Centrum Prawa Bankowego i Informacji
www.cpb.pl

Szkolenie

Wdrożenie RODO, aspekt praktyczny

godz. 9.00-16.00

13 lutego 2018 r.,

Centrum Konferencyjne KOPERNIKA, ul. Kopernika 30 w Warszawie

Głównym celem szkolenia jest wskazanie czynników i posiadanych w bankach zasobów, które pozwolą na usprawnienie implementacji RODO, zgodnie z założeniami regulatorów, przy możliwie niewielkich kosztach. Takie podejście może stać się czynnikiem poprawy pozycji konkurencyjnej banku.

Prowadzący:

- dr Stefan Szyszko- krajowy i europejski ekspert ds. ochrony danych

9.00 – 9.10 Rejestracja i poranna kawa
9.10 – 10.50 Część I

1. Ustalenie, w jakiej fazie dojrzałości organizacyjnej znajduje się AD w odniesieniu do zarządzania procesami biznesowymi:
   a) Czy, a jeśli tak, to jakie mechanizmy normatywne są wykorzystywane:
      - ISO-9001
      - Inne?
   b) Czy możliwe jest wykorzystanie tych mechanizmów do:
      - Zautomatyzowanej inwentaryzacji całości procesów zarządzania ryzykiem przetwarzania danych
      - Uproszczeniem obsługi ryzyka wynikającego z RODO?
2. Ustalenie, w jakiej fazie dojrzałości organizacyjnej znajduje się AD w odniesieniu do zarządzania bezpieczeństwem przetwarzania danych:
   a) Czy, a jeśli tak, to jakie mechanizmy normatywne są wykorzystywane:
      - ISO-2700x
      - Inne?
   b) Czy możliwe jest wykorzystanie tych mechanizmów do:
      - Zautomatyzowanej inwentaryzacji całości procesów zarządzania ryzykiem przetwarzania danych
      - Uproszczeniem obsługi ryzyka wynikających z RODO?

10.50 – 11.00 Przerwa kawowa
11.00 – 12.40 Część II

3. Ustalenie, w jakiej fazie dojrzałości organizacyjnej znajduje się AD w odniesieniu do zarządzania ciągłością działania:
   a) Czy, a jeśli tak, to jakie mechanizmy normatywne są wykorzystywane?
   b) Czy możliwe jest wykorzystanie tych mechanizmów do:
      - Zautomatyzowanej inwentaryzacji całości procesów zarządzania ryzykiem przetwarzania danych
      - Uproszczeniem obsługi ryzyka wynikających z RODO?
4. Punkt dla tych AD, które mają wdrożone ISO-2700x lub przynajmniej zarządzają bezpieczeństwem w sposób zgodny z zasadami tych norm, ale nie poddały się certyfikacji:
   a) Czy dostawca outsourcingu przetwarzania danych oferuje wsparcie wdrożeniowe w procesie analizy i oceny ryzyka, np. w postaci plug-ins dla norm serii ISO-27xxx:
      - „Kontrolki" wg załącznika do ISO-27001

Sprawy organizacyjne:
Katarzyna Cechowska
k.cechowska@wydawnictwocpb.pl
tel. (22) 623 84 53

- Ewentualny inny standard normalizacyjny
- Dlaczego taki, a nie inny?

b) Czy dostawca outsourcingu przetwarzania danych oferuje wsparcie w obsłudze kontroli ze strony organów nadzoru w przypadku powierzenia przetwarzania tak daleko posuniętego, że klient jest pozbawiony szczegółowej wiedzy oraz technicznych możliwości właściwej samodzielnej interakcji z organem nadzoru podczas kontroli?
   - Jednym z celów outsourcingu jest uwolnienie się od samodzielnych ingerencji w technologiczne szczegóły przetwarzania
   - W takich warunkach (vide Cloud Computing) w pełni samodzielna obsługa kontroli jest bardzo trudna
   - GDPR / RODO nakłada tu dodatkowe reżimy ze względu na wymagany czas reakcji

12.40 – 13.10 Lunch

13.10 – 14.30 Część III

5. Dobre praktyki zarządzania procesami przetwarzania danych:
   a) Identyfikacja danych i ich przepływów
      - W systemach centralnych
      - W przetwarzaniu rozproszonym
   b) Jak ulokować nakazane przez GDPR/RODO „rejestrowanie czynności przetwarzania"?
      - Jak termin może być interpretowany – dostępny zakres swobody AD
      - Rola IOD (następcy ABI)

