ISO/IEC 27018:2025, Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności: Wytyczne dotyczące ochrony informacji umożliwiających identyfikację osoby (PII) w chmurach publicznych działających jako podmioty przetwarzające PII (wydanie 3, 2025-08)

Ochrona PII w chmurze publicznej

36 wymagań. Dla tej normy nie istnieje akredytowany certyfikat. Stan na 07/2026.

ISO/IEC 27018 nie jest normą systemu zarządzania, lecz zbiorem wytycznych z rozszerzonymi zabezpieczeniami opartymi na ISO/IEC 27002:2022. Nie istnieje samodzielny akredytowany certyfikat dla ISO/IEC 27018. Zabezpieczenia te są ujmowane w Deklaracji Stosowania systemu ISO/IEC 27001, a certyfikat jest wówczas wystawiany na zgodność z ISO/IEC 27001 z odniesieniem do ISO/IEC 27018. Norma dotyczy dostawcy publicznej usługi w chmurze, który przetwarza informacje umożliwiające identyfikację osoby w imieniu swoich klientów usługi w chmurze. Organizacja, która jedynie korzysta z usług w chmurze, nie pełni tej roli i powinna rozsądnie oceniać wymagania w odniesieniu do swoich dostawców, a nie do samej siebie. Dla Leanshift ta lista kontrolna stanowi zatem przede wszystkim macierz oceny dostawców. Każdy punkt można przedstawić dostawcy jako pytanie i zabezpieczyć poprzez umowę powierzenia przetwarzania danych na podstawie art. 28 RODO. Wynikiem takiej oceny jest wewnętrzny rejestr zgodności lub profil oceny dostawcy, a nie certyfikat. Co do numeracji: punkty od A.2 do A.12 odpowiadają zasadom ochrony prywatności z Załącznika A normy, pozycje numerowane jak A.11.6 to wymienione tam dodatkowe zabezpieczenia. Pozycje numerowane jak 8.10 czy 5.34 odnoszą się do zabezpieczeń z ISO/IEC 27002:2022, które norma doprecyzowuje dla chmury. Pozycje z przyrostkiem (Grundsatz), co oznacza zasada, wynikają z samej zasady danego punktu, w przypadkach gdy Załącznik A nie zawiera dla niej dedykowanego dodatkowego zabezpieczenia.

Firma	Data	Opracował

A.2 Zgoda i możliwość wyboru 2

A.2.1 **Dostawca usługi w chmurze wspiera klienta usługi w chmurze w realizacji praw osób, których dane dotyczą, takich jak prawo dostępu, sprostowania, usunięcia i sprzeciwu. Odpowiedzialności i terminy są ustalone w umowie.** Dokument

Jak to wykazać: Dowodem jest umowa powierzenia przetwarzania danych na podstawie art. 28 RODO zawierająca klauzulę dotyczącą wsparcia w realizacji praw osób, których dane dotyczą, wraz ze środkami technicznymi wbudowanymi w sam serwis: funkcjami eksportu, korekty i usuwania danych, lub udokumentowaną procedurą wsparcia z określonym terminem odpowiedzi. Pytanie do dostawcy: jaką funkcję lub proces oferujecie, abyśmy mogli zrealizować żądanie dostępu lub usunięcia danych w ciągu jednego miesiąca?

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

A.2 (Grundsatz) **Informacje umożliwiające identyfikację osoby należące do klientów usługi w chmurze są przetwarzane wyłącznie na udokumentowane polecenie klienta. Uzyskiwanie zgody osób, których dane dotyczą, pozostaje zadaniem klienta jako administratora danych, a dostawca nie wyręcza go w tym zakresie.**

Jak to wykazać: Dowodem jest klauzula dotycząca poleceń w umowie powierzenia przetwarzania danych oraz potwierdzenie, że dostawca nie wykorzystuje danych wtórnie, na przykład polityka prywatności usługi i dokumentacja produktu. Pytanie do dostawcy: czy przetwarzacie dane naszych klientów w jakikolwiek sposób wykraczający poza nasze polecenia, na przykład do celów rozwoju produktu lub trenowania modeli?

