**PYTANIA DO LISTY KONTROLNEJ**

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Czy organizacja powołała i zgłosiła inspektora ochrony danych (IOD) do Prezesa Urzędu Ochrony Danych Osobowych?
3. Czy nośniki, które nie będą dłużej wykorzystywane są bezpiecznie wycofywane, zgodnie z formalnymi procedurami?
4. Czy nośniki zawierające informacje są chronione przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu?
5. Czy użytkownicy mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali ważne uprawnienia?
6. Czy organizacja wdrożyła formalny proces rejestrowania i wyrejestrowywania użytkowników w systemach informatycznych?
7. Czy przydzielanie i wykorzystanie praw uprzywilejowanego dostępu do systemów informatycznych zostało ograniczone i jest nadzorowane?
8. Czy przydzielanie poufnych informacji uwierzytelniających w systemach informatycznych podlega formalnemu procesowi zarządzania?
9. Czy właściciele aktywów przeglądają prawa dostępu użytkowników w regularnych odstępach czasu?
10. Czy przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji są odbierane po zakończeniu zatrudnienia, umowy, lub porozumienia?
11. Czy użytkownicy mają obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających w systemach informatycznych?
12. Czy dostęp do informacji oraz funkcji systemu aplikacyjnego został ograniczony zgodnie z polityką kontroli dostępu?
13. Czy tam gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji jest kontrolowany przez procedurę bezpiecznego logowania?
14. Czy systemy zarządzania hasłami są interaktywne i zapewniają wybór haseł jakości adekwatnej do istniejących zagrożeń?
15. Czy wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, podlega ograniczeniom i ścisłemu nadzorowi?
16. Czy dostęp do kodu źródłowego programów został ograniczony?
17. Czy opracowano i wdrożono politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji?
18. Czy opracowano politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożono ją na wszystkich etapach cyklu życia kluczy?
19. Czy określono granice bezpieczeństwa i wykorzystuje się je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji?
20. Czy bezpieczne strefy są chronione odpowiednimi zabezpieczeniami zapewniającymi dostęp wyłącznie osobom uprawnionym?
21. Czy zaprojektowano i zastosowano zabezpieczenia fizyczne biur, pomieszczeń i obiektów?
22. Czy zaprojektowano i zastosowano fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami?
23. Czy zaprojektowano i zastosowano procedury pracy w obszarach bezpiecznych?
24. Czy organizacja sprawuje nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń?
25. Czy sprzęt służący do przetwarzania informacji jest prawidłowo konserwowany w celu zapewnienia jego ciągłej dostępności i integralności?
26. Czy informacje wynoszone poza siedzibę organizacji zostały zabezpieczone przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą organizacji?
27. Czy przed zbyciem lub przekazaniem sprzętu do ponownego użycia sprawdza się wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane?
28. Czy użytkownicy zapewniają odpowiednią ochronę sprzętu pozostawianego bez opieki?
29. Czy zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, są nadzorowane?
30. Czy działania administratorów i operatorów systemów są rejestrowane, a dzienniki zdarzeń chronione i systematycznie przeglądane?
31. Czy informacje przekazywane w formie wiadomości elektronicznych są odpowiednio chronione?
32. Czy informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje są chronione, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu?
33. Czy organizacja regularnie monitoruje, przegląda i audytuje dostarczanie usług zewnętrznych?
34. Czy organizacja ustanowiła odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowana reakcję na incydenty związane z bezpieczeństwem informacji?
35. Czy zdarzenia związane z bezpieczeństwem informacji są zgłaszane odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe?
36. Czy wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania zostały zidentyfikowane, udokumentowane i są aktualizowane dla każdego systemu informacyjnego oraz całości organizacji?
37. Czy wdrożono odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania?
38. Czy organizacja zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?
39. Czy organizacja oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych?
40. Czy organizacja po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych zależnie od decyzji podmiotu, który dane powierzył usunie lub zwróci mu wszelkie dane osobowe oraz usunie wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują jej przechowywanie danych osobowych?
41. Czy organizacja jeżeli do wykonania w imieniu podmiotu, który jej powierzył dane osobowe, konkretnych czynności przetwarzania korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożyła te same obowiązki ochrony danych jak w relacji z podmiotem, który jej powierzył dane osobowe?