ISO 27001:2013 - A.18.1.1 - Identyfikacja obowiązujących przepisów i wymagań kontraktowych

Norma ISO 27001 A.18.1.1 mówi:

"Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjnego oraz całości organizacji".

Jako Key Account Manager współpracujący z kilkoma organizacjami w zakresie Audytu Bezpieczeństwa Informacji i Audytu Prywatności Danych, mam do czynienia z pytaniami klientów dotyczącymi dostarczania jednoznacznych i obiektywnych dowodów spełnienia konkretnych wymagań.

Należy zauważyć, że wdrożenie i utrzymanie zabezpieczeń zapewniających zgodność nie jest łatwym zadaniem, ale niespełnienie tego warunku niesie ryzyko niezgodności nie tylko z normą ISO 27001:2013, ale także z wszelkimi istotnymi wymaganiami prawnymi, ustawowymi, wykonawczymi i kontraktowymi.

Audytorzy Bezpieczeństwa Informacji nie są doradcami prawnymi, adwokatami czy radcami prawnymi, ale odgrywają ważną rolę, sprawdzając dowody potwierdzające zgodność z przepisami.

Organizacje mogą rozważyć wykorzystanie następujących obiektywnych dowodów, celem przedstawienia audytorom jako dowodów zgodności:

- Udokumentowana lista wymagań związanych z konkretnym klientem, znajdujących się w umowach, w zakresie w jakim odnoszą się do bezpieczeństwa informacji / prywatności danych (także kopia obecnego kontraktu);
- Udokumentowany wykaz wszystkich obowiązujących przepisów i regulacji prawnych oraz innych wymogów w zakresie bezpieczeństwa informacji / prywatności danych, które organizacja powinna spełniać;
- E-maile, porządki obrad, protokoły z posiedzeń, notatki itd. zapisane przez Zespoły ds. zgodności z wymaganiami / legalności oraz inne podmioty zobowiązane do wypełniania obowiązków związanych z bezpieczeństwem informacji / zachowaniem prywatności danych (takie jak Dział Zakupów, Inspektor Ochrony Danych, HR, Finanse, IT, członkowie zarządu) w zakresie, w jakim odnoszą się do bezpieczeństwa informacji w kontekście celów zgodności - tj. dowód na to, że kierownictwo aktywnie uczestniczy w ocenie zakresu, w którym zgodność jest potrzebna, i ma świadomość ryzyka wystąpienia niezgodności;
- Udokumentowane Plany określające, że organizacja spełnia lub planuje spełnić wymagania (w tym określenie, kto jest odpowiedzialny za ich wdrożenie, a także kiedy zostaną spełnione);
- Sprawozdania z audytu wewnętrznego i zewnętrznego / oceny dotyczące obowiązujących zobowiązań dotyczących zgodności, w tym szczegółowe działania korygujące w przypadku stwierdzonych niezgodności;
- Lista działań z dowodami jej dystrybucji, przypisanymi właścicielami procesów (powinno być to także najwyższe kierownictwo) i aktualnym statusem;
- Opublikowana Polityka Zgodności wraz z normami, procedurami i wytycznymi;
- Szczegółowa ocena ryzyka związanego z ISMS (system zarządzania bezpieczeństwem informacji);

Audytorzy bezpieczeństwa informacji, którzy otrzymali tego rodzaju obiektywne dowody, mogą ustalić, czy organizacja spełnia obowiązujące wymagania, a także wskazać obszary, które mogą wymagać uwagi lub poprawy.

Informacje dodatkowe: Różnice między wymaganiami ustawowymi, regulacyjnymi i kontraktowymi

Wymagania ustawowe to wymagania stawiane przez prawo, odnoszące się do aktualnych przepisów, które zostały uchwalone przez organ ustawodawczy.

Wymagania regulacyjne są to obowiązkowe wymagania wyspecyfikowane przez organ, uprawniony przez organ ustawodawczy. Ważne jest, aby pamiętać, że wymagania regulacyjne zmieniają się częściej niż wymagania ustawowe.

Wymagania kontraktowe to obowiązki, za które każda ze stron jest prawnie odpowiedzialna, a które są zawarte w umowie z klientem, usługodawcą lub dostawcą.

Poniżej przedstawiamy kilka przykładów wymagań dotyczących bezpieczeństwa cybernetycznego i prywatności danych:

USTAWOWE WYMAGANIA ODNOŚNIE BEZPIECZEŃSTWA CYBERNETYCZNEGO I PRYWATNOŚCI

Prawo federalne USA

- Ustawa o ochronie prywatności dzieci w internecie (**COPPA**)
- Ustawa o sprawiedliwej sprawozdawczości kredytowej (**FCRA**)
- Ustawa o uczciwych i dokładnych transakcjach kredytowych **(FACTA**) - w tym zasada "czerwonej flagi"
- Ustawa o prawach rodzinnych w zakresie edukacji i prywatności (**FERPA**)
- Federalna ustawa o zarządzaniu bezpieczeństwem informacji (**FISMA**)
- Ustawa federalnej Komisji Handlu (**FTC**)
- Ustawa Gramm-Leach-Bliley (**GLBA**)
- Ustawa dotycząca przenośności i odpowiedzialności w zakresie ubezpieczeń zdrowotnych (**HIPAA**)
- Ustawa Sarbanes-Oxley (**SOX**)

Inne przykładowe wymagania ustawowe:

- Kanada - Ustawa o ochronie danych osobowych i dokumentach elektronicznych (**PIPEDA**)
- Wielka Brytania - Ustawa o ochronie danych (**DPA**)
- Polska - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000) **(UODO)**
- Polska - Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560) **(KSC)**

Przepisy prawa wspólnotowego UE

- Ogólne rozporządzenie o ochronie danych Unii Europejskiej (**EU GDPR**)

- DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS)

Przykładowe wymagania regulacyjne w Polsce:

- Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony

Niezależnie od tego, czy chcesz **uzyskać certyfikat systemu zarządzania, przetestować produkty, czy przeszkolić personel w zakresie zarządzania jakością**, DEKRA jest Twoim globalnym partnerem.

Dysponując ponad 1.000 obszarów działalności na całym świecie, DEKRA oferuje szerokie portfolio usług w zakresie jakości, zdrowia, bezpieczeństwa, zarządzania środowiskiem i odpowiedzialności społecznej.

30.000 firm w ponad 50 krajach korzystało z usług DEKRA podczas certyfikacji, przeprowadzania testów lub szkoleń, aby osiągnąć stawiane sobie cele. **Co możemy dla Ciebie zrobić?**

Kim Graham, Starszy manager ds. rozwoju firmy
DEKRA Certification, Inc.

Aby uzyskać więcej informacji na temat certyfikacji DEKRA ISO 27001:2013, programów audytu i oceny oraz szkoleń bezpieczeństwa danych firmy DEKRA, prosimy o kontakt:

Piotr Ubych, Menedżer ds. Usług Ochrony Danych
DEKRA Certification Sp. z o.o.
ul. Legnicka 48 H, 54-202 Wrocław
Tel. +48. 71. 780-47-77 do 78
Fax +48. 48.71.780-47-79
piotr.ubych@dekra.com

ZESPÓŁ SZKOLEŃ
Tel.: +48 22 850-01-75 do 79
Fax: +48 22 577-36-36
E-mail: szkolenia.pl@dekra.com