**A.9 Kontrola dostępu** — A.9.1 Wymagania biznesowe wobec kontroli dostępu — A.9.2 Zarządzanie dostępem użytkowników — A.9.3 Obowiązki użytkowników	Uwagi do pkt A.9: Dostęp do ośrodków przechowywania danych i przechowywanych w nich danych należy ograniczyć do państw członkowskich, Komisji Europejskiej i zatwierdzonych audytorów zewnętrznych (art. 15 ust. 8 dyrektywy 2014/40/UE; art. 25 ust. 1 lit. j) rozporządzenia wykonawczego (UE) 2018/574)	Polityka kontroli dostępu, w tym opis ról, grup, praw dostępu, procedur przyznawania i cofania prawa dostępu do systemów informacyjnych. Określenie zasady usuwania nieużywanych już kont po krótkim czasie.

Dziedzina	Punkty kontrolne ([1])	Wytyczne regulacyjne	Wytyczne dotyczące dowodów
	— A.9.4 Kontrola dostępu do systemów i aplikacji **A.14 Pozyskiwanie, rozwój i utrzymywanie systemów** — A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia		Matryce związane z kontrolą dostępu (np. matryca kontroli rozdziału obowiązków, kontrola zdalnego dostępu itp.). Sekcja dotycząca praw dostępu zawarta w polityce/procedurach kontroli dostępu. Polityka kontroli dostępu obejmuje rejestr przyporządkowywania praw dostępu do odpowiednich zasobów lub procesów. Dostosowane i udokumentowane konta administracyjne z konkretnymi prawami dostępu przyznanymi odpowiedniemu personelowi. Udokumentowane zarządzanie procesem kont administratora. Dostępne dzienniki aktywności konta administratora. Administracyjne systemy informacyjne wyodrębnione i oddzielone od reszty infrastruktury w celu zwiększenia odporności. Formalnie udokumentowane wymogi dotyczące oprogramowania do celów zapewniania kompatybilności.
Bezpieczeństwo komunikacji	**A.10 Kryptografia** — A.10.1 Zabezpieczenia kryptograficzne **A.13 Bezpieczeństwo komunikacji** — –A.13.1 Zarządzanie bezpieczeństwem sieci — A.13.2 Przesyłanie informacji	Uwagi do pkt A.13: Wymiana danych między repozytoriami pierwotnymi a repozytorium wtórnym i routerem musi odbywać się zgodnie ze specyfikacjami technicznymi określonymi przez dostawcę repozytorium wtórnego (art. 28 ust. 1 rozporządzenia wykonawczego (UE) 2018/574) Wymiana wszelkich informacji drogą elektroniczną musi być prowadzona przy użyciu bezpiecznych środków. Mające zastosowanie protokoły bezpieczeństwa i zasady dotyczące łączności muszą być oparte na niezastrzeżonych i otwartych standardach (art. 36 ust. 1 rozporządzenia wykonawczego (UE) 2018/574)	Istnieją odpowiednie procesy kryptograficzne. Istnieją zabezpieczenia chroniące poufność (prywatnego) klucza lub kluczy. Wprowadzona i utrzymywana polityka lub procedura konfiguracji systemu. Tabele konfiguracji systemu. Harmonogram i plan cykli przeglądu konfiguracji systemu. Udokumentowane wcześniejsze ćwiczenia/testy krytycznych systemów informacyjnych. Harmonogram i plan przeglądów konfiguracji bezpieczeństwa.

