17.6.2025

Esencja z webinaru

RODO na pokaz - kiedy ochrona prywatności kończy się na papierze?

Dziękuję za udział w webinarze

Jeśli uważasz, że przekazałem wiedzę w sposób rzetelny
to dodaj proszę swoją opinię na wizytówce ODO 24 w Google.

Z góry dziękuję 😊

Jeśli potrzebujesz dodatkowego wsparcia merytorycznego – zachęcam do skorzystania z bezpłatnych porad prawnych i IT.

Specjalista ds. ochrony danych
Koordynator Zespołu Merytorycznego

Linki do źródeł wiedzy, inspiracji i nie tylko

Linki
Nagranie • RODO na pokaz - kiedy ochrona prywatności kończy się na papierze?
Polecamy • Kalkulator analizy ryzyka w RODO • Kalkulator oceny naruszeń RODO • Jak przeprowadzić analizę ryzyka zgodnie z RODO – praktyczne wskazówki • Uwzględnienie ochrony danych w fazie projektowania • Kim jest inspektor ochrony danych osobowych
W czym możemy pomóc • Outsourcing IOD • Analiza ryzyka i DPIA – zgodnie z RODO • Praktyczny kurs dla IOD
Bezpłatne konsultacje • Porozmawiaj z naszymi doradcami  Marcin Kuźniak umów spotkanie  Cezary Lutyński umów spotkanie

Pytania i odpowiedzi

Szanowni Państwo,
dziękuję za udział w webinarium i przesyłam odpowiedzi na zadane za pomocą czatu pytania. Jednocześnie uczulam, że odpowiedzi tych nie należy traktować jako „prawdy objawionej", gdyż – z uwagi na formę zadawania pytań – są to raczej wskazówki, sformułowane w oparciu o skromne informacje na temat stanu faktycznego.

Co z rozporządzeniem e-privacy?

Komisja Europejska wycofała się z prac nad tym rozporządzeniem. Oznacza to, że nie zostanie ono przyjęte.

ISO 27701 - rozszerzenie ISO 27001 i 27002 w zakresie zarządzania informacjami o ochronie prywatności?

Tak, 27701 stanowi rozszerzenie norm ISO/IEC 27001 Zarządzanie bezpieczeństwem informacji i ISO/IEC 27002 Kontrola bezpieczeństwa w zakresie ochrony prywatności. Zawiera wytyczne dla organizacji, które są odpowiedzialne za przetwarzanie danych osobowych w ramach systemu zarządzania bezpieczeństwem informacji (ISMS), w szczególności: administratorów danych, podmiotów przetwarzających dane osobowe. To bardzo konkretne rozszerzenie, dla organizacji które już wdrożyły ISO27001 i 27002 albo są w trakcie, przetwarzają dane osobowe i chcą być zgodne z RODO.

W jaki sposób ADO może przewidzieć wszystkie zagrożenia?

ADO nie jest w stanie przewidzieć wszystkich zagrożeń związanych z przetwarzaniem danych osobowych – i prawo tego od niego nie wymaga. Może jednak podejść do tego w sposób systemowy, identyfikując najbardziej prawdopodobne i istotne zagrożenia na podstawie analizy kontekstu przetwarzania, w tym wykorzystywanych zasobów.

Do przetwarzania danych wykorzystywane są różne zasoby, które same w sobie mogą stanowić źródło ryzyka (m.in.):

- **systemy informatyczne** – serwery, oprogramowanie, usługi chmurowe, urządzenia mobilne, które mogą posiadać podatności techniczne,
- **zasoby ludzkie** – pracownicy, współpracownicy, podmioty przetwarzające, których błędy lub celowe działania mogą prowadzić do naruszeń,
- **lokalizacje przetwarzania** – biura, serwerownie, praca zdalna, które niosą ryzyka fizyczne i organizacyjne.

ADO może także wykorzystywać inne dostępne narzędzia, jak analiza znanych incydentów i podatności (np. z baz ENISA, CERT, CVE), prowadzenie regularnych analiz ryzyka, przegląd i aktualizacja środków ochrony, szkolenia dla personelu czy procedury reagowania na incydenty.

Jak rozwiązać problem terminu przechowywania danych w systemach informatycznych? Nikt tych danych nie usuwa, często dokumentów papierowych już nie ma, a w systemie istnieją.

Retencja danych to już podstawa w kontekście RODO czy ISO27001.

W pierwszej kolejności to:

1. Inwentaryzacja danych (jakie dane mamy w systemach, gdzie trzymamy, do czego służą, kto ich używa, czy są powiązane z dokumentacją papierową oraz czy są objęte konkretnym okresem przechowywania).
2. Przypisanie okresu retencji (przepisy, cel i co ważne kopii zapasowej).
3. Opracowanie i wdrożenie polityki retencji danych, gdzie określimy: zasady przechowywania, osoby odpowiedzialne za kontrolę terminów np.: dział IT w systemach IT. Na podstawie kopii zapasowej określenie retencji danych, nadpisywania tych danych na nośnikach – zgodnie
z potrzebą biznesową wykonywania kopii.

Czy analiza ryzyka według czynności czy według zasobów jest bardziej wskazana / pomocna / pożyteczna?

Patrząc z puntu widzenia normy ISO27001 i naszego podejścia w ODO24, na pewno analiza ryzyka hybrydowa - według zasobów (aktywa: systemy, urządzenia, oprogramowanie) plus procesy (Rekrutacja, zatrudnienie) zmapowane z aktywami. Jest to klasyczne podejście pod normę ISO, lepsza kontrola nad technicznymi aspektami ryzyka: awarie, dostęp fizyczny. Jeśli mamy pełne wsparcie IT, podejście opierające się na zasobach jest bardziej techniczne.

Kto odpowiada za szkolenia - ADO czy IOD?

Odpowiedzialność za wdrożenie środka organizacyjnego w postaci szkolenia ciąży na administratorze. Oznacza to, że jeśli zostanie stwierdzony brak adekwatnego poziomu ochrony danych dlatego, że nie zostały przeprowadzone szkolenia, to administrator poniesie odpowiedzialność i może zostać obciążony karami. W strukturze administratora takie zadania może wykonywać IOD – jeżeli został powołany. Oznacza to, że administrator może rozliczać IOD z realizacji jego obowiązków.

Wartość ODO 24 tkwi w merytoryce zespołu ekspertów

Ochrona danych osobowych

Bezpieczeństwo informacji

Szkolenia RODO

Sprawdź nas

Tomasz Ochocki
Koordynator
zespołu merytorycznego

ZAPYTAJ O OFERTĘ