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

A.3 Zgodność z prawem i określenie celu 2

A.3.1 **Cel, dla którego dostawca przetwarza informacje umożliwiające identyfikację osoby, jest ograniczony do świadczenia uzgodnionej usługi i jest określony w umowie. Nie dochodzi do przetwarzania na własne cele dostawcy.** Dokument

Jak to wykazać: Dowodem jest umowa powierzenia przetwarzania danych określająca przedmiot, charakter, cel i czas trwania przetwarzania, a także kategorie osób, których dane dotyczą, zgodnie z art. 28 ust. 3 RODO. Pytanie do dostawcy: proszę o załącznik umowny, który wyczerpująco opisuje cel przetwarzania. Dla małych organizacji wystarczy standardowy aneks dostawcy dotyczący przetwarzania danych, o ile zawiera te informacje.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

A.3.2 **Informacje umożliwiające identyfikację osoby powierzone dostawcy nie są wykorzystywane do reklamy, marketingu ani innych własnych celów komercyjnych dostawcy bez uprzedniej wyraźnej zgody. Świadczenie usługi nie jest uzależnione od takiej zgody.**

Jak to wykazać: Dowodem jest wyraźna klauzula umowna wykluczająca komercyjne wykorzystanie wtórne, wraz z regulaminem usługi. Pytanie do dostawcy: proszę pisemnie potwierdzić, że dane klientów nie są wykorzystywane do reklamy, profilowania ani trenowania modeli AI. Jeśli takiego zobowiązania brakuje, usługa nie nadaje się do przetwarzania informacji umożliwiających identyfikację osoby.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.4 Ograniczenie zbierania danych 1

A.4 (Grundsatz) **Poza danymi, które klient wprowadza do usługi, dostawca nie zbiera dodatkowych informacji umożliwiających identyfikację osoby na własne cele, takich jak telemetria, profile użytkowania czy analiza treści. Zbierane dane operacyjne i metadane są nazwane i uzasadnione.**

Jak to wykazać: Dowodem jest lista danych rejestrowanych przez usługę obok danych treściowych (dzienniki dostępu, telemetria, dane diagnostyczne) wraz z celem i okresem przechowywania, a także zrzut ekranu ustawienia wyłączającego opcjonalną telemetrię. Pytanie do dostawcy: jakie dodatkowe dane użytkowania, telemetrii i diagnostyczne zbieracie, do czego je wykorzystujecie i czy możemy wyłączyć to zbieranie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.5 Minimalizacja danych 2

A.5.1 **Pliki tymczasowe powstające podczas przetwarzania informacji umożliwiających identyfikację osoby, takie jak pamięć robocza, pamięci podręczne czy dzienniki wycofywania zmian, są bezpiecznie usuwane w określonym terminie.**

Jak to wykazać: Dowodem jest procedura operacyjna lub procedura usuwania z określonym okresem przechowywania danych tymczasowych, potwierdzona konfiguracją systemu, na przykład wartością TTL pamięci podręcznej lub zaplanowanym zadaniem porządkującym wraz z dziennikiem jego wykonania. Pytanie do dostawcy: po jakim czasie usuwane są pamięci podręczne, pliki tymczasowe i stany pośrednie, i w jaki sposób jest to monitorowane?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

8.11 **Wszędzie tam, gdzie operacje, testy lub wsparcie nie wymagają danych rzeczywistych, informacje umożliwiające identyfikację osoby są maskowane, pseudonimizowane lub anonimizowane. Ilość przetwarzanych danych pozostaje ograniczona do tego, co jest faktycznie potrzebne usłudze.**

Jak to wykazać: Dowodem jest ustalenie, które środowiska mogą mieć dostęp do danych rzeczywistych, wraz ze zrzutami ekranu lub skryptami maskowania stosowanego w systemach testowych i deweloperskich. Pytanie do dostawcy: czy wasze zespoły wsparcia i deweloperskie pracują na danych produkcyjnych, a jeśli tak, to pod jakimi zabezpieczeniami? Dla małych organizacji wystarczy zasada, że systemy testowe działają wyłącznie na wygenerowanych danych przykładowych.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.6 Ograniczenie wykorzystania, przechowywania i ujawniania 3

