dr hab. prof. UO DARIUSZ SZOSTEK
Kancelaria Szostek-Bar i Partnerzy

RODO a cyberbezpieczeństwo

RODO a cyberbezpieczeństo

- ROZPORZĄDZENIE RODO

25 maja 2018

- Projekt ustawy o krajowym systemie cyberbezpieczeństwa

Termin wejścia w życie – jesień 2018r.

Pojęcia

- Cyberbezpieczeństwo – odporność systemów informacyjnych na wszelkie działania naruszające
- poufność,
- integralność,
- dostępność i autentyczność przetwarzanych danych
- lub związanych z nimi usług oferowanych przez te systemy

- RODO

Skutkiem naruszenia bezpieczeństwa danych może być:

- Zniszczenie
- Utracenie
- Zmodyfikowanie
- Nieuprawnione ujawnienie
- Nieuprawniony dostęp do danych osobowytch

POJĘCIA

- INCYDENT KRYTYCZNY
- INCYDENT KRYTYCZNY
- INCYDENT POWAŻNY
- INCYDENT ISTOTNY
- INCYDENT W PODMIOCIE PUBLICZNYM

OBSŁUGA INCYDENTU

Czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację ,

Podejmowanie działań naprawczych

Ograniczanie skutków incydentu

Pojęcia

- Ryzyko
- Szacowanie ryzyka
- Zagrożenie cyberbezpieczeństwa
- Zarządzanie incydentem
- Zarządzanie ryzykiem

Dostawca usług cyfrowych

- **Art. 17.** 1. Dostawcą usługi cyfrowej jest
  - osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej,
  - mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej
  - albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej,

  - świadcząca usługę cyfrową w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

- (Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650), wymienioną w załączniku nr 2 do ustawy, z wyjątkiem przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646). Załącznik nr 2 do ustawy określa rodzaje usług cyfrowych.

Usługi cyfrowe (załącznik II)

- Internetowa platforma handlowa

- Usługa, która umożliwia konsumentom lub przedsiębiorcom
- zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej
- albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową

Usługi cyfrowe (załącznik II)

- Usługa przetwarzania w chmurze

- Usługa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych
- do wspólnego wykorzystywania przez wielu użytkowników.

Usługi cyfrowe (załącznik II)

- Wyszukiwarka internetowa

- Usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub
- stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu,
- przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem.

Rozdział VII

Zasady udostępniania informacji i przetwarzania danych osobowych

Lex specialis do RODO ?

Art. 37

- **Art. 37.** 1. Do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764 oraz z 2017 r. poz. 933).

- 2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV **może**, po konsultacji ze zgłaszającym operatorem usługi kluczowej, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.

- 3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, opublikować
  - na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej lub Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego
  - informacje o incydentach istotnych lub wystąpić do organu właściwego dla dostawcy usług cyfrowych, aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości,
  - gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym.

- 4. Opublikowanie informacji, o której mowa w ust. 2 i 3, nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, **a także przepisów o ochronie danych osobowych**.

Art. 38

- Nie udostępnia się informacji przetwarzanych na podstawie ustawy, jeżeli ich ujawnienie naruszyłoby
  - ochronę interesu publicznego w odniesieniu do bezpieczeństwa lub porządku publicznego,
  - a także negatywnie wpłynęłoby na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania.

Art. 39

- **Art. 39.** 1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3,
- CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa
- przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa,
- w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, **w zakresie i w celu niezbędnym do realizacji tych zadań**.

Art. 39

- 2. CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa, przetwarzając dane osobowe określone w art. 9 ust. 1 rozporządzenia 2016/679,

- prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu, a także opracowują procedury bezpiecznej wymiany informacji.

Art. 39

- 3. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa:
  - 1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych;
  - 2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
  - 3) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług;
  - 4) gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.

Art. 39

- 4. W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik oraz organy właściwe do spraw cyberbezpieczeństwa przetwarzają dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa:
  - 1) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług;
  - 2) gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych;
  - 3) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.

- 5. Dane, o których mowa w ust. 3 i 4, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne dla realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3.

- 6. Dane, o których mowa w ust. 3 i 4, niezbędne dla realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa w terminie 5 lat od zakończenia obsługi incydentu, którego dotyczą.

-

- W celu realizacji zadań określonych w ustawie CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa

- **mogą wzajemnie przekazywać dane osobowe**, o których mowa w ust. 3,

- w zakresie niezbędnym do realizacji tych zadań i współpracować z organem właściwym do spraw ochrony danych osobowych.