Dziedzina	Punkty kontrolne ([1])	Wytyczne regulacyjne	Wytyczne dotyczące dowodów
			Dokumentacja dotycząca wdrażania rozdziału sieci i systemu oraz danych. Sprawozdania z monitorowania krytycznych sieci i systemów informacyjnych. Udokumentowana polityka w zakresie procedur monitorowania, w tym minimalne wymogi w zakresie monitorowania. Dowód istnienia narzędzi systemów monitorowania.
Ciągłość działania	**A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji** — A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami **A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania** — A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania — A.17.1 Ciągłość bezpieczeństwa informacji — A.17.2 Nadmiarowość **A.18 Zgodność** — A.18.1 Zgodność z wymaganiami prawnymi i umownymi	Uwagi do pkt A.17: Wszystkie składniki i usługi repozytorium muszą spełniać wymóg miesięcznego nieprzerwanego czasu działania na poziomie co najmniej 99,5 % (art. 25 ust. 1 lit. i) rozporządzenia wykonawczego (UE) 2018/574) Możliwość przenoszenia danych musi być zabezpieczona zgodnie z mającym zastosowanie słownikiem wspólnych danych (art. 36 ust. 2 rozporządzenia wykonawczego (UE) 2018/574) Dostawca musi posiadać mający zastosowanie plan wyjścia. (art. 19 rozporządzenia delegowanego (UE) 2018/573) Uwagi do pkt A.18.1: Przetwarzanie danych musi odbywać się zgodnie z rozporządzeniem (UE) 2016/679 (ogólne rozporządzenie o ochronie danych) oraz być zgodne z umową o przetwarzanie danych zawartą między dostawcą repozytorium pierwotnego a dostawcą repozytorium wtórnego.	Formalnie udokumentowana strategia zapewniająca ciągłość usług, w tym zakładany czas wznowienia kluczowych usług i procesów. Plany awaryjne dla systemów krytycznych, w tym jasne kroki i procedury dotyczące wspólnych zagrożeń, czynników wyzwalających aktywację, etapów i zakładanego czasu wznowienia funkcji. Zapisy dotyczące poszczególnych działań szkoleniowych oraz sprawozdania z okresu po ćwiczeniu. Środki mające na celu radzenie sobie z klęskami żywiołowymi (np. trzęsienie ziemi, powódź, pożar), np. miejsca w innych regionach przejmujące działalność w przypadku awarii, kopie zapasowe danych krytycznych, które muszą być wykonane w odległej lokalizacji (geograficznie różniącej się od ośrodka dokonującego gromadzenia i przetwarzania danych), w wystarczającej odległości, aby uniknąć wszelkich szkód spowodowanych klęską żywiołową w głównej siedzibie itp. Formalnie udokumentowane procedury/polityka wdrażania zdolności w zakresie przywracania gotowości do pracy po klęsce żywiołowej, w tym wykaz katastrof naturalnych lub poważnych klęsk żywiołowych, które mogą mieć wpływ na usługi, oraz wykaz zdolności w zakresie przywracania gotowości do pracy po klęsce żywiołowej (dostępnych wewnętrznie lub zapewnionych przez osoby trzecie). Rejestr poszczególnych działań szkoleniowych dla personelu biorącego udział w operacjach przywracania gotowości do pracy po wystąpieniu klęski żywiołowej.

Dziedzina	Punkty kontrolne ([1])	Wytyczne regulacyjne	Wytyczne dotyczące dowodów
Aktywa i integralność danych	**A.8 Zarządzanie aktywami** — A.8.1 Odpowiedzialność za aktywa — A.8.2 Klasyfikacja informacji — A.8.3 Postępowanie z nośnikami	Uwagi do pkt A.8.1: Uwzględnienie aktywów związanych z bazami danych i repozytoriami (tj. system zarządzania bazami danych, obiekty bazy danych, serwer bazy danych) Uwagi do pkt A.8.2: Wysoka wrażliwość. Dane zawierają szczególnie chronione informacje handlowe. Dane są wykorzystywane do dochodzeń prowadzonych przez organy krajowe i unijne	Udokumentowane procedury/polityka zarządzania aktywami, w tym role, obowiązki, aktywa i konfiguracje, które są przedmiotem polityki. Wykaz aktywów krytycznych zarządzanych centralnie oraz zarządzanych i utrzymywanych konfiguracji krytycznych systemów. Formalnie udokumentowane i utrzymywane zarządzanie aktywami w zakresie oprogramowania/sprzętu komputerowego. Aktualne procedury/polityka zarządzania aktywami, uwagi do przeglądu lub dzienniki zmian.

([1]) Numeracja punktów kontrolnych odpowiada numeracji w normie ISO/IEC 27001:2013. W przypadku rozbieżności należy odnieść się do numeracji użytej w niniejszym dokumencie.
([2]) Strona trzecia jest niezależnym podmiotem zaangażowanym w funkcjonowanie usługi, ale nie jest podmiotem głównym i ma mniejsze znaczenie dla świadczenia usług (np. w segmencie wyższego szczebla (dostawca, sprzedawca) lub niższego szczebla (dystrybutor, odsprzedawca).