A.6.1 **Jeżeli dostawca otrzyma prawnie wiążące żądanie ujawnienia informacji umożliwiających identyfikację osoby, na przykład od organu publicznego, informuje o tym z wyprzedzeniem klienta usługi w chmurze, o ile prawo na to pozwala.**

Jak to wykazać: Dowodem jest klauzula umowna dotycząca powiadamiania oraz wewnętrzny proces obsługi żądań organów z wyznaczonym właścicielem. Pytanie do dostawcy: czy powiadamiacie nas przed przekazaniem danych i czy publikujecie raport przejrzystości dotyczący żądań organów? Aktualny raport przejrzystości stanowi mocny dowód.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.6.2 **Jeżeli dostawca ujawnia informacje umożliwiające identyfikację osoby stronom trzecim, rejestruje to zdarzenie w sposób umożliwiający jego prześledzenie: kto otrzymał dane, kiedy to nastąpiło, jakich danych dotyczyło i na jakiej podstawie oparte było ujawnienie.** Dokument

Jak to wykazać: Dowodem jest rejestr ujawnień lub historia zgłoszeń zawierająca te pola, nawet jeśli nie ma jeszcze żadnych wpisów. Pusty, ale prowadzony rejestr jest akceptowalny i stanowi praktyczne rozwiązanie dla małych organizacji. Pytanie do dostawcy: czy prowadzicie rejestr ujawnień danych i czy możemy otrzymać z niego wyciągi?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

8.10 **Informacje umożliwiające identyfikację osoby są usuwane po upływie uzgodnionego okresu przechowywania lub po zakończeniu umowy, w tym kopie przechowywane w kopiach zapasowych, po zakończeniu ich cyklu rotacji.**

Jak to wykazać: Dowodem jest koncepcja usuwania danych z okresami przechowywania dla poszczególnych kategorii danych, okresem przechowywania kopii zapasowych oraz dziennikiem usuwania lub potwierdzeniem usunięcia. Pytanie do dostawcy: jak długo nasze dane pozostają w waszych kopiach zapasowych po zakończeniu umowy i czy otrzymujemy pisemne potwierdzenie ich usunięcia?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.7 Dokładność i jakość 2

A.7 (Grundsätzlich) **Dostawca nie zmienia z własnej inicjatywy powierzonych mu informacji umożliwiających identyfikację osoby. Korekty i aktualizacje są dokonywane wyłącznie na polecenie klienta usługi w chmurze lub za pomocą funkcji obsługiwanych bezpośrednio przez klienta.**

Jak to wykazać: Dowodem są funkcje edycji dostępne w usłudze wraz z historią zmian oraz klauzula dotycząca poleceń w umowie powierzenia przetwarzania danych. Pytanie do dostawcy: czy możemy sami korygować rekordy i czy każda zmiana jest rejestrowana w sposób umożliwiający jej prześledzenie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

8.13 **Integralność informacji umożliwiających identyfikację osoby jest chroniona podczas przechowywania, transmisji i odtwarzania. Istnieją kopie zapasowe, a ich zdolność do odtworzenia została przetestowana.**

Jak to wykazać: Dowodem jest konfiguracja kopii zapasowych, mechanizmy sum kontrolnych lub integralności oraz co najmniej jeden udokumentowany test odtworzenia rocznie z datą i wynikiem. Pytanie do dostawcy: jak często testujecie odtwarzanie danych i jaki czas odzyskiwania gwarantujecie w ramach poziomu usługi?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.8 Otwartość, przejrzystość i informowanie 2

A.8.1 **Korzystanie z podwykonawców przetwarzających informacje umożliwiające identyfikację osoby jest ujawniane przed zawarciem umowy. Zmiany na liście podwykonawców są zgłaszane klientowi z odpowiednim wyprzedzeniem, tak aby mógł zgłosić sprzeciw lub wypowiedzieć umowę.** Dokument

