Wdrożenie wymagań RODO w organizacji – niezbędne czynności i harmonogram ich realizacji

System ochrony d.o. – obecnie

- Administrator Bezpieczeństwa Informacji - fakultatywnie
- Obowiązkowa dokumentacja ochrony d.o.:
  - Polityka Bezpieczeństwa,
  - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
  - Upoważnienia do przetwarzania danych osobowych.
- Rejestracja zbiorów w Biurze GIODO lub prowadzenie Rejestru zbiorów danych
- Realizacja sprawdzeń (jeżeli jest powołany ABI)

System ochrony d.o. - RODO

- Określenie procesów w których przetwarzane są dane osobowe

Jedna z metod, to analiza przetwarzanych danych osobowych przez pryzmat celu. Przykładowe cele:

- zatrudnienie,
- księgowość,
- nabór dzieci do przedszkola / szkoły,
- prowadzenie rejestru mieszkańców.

Proces – zespół działań nakierowanych na realizację celu.

System ochrony d.o. - RODO

- Ocena ryzyka związanego z przetwarzaniem danych osobowych w organizacji

  - Co się może stać z danymi osobowymi?
    (zostaną zniszczone, skradzione, wyciekną)
  - Czy te zagrożenia są realne?
  - Czy można je wyeliminować lub ograniczyć?
  - W jaki sposób?
  - W jaki sposób incydent dotyczący danych osobowych wpłynie na naruszenie praw i wolności podmiotów danych?

System ochrony d.o. - RODO

- Wdrożenie zabezpieczeń technicznych i organizacyjnych wynikających z oceny ryzyka oraz stworzenie odpowiednich polityk.

- Zapewnienie rozliczalności, czyli możliwości wykazania, że w organizacji są przestrzegane przepisy RODO.

Etapy wdrożenia

- **Powołać zespół wdrożeniowy**

W skład zespołu powinien wejść:

- przedstawiciel kierownictwa,
- Administrator Bezpieczeństwa Informacji,
- Administrator Systemu Informatycznego,
- przedstawiciel Działu Kadr,
- przedstawiciele kluczowych komórek organizacyjnych,
- opcjonalnie – konsultant zewnętrzny.

Etapy wdrożenia

- **Ustalić szczegółowy harmonogram prac**

Przy opracowywaniu harmonogramu uwzględnić podział zadań na:

- takie, które mogą być wykonane niezwłocznie
- które będą oczekiwały na uchwalenie przepisów dostosowawczych (przepisy zmieniające inne ustawy)
- które powinny być zrealizowane po wydaniu odpowiednich wytycznych:

GIODO – wytyczne dotyczące analizy ryzyka przetwarzania danych osobowych

Grupa Robocza art. 29 – wytyczne dotyczące zgody, transparentności przetwarzania d.o., naruszeń ochrony d.o. – grudzień 2017 r.

Etapy wdrożenia

- **Przeprowadzić audyt otwarcia w zakresie**

  - realizacji wymogów formalno-prawnych w zidentyfikowanych procesach,
  - badania zgodności systemów informatycznych z RODO.

Etapy wdrożenia

Wymogi formalno-prawne, między innymi:

- Przeprowadzić inwentaryzację zbiorów zawierających d.o.
- Ustalić status administratora i współadministratorów
- Ustalić podstawy prawne przetwarzania d.o. zgodnie z RODO (art. 6)
- Zweryfikować treści oświadczeń zgody na przetwarzanie d.o. (art. 7)
- Ustalić zasady realizacji obowiązku informacyjnego wymaganego przy zbieraniu danych osobowych (art. 13)
- Zweryfikować powierzanie przetwarzania danych osobowych innym podmiotom (art. 28) – wybór procesora, treść umowy

Etapy wdrożenia

<u>Zgodność systemu informatycznego, między innymi zweryfikować:</u>

- Możliwość realizacji praw osób, których dane dotyczą (art. 15-18 i 20)
  - prawo do sprostowania danych
  - prawo do „bycia zapomnianym”
  - prawo do ograniczenia przetwarzania
  - prawo do przenoszenia danych
  - prawo do dostępu do danych
- Możliwość odnotowanie informacji o odbiorcach danych (art. 15)
- Możliwość odnotowanie źródła pochodzenia danych (art. 15)
- Dokonać przeglądu stosowanych zabezpieczeń

Etapy wdrożenia

- Przeprowadzić pełną oceny skutków dla ochrony danych (jeśli proces tego wymaga) lub ocenę ryzyka naruszenia praw i wolności podmiotów danych (art.35)
- Przeprowadzić analizę ryzyka dla zasobów, które uczestniczą w przetwarzaniu d.o.
- Przygotować plan postępowania z ryzykiem
- Zaktualizować harmonogram wdrożenia o zadania wynikające z:
  - Audytu wstępnego
  - Planu postępowania z ryzykiem
  - W harmonogramie uwzględnić szkolenia pracowników

Niektóre obowiązki ADO

Art. 32

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych,

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

Etapy wdrożenia

Dokumentacja

- Określić procedury dotyczące:
  - obsługi żądań podmiotów danych kierowanych do IOD,
  - realizacji zadań związanych ze zgłaszaniem naruszeń ochrony danych osobowych (art. 33)
- Uzupełnić dokumentację o zapisy dotyczące:
  - powołania i zadań IOD
  - metodyki analizy ryzyka
  - procedur zapewnienia ciągłości działania
  - procedur przeglądów zastosowanych zabezpieczeń
- Utworzyć Rejestr czynności przetwarzania d.o.

Sprawdzenie stanu przygotowań

Termin – początek maja 2018 r.

Cel – weryfikacja realizacji zadań określonych w harmonogramie, w tym środków technicznych i organizacyjnych wynikających z przeprowadzonej analizy ryzyka

Działania po 25.05.2018 r.

- Wyznaczenie IOD i powiadomienie Prezesa Urzędu Ochrony Danych (art. 37)
- Stosowanie kodeksów postępowania i certyfikacja (art. 41-43)
- Uwzględnianie ochrony danych w fazie projektowania (art. 25)

Wdrożenie RODO i co dalej?

- Procesowe podejście do ochrony danych osobowych

  Administrator musi zadbać nie tylko o to, by wykazać zgodność przetwarzania danych z przepisami prawa oraz zastosowanie odpowiednich zabezpieczeń w momencie ich wdrażania, ale również zagwarantować, że ten stan nie zmieni się wraz z przejściem na poziom codziennej obsługi procesów przetwarzania d.o.

Usługi ZETO Koszalin Sp. z o.o. związane z RODO

- Szkolenia pracowników, zespołu powołanego do wdrożenia RODO, kandydata do pełnienia funkcji IODO
- Współudział w procesie wdrażania RODO na każdym etapie
- Pomoc w ocena ryzyka związanego z przetwarzaniem d.o.
- Audyt bezpieczeństwa informacji zgodny z normą ISO/IEC 27001:2013

Dziękuję za uwagę

Jolanta Kubiak

Zakład Elektronicznej Techniki Obliczeniowej Sp. z o.o.
w Koszalinie