6. Wdrożenie zasady minimalizacji przetwarzania danych w ramach zapewnienia adekwatności zakresu przetwarzania do jego celów:
   a) Cel: identyfikacja procesów przetwarzania, z których można zrezygnować ze względu na ryzyko nieadekwatnie duże do korzyści biznesowych
   b) Rola IOD (następcy ABI)

7. Wdrożenie zasady minimalizacji przetwarzania danych w ramach zapewnienia pełnego panowania nad jego całością:
   a) Cel: identyfikacja procesów przetwarzania lokalnego, z których można zrezygnować ze względu na ryzyko nieadekwatnie duże do korzyści biznesowych, lub z powrotem przetwarzać wyłącznie w sposób scentralizowany
   b) Warianty postępowania, gdy okaże się że cel ten nie będzie mógł zostać zrealizowany ze względów takich jak:
      - Wygoda przetwarzania
      - Koszty
   c) Dyskusja dostępnych rozwiązań kategorii: ZNAJDŹ DANE OSOBOWE W SWOICH SYSTEMACH
   d) Rola IOD (następcy ABI)

8. Analiza ryzyka, w szczególności adresującą takie kwestie jak:
   a) Zarządzanie „czasem życia" danych, w szczególności ich:
      - Pseudonimizacją (anominizacją)
      - Usuwaniem
      - Kontrolą udostępniania
   b) Ograniczanie przetwarzania danych:
      - Wyszukiwanie danych w systemach transakcyjnych oraz archiwalnych
      - Analiza i ocena ryzyka wszystkich zidentyfikowanych form przetwarzania
      - Czy i kiedy można usuwać dane z archiwów:

      – Jeśli w ogóle usuwać, to jakimi technikami można to czynić
      – Zarządzanie widokami danych w zależności od posiadanych uprawnień dostępowych, zmieniających się w „czasie życia danych"
   c) Szyfrowanie danych – kiedy, w jakim celu, jak?
   d) Zarządzanie:

Sprawy organizacyjne:
Katarzyna Cechowska
k.cechowska@wydawnictwocpb.pl
tel. (22) 623 84 53

- Dopuszczeniami do przetwarzania danych
- Uprawnieniami do systemów przetwarzania danych. Zarządzanie to nie tylko nadawanie uprawnień. Trzeba je, adekwatnie do sytuacji:

– Zmieniać
– Odbierać

e) Korelacja zarządzania z własnością procesów biznesowych:
- Identyfikacja „SIEROT":

- Procesów
- Systemów
- Danych

f) Ryzyka nieadekwatnej współpracy:
- Pionów biznesowych
- IT
- HR
- Compliance
- Audyt/ Kontrola

g) Rola IOD (następcy ABI)

14.30 – 14.40 Przerwa kawowa

14.40 – 16.10 Część IV

9. Sprostanie obowiązkom notyfikacyjnym przez AD:
   a) Naruszenie ochrony
   b) Inne obowiązki informacyjne w odniesieniu do podmiotów danych oraz organów nadzoru
   c) Rola IOD (następcy ABI)

10. Wnioski z powyższych etapów szkolenia:
   a) Dobre praktyki w obszarze domyślnej ochrony danych:
      - Privacy by design/ privacy by default
   b) Nowy podział ryzyka kontraktowego: AD/ procesor w odniesieniu do umów na produkty i usługi
   c) Wzorce umów, uwzględniające nowe aspekty związane z GDPR/ RODO, wyraźnie "procesorów" na to uwrażliwiające?
      - Jakie dokładnie kwestie wymuszone wprowadzeniem GDPR/ RODO są adresowane
      - Dlaczego tak, a nie inaczej?
   d) Analiza i ocena ryzyka dla dostarczanych produktów i usług
      - Podział kosztów materializacji ryzyka: AD/ procesor
   e) Kary umowne – jak nimi zarządzać w nowej rzeczywistości GDPR/ RODO?
      - Ewentualne dodatkowe ubezpieczenia?
   f) Zadania dla IOD (następcy ABI)

11. Reagowanie na naruszenia ochrony danych:
   a) Co nakazuje GDPR/ RODO?
   b) Jak to wdrożyć?
   c) Rola IOD (następcy ABI)

12. Resume- wskazówki dla IOD (następcy ABI) w odniesieniu do wszystkich wyżej omawianych kwestii:
   a) Zasady współpracy
   b) Podział zadań
   c) Alokacja zasobów

16.10 Zakończenie

Sprawy organizacyjne:
Katarzyna Cechowska
k.cechowska@wydawnictwocpb.pl
tel. (22) 623 84 53