Jak to wykazać: Dowodem jest aktualna lista podwykonawców, opublikowana lub udostępniona umownie, zawierająca nazwę, kraj i cel przetwarzania, wraz z zasadą powiadamiania zgodną z art. 28 ust. 2 RODO. Pytanie do dostawcy: gdzie znajdziemy waszą listę podwykonawców, z jakim wyprzedzeniem informujecie o zmianach i w jaki sposób możemy zgłosić sprzeciw?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.8 (Grundsätze) **Przed zawarciem umowy dostawca udostępnia zrozumiałe informacje o tym, w jaki sposób przetwarzane są informacje umożliwiające identyfikację osoby, jakie zabezpieczenia są stosowane i w jakich jurysdykcjach odbywa się przetwarzanie.**

Jak to wykazać: Dowodem jest polityka prywatności, dokument techniczny dotyczący bezpieczeństwa, strona centrum zaufania oraz umowa powierzenia przetwarzania danych zawierająca środki techniczne i organizacyjne jako załącznik. Pytanie do dostawcy: proszę o aktualną listę środków technicznych i organizacyjnych jako załącznik umowny, a nie jedynie materiał marketingowy.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.9 Udział osoby fizycznej i dostęp do danych 2

A.9 (Grundsätze) **Usługa zapewnia klientowi usługi w chmurze środki techniczne umożliwiające samodzielną realizację żądań dostępu, sprostowania i usunięcia zgłaszanych przez osoby, których dane dotyczą, na przykład za pomocą funkcji eksportu, wyszukiwania i usuwania.**

Jak to wykazać: Dowodem jest dokumentacja produktu opisująca funkcje eksportu i usuwania, potwierdzona wewnętrznym testem: przeprowadzenie jednego żądania dostępu od początku do końca z odnotowaniem czasu realizacji. Pytanie do dostawcy: czy możemy samodzielnie, bez waszego wsparcia, odnaleźć, wyeksportować i usunąć wszystkie dane dotyczące jednej osoby?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

5.34 **Jeżeli klient nie jest w stanie samodzielnie zrealizować żądania osoby, której dane dotyczą, dostawca udziela wsparcia w uzgodnionym terminie. Żądania kierowane przez osoby, których dane dotyczą, bezpośrednio do dostawcy, są przekazywane klientowi, a nie odpowiadane samodzielnie przez dostawcę.**

Jak to wykazać: Dowodem jest odpowiednia klauzula w umowie powierzenia przetwarzania danych z konkretnym terminem odpowiedzi oraz historia zgłoszeń wsparcia jako rzeczywisty przykład. Pytanie do dostawcy: jaki termin gwarantujecie na wsparcie w realizacji praw osób, których dane dotyczą, i ile to kosztuje?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.10 Rozliczalność 4

A.10.1 **Naruszenia dotyczące informacji umożliwiających identyfikację osoby są zgłaszane klientowi usługi w chmurze bez zbędnej zwłoki, z podaniem zakresu, danych, których dotyczyły, przyczyny oraz podjętych działań. Zdefiniowany jest proces powiadamiania z przypisanymi odpowiedzialnościami i terminami.** Dokument

Jak to wykazać: Dowodem jest plan reagowania na incydenty wraz z łańcuchem eskalacji, umowny termin powiadamiania (w praktyce sprawdza się od 24 do 48 godzin, tak aby klient mógł dotrzymać terminu 72 godzin zgodnie z art. 33 RODO) oraz zapisy dotyczące wcześniejszych incydentów lub przeprowadzonego ćwiczenia. Pytanie do dostawcy: w jakim terminie zgłaszacie incydent, jakim kanałem i jakie informacje przekazujecie wraz ze zgłoszeniem?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.10.2 **Polityki bezpieczeństwa, procedury operacyjne oraz związane z nimi zapisy są przechowywane przez określony czas, tak aby przetwarzanie można było odtworzyć po fakcie.** Dokument

