LEWIATAN

PROJEKTOWANE ZMIANY W UNIJNYCH PRZEPISACH O OCHRONIE DANYCH OSOBOWYCH

Magdalena Piech

Ossa, Rawa Mazowiecka, 30 listopada 2013 r.

KOGO DOTYCZY?

- branża bankowa
- telekomunikacyjna
- ubezpieczeniowa
- IT
- handel elektroniczny
- marketing bezpośredni

- przedsiębiorcy przetwarzający dane osób fizycznych
- przedsiębiorcy chcący reklamować swoje usługi i towary, szczególnie w Internecie
- firmy świadczące usługi dla biznesu

Projekt rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (2012/0011 COD)

Zaangażowane podmioty:

- Komisja Europejska (Projekt)
- Parlament Europejski
- Rada Unii Europejskiej

(PL: Ministerstwo Administracji i Cyfryzacji)

STAN PRAC

Stan prac

25.01.2012r. Przedstawienie Projektu przez Komisję Europejską

31.05.2013r. Rada UE: Raport Prezydencji Irlandzkiej (Rozdz. I-IV)

21.10.2013r. Parlament Europejski: Sprawozdanie Komisji LIBE.

LEWIATAN

CELE

CELE PROJEKTU

- aktualizacja dyrektywy z 1995r.
- harmonizacja przepisów UE
- zasada *one stop shop*
- zmniejszenie kosztów (?)
- wzmocnienie praw podmiotów danych

CZEGO NALEŻY SIĘ SPODZIEWAĆ ?