- Przetwarzanie przez CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa danych osobowych, o których mowa w ust. 3, nie wymaga realizacji obowiązków, o których mowa w art. 15, art. 16 i art. 18 ust. 1 lit. a i d i art. 19 zdanie drugie rozporządzenia 2016/679,

- jeżeli uniemożliwiłoby to realizację zadań CSIRT NASK, CSIRT MON i sektorowych zespołów cyberbezpieczeństwa, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3,

- i jest możliwe, gdy CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem, stosują mechanizmy kontroli dostępu oraz opracowują procedury bezpiecznej wymiany informacji.

- CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa publikują na swojej stronie internetowej:
  - 1) dane kontaktowe administratora danych oraz gdy ma to zastosowanie, dane kontaktowe inspektora ochrony danych;
  - 2) cele przetwarzania i podstawę prawną przetwarzania;
  - 3) kategorie przetwarzanych danych osobowych;
  - 4) informacje o odbiorcach danych osobowych;
  - 5) okres, przez który dane osobowe będą przechowywane;
  - 6) informacje o ograniczeniach obowiązków i praw osób, których dane dotyczą;
  - 7) informacje o prawie wniesienia skargi do organu właściwego do spraw ochrony danych osobowych;
  - 8) źródło pochodzenia danych osobowych

Art. 40

- **Art. 40.** 1. CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i minister właściwy do spraw informatyzacji przetwarzają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, o których mowa w ustawie.

- 2. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przekazują dane, o których mowa w ust. 1, **organom ścigania w związku z incydentem wyczerpującym znamiona przestępstwa**.

Ochrona danych
aspekty techniczne i zabezpieczenie fizyczne.

Konieczność zabezpieczenia danych w kancelarii.

Praca kancelarii prawnych wiąże się z koniecznością:
- pozyskiwania,
- przechowywania,
- przetwarzania,
- udostępniania
- usuwania
- niszczenia

danych dotyczących klientów, ich przeciwników procesowych, ale także danych pracowników i współpracowników.

Są to zarówno dane osobowe, jak i dokumenty zgromadzone w trakcie postępowania przedsądowego oraz w trakcie procesu sądowego.

Zabezpieczenie danych.

Podejmując decyzje w zakresie stosowanych środków zabezpieczenia danych, należy kierować się koniecznością zabezpieczenia przez istniejącymi zagrożeniami.

Należy dokonać analizy ryzyka wiążącego się z przetwarzaniem danych osobowych, uwzględniając przy tym zagrożenia wewnętrzne oraz zewnętrzne, kształtujące poziom ryzyka związanego z przetwarzaniem danych.

Stosowane środki zabezpieczenia danych osobowych powinny być dostosowane do kategorii przetwarzanych danych oraz istniejących zagrożeń.

Obszary zabezpieczenia danych w kancelarii.

Niezależnie jednak od wykorzystanych standardów przy projektowaniu systemu bezpieczeństwa należy brać pod uwagę bezpieczeństwo w kilku sferach:

- w sferze fizycznego zabezpieczenia dostępu do lokalu kancelarii danych, dokumentów,
- w sferze organizacyjnej obejmującej odpowiedzialność poszczególnych osób zatrudnionych w kancelarii,
- w sferze prawnej dotyczącej legalności przetwarzania danych i klauzul umownych oraz
- w sferze technologicznej obejmującej stosowane rozwiązania zabezpieczające systemy informatyczne ich aktualizacje, obejmującej urządzenia, nadzór nad systemem i uporządkowany i sformalizowany dostęp do danych.

Atak ransomware na Kancelarie przez pocztę elektroniczną

Od: GIODO <kanelaria@giodo.gov.pl>
Data: 2017-06-23 17:03:23
Temat: Powiadomienie o planowanej kontroli GIODO w państwa Kancelarii
Do:

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Biuro Generalnego Inspektora Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
tel. 22 531 03 00
fax. 22 531 03 01

Powiadomienie o planowanej kontroli GIODO.PDF.zip
2.2 KB

Bezpieczeństwo urządzeń dostępowych - 10 złotych zasad

1) Chroń dostęp do urządzenia hasłem/pinem/kartą.
2) Pracuj na najniższych możliwych uprawnieniach.
3) Instaluj aktualizacje bezpieczeństwa.
4) Nie udostępniaj haseł.
5) Włącz blokowanie ekranu.
6) Używaj zawsze aktualnego oprogramowania antywirusowego.
7) Nie używaj bez skanowania w komputerach podłączonych do sieci pendriva, który był podłączony do innego komputera
8) Szyfruj twarde dyski komputera, pendriva.
9) Wykonuj kopie bezpieczeństwa (poza siedzibą).
10) Szyfruj kopie bezpieczeństwa.

Dziękuję za uwagę ☺

dariusz.szostek@szostek-bar.pl