Jak to wykazać: Dowodem jest zasada przechowywania wraz z historią wersji polityk, na przykład za pomocą rejestru dokumentów lub systemu kontroli wersji z datą zatwierdzenia. Pytanie do dostawcy: jak długo przechowujecie wersje polityk i związane z nimi zapisy oraz czy uzyskamy do nich dostęp w przypadku audytu?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.10.3 **Istnieje określona procedura zwrotu, przekazania i zniszczenia informacji umożliwiających identyfikację osoby po zakończeniu umowy, wskazująca formaty, terminy oraz sposób postępowania z kopiami.** Dokument

Jak to wykazać: Dowodem jest klauzula wyjścia w umowie powierzenia przetwarzania danych oraz potwierdzenie usunięcia danych po zakończeniu umowy. Pytanie do dostawcy: w jakim formacie i w jakim terminie otrzymamy z powrotem nasze dane, kiedy zniszczone zostaną wszystkie kopie i czy otrzymamy pisemne potwierdzenie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

5.35 **Skuteczność zabezpieczeń jest niezależnie weryfikowana w regularnych odstępach czasu, na przykład za pomocą audytów wewnętrznych, testów penetracyjnych lub raportów zapewniających stron trzecich. Wyniki są udostępniane klientowi usługi w chmurze w odpowiedniej formie.**

Jak to wykazać: Dowodem jest certyfikat ISO/IEC 27001 wraz z Deklaracją Stosowania obejmującą zabezpieczenia ISO/IEC 27018, lub raport SOC 2, wraz z aktualnymi podsumowaniami testów penetracyjnych. Pytanie do dostawcy: proszę o certyfikat, jego zakres oraz potwierdzenie, że ISO/IEC 27018 jest odzwierciedlone w Deklaracji Stosowania. Należy sprawdzić, czy zakres rzeczywiście obejmuje wykorzystywaną usługę.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11 Bezpieczeństwo informacji 13

A.11.1 **Każda osoba mająca dostęp do informacji umożliwiających identyfikację osoby jest zobowiązana do zachowania poufności, niezależnie od tego, czy jest zatrudniona bezpośrednio, czy współpracuje zewnętrznie.** Dokument

Jak to wykazać: Dowodem są podpisane umowy lub zobowiązania o zachowaniu poufności, które pozostają w mocy po zakończeniu współpracy. Pytanie do dostawcy: czy wszyscy pracownicy i podwykonawcy usług mający dostęp do danych są pisemnie zobowiązani do zachowania poufności?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.2 **Wydruki i inne papierowe kopie zawierające informacje umożliwiające identyfikację osoby są tworzone wyłącznie w przypadku bezwzględnej konieczności. Dopuszczalny zakres reguluje odpowiednia zasada.**

Jak to wykazać: Dowodem jest zasada dotycząca postępowania z wydrukami, która w centrach danych zazwyczaj oznacza całkowity zakaz drukowania w obszarach przechowujących dane klientów. Pytanie do dostawcy: czy w waszej działalności w ogóle drukowane są dane klientów, a jeśli tak, to na jakich warunkach?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.3 **Odtwarzanie danych z kopii zapasowych jest wcześniej autoryzowane i rejestrowane, wraz z informacją o osobie, która zainicjowała odtworzenie, i danych, których to dotyczyło.** Dokument

Jak to wykazać: Dowodem jest dziennik odtwarzania zawierający znacznik czasu, inicjatora i zakres, generowany zazwyczaj automatycznie przez narzędzie do tworzenia kopii zapasowych. Pytanie do dostawcy: czy rejestrujecie każde odtworzenie danych i czy możemy wglądać w te dzienniki w przypadku audytu?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.4 **Nośniki danych zawierające informacje umożliwiające identyfikację osoby, które opuszczają siedzibę, są chronione przed nieuprawnionym dostępem i utratą, z reguły za pomocą szyfrowania i rejestru transportu.**

Jak to wykazać: Dowodem jest potwierdzenie szyfrowania (pełne szyfrowanie nośnika), zapisy transportu i przekazania oraz inwentarz nośników. Pytanie do dostawcy: czy nośniki z danymi klientów kiedykolwiek opuszczają wasze lokalizacje, na przykład na potrzeby kopii zapasowych, i w jaki sposób są chronione podczas transportu?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.5 **Wykorzystywanie niezaszyfrowanych nośników i urządzeń przenośnych do informacji umożliwiających identyfikację osoby jest zabronione lub ograniczone do uzasadnionych wyjątków z udokumentowaną zgodą.**

Jak to wykazać: Dowodem jest polityka dotycząca nośników wymiennych wraz z jej technicznym wymuszeniem, na przykład obowiązkowym szyfrowaniem urządzeń lub zablokowanymi portami USB za pomocą zarządzania urządzeniami. Pytanie do dostawcy: czy pracownicy mogą kopiować dane klientów na niezaszyfrowane urządzenia i co temu technicznie zapobiega?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.6 **Informacje umożliwiające identyfikację osoby przesyłane przez sieci publiczne są szyfrowane. Stosowane mechanizmy odpowiadają aktualnemu stanowi techniki.**

Jak to wykazać: Dowodem jest konfiguracja TLS (aktualna wersja protokołu, brak przestarzałych szyfrów) oraz raport z zewnętrznego testu konfiguracji. Praktyczne rozwiązanie dla małych organizacji: przeprowadzenie raz w roku bezpłatnego skanu TLS i archiwizacja wyniku. Pytanie do dostawcy: jakie szyfrowanie transmisji stosujecie obowiązkowo i czy aktywne jest szyfrowanie danych w spoczynku?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.7 **Dokumenty papierowe zawierające informacje umożliwiające identyfikację osoby są niszczone w sposób wykluczający ich odtworzenie.**

Jak to wykazać: Dowodem są niszczarki o odpowiednim poziomie bezpieczeństwa lub certyfikaty zniszczenia od dostawcy usług działającego zgodnie z normą DIN 66399 lub normą równoważną. Pytanie do dostawcy: w jaki sposób niszczycie dokumenty papierowe dotyczące klientów i czy przechowujecie certyfikaty zniszczenia?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.8 **Identyfikatory użytkowników są przypisywane wyłącznie jednej osobie i nie są ponownie wydawane ani współdzielone. Konta współdzielone istnieją wyłącznie w uzasadnionych wyjątkach i z dodatkową możliwością śledzenia.**

Jak to wykazać: Dowodem jest lista użytkowników z systemu tożsamości wolna od kont grupowych, wraz z zasadą, że prace administracyjne są wykonywane z konta osobistego. Pytanie do dostawcy: czy wasz personel operacyjny pracuje na kontach osobistych i czy uwierzytelnianie wieloskładnikowe jest obowiązkowe?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.9 **Dostawca jest w stanie w każdej chwili wskazać, które osoby lub role mają uprawnienia dostępu do informacji umożliwiających identyfikację osoby, i utrzymuje ten wykaz na bieżąco.** Dokument

Jak to wykazać: Dowodem jest zestawienie uprawnień dostępu według ról, potwierdzone cyklicznym przeglądem dostępu z datą i wynikiem. Dla małych organizacji wystarczy półroczny, zatwierdzony eksport listy użytkowników. Pytanie do dostawcy: ilu waszych pracowników ma dostęp do naszych danych i jak często to weryfikujecie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.10 **Konta użytkowników są zarządzane przez cały cykl ich życia: tworzenie, modyfikację oraz niezwłoczną dezaktywację w przypadku odejścia lub zmiany roli danej osoby.**

Jak to wykazać: Dowodem jest procedura nadawania i odbierania uprawnień z listą kontrolną, wraz z dziennikami dezaktywowanych kont ze znacznikami czasu. Pytanie do dostawcy: w jakim terminie odbieracie dostęp pracownikom, którzy odchodzą, i jak to dokumentujecie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.11 **Zobowiązania dostawcy w zakresie bezpieczeństwa i prywatności są ustalone w umowie, w tym środki techniczne i organizacyjne, wiążący charakter poleceń klienta oraz prawo klienta do audytu.** Dokument

Jak to wykazać: Dowodem jest podpisana umowa powierzenia przetwarzania danych na podstawie art. 28 RODO wraz z załącznikiem dotyczącym środków oraz prawem do audytu lub informacji. Pytanie do dostawcy: proszę o podpisaną umowę powierzenia przetwarzania danych wraz z załącznikami, a nie jedynie odesłanie do ogólnych warunków świadczenia usług.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.12 **Podwykonawcy przetwarzający informacje umożliwiające identyfikację osoby podlegają co najmniej takim samym zobowiązaniom jak sam dostawca. Ich wybór i bieżący nadzór regulowane są przez określony proces.**

Jak to wykazać: Dowodem jest przeniesienie zobowiązań do umów z podwykonawcami (art. 28 ust. 4 RODO) oraz datowana ocena dostawców. Pytanie do dostawcy: w jaki sposób oceniacie swoich podwykonawców i jakich dowodów od nich wymagacie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.11.13 **Przed ponownym wykorzystaniem przestrzeni dyskowej zapewnia się, że żadne dane wcześniejszych użytkowników nie pozostają dostępne, ani na nośnikach fizycznych, ani w środowiskach zwirtualizowanych.**

Jak to wykazać: Dowodem jest procedura czyszczenia lub nadpisywania stosowana przy zwalnianiu przestrzeni dyskowej, zapisy dotyczące niszczenia nośników oraz opis rozdzielenia najemców zawarty w dokumencie architektury. Pytanie do dostawcy: w jaki sposób zapewniacie, że ponownie wykorzystywana przestrzeń dyskowa nie zawiera pozostałości danych innych klientów?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.12 Zgodność w zakresie ochrony prywatności 3

A.12.1 **Kraje, w których informacje umożliwiające identyfikację osoby są przechowywane i przetwarzane, są wskazane i znane klientowi usługi w chmurze. Zmiany lokalizacji przechowywania są zgłaszane.** Dokument

Jak to wykazać: Dowodem jest zestawienie lokalizacji i regionów dostawcy, zawarte w umowie lub w dokumentacji, wraz ze zrzutem ekranu ustawienia regionu w wykorzystywanej usłudze. Pytanie do dostawcy: w jakich krajach spoczywają nasze dane, z jakich krajów uzyskuje się do nich dostęp, na przykład w ramach wsparcia, i czy możemy przypisać na stałe konkretny region?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

A.12.2 **Transfery informacji umożliwiających identyfikację osoby do państw trzecich są znane, uzasadnione i objęte odpowiednimi zabezpieczeniami.** Dokument

Jak to wykazać: Dowodem są standardowe klauzule umowne lub decyzja stwierdzająca odpowiedni poziom ochrony, potwierdzone oceną skutków transferu danych, która dla małych organizacji może być krótka: dotknięte kategorie danych, kraj docelowy, ryzyko, zastosowane środki dodatkowe. Pytanie do dostawcy: na jakiej podstawie prawnej przekazujecie dane do państw trzecich i jakie środki dodatkowe stosujecie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

5.31 **Wymagania prawne i umowne mające zastosowanie do przetwarzania informacji umożliwiających identyfikację osoby są zidentyfikowane i utrzymywane na bieżąco wraz ze zmianami sytuacji prawnej. Oceniane są sprzeczności między jurysdykcjami.**

Jak to wykazać: Dowodem jest zestawienie obowiązujących wymagań (RODO, przepisy krajowe, obowiązki branżowe) z wyznaczonym właścicielem i datą przeglądu. W małej organizacji wystarczy jednostronicowa lista przeglądana raz w roku. Pytanie do dostawcy: czy wy lub wasi podwykonawcy podlegacie jurysdykcjom umożliwiającym organom dostęp do naszych danych, i jak sobie z tym radzicie?

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

Wymagania zostały sformułowane samodzielnie i nie zastępują tekstu normy. Wiążąca jest wyłącznie oryginalna norma danego wydawcy. Niniejsza lista jest narzędziem pracy, nie stanowi dowodu zgodności ani certyfikacji. Leanshift nie posiada certyfikatu w zakresie żadnej z tych norm, nie jest jednostką certyfikującą i nie jest powiązana z ISO, IEC, DIN, IATF, IAQG ani SAE. W razie wątpliwości rozstrzygająca jest niemiecka wersja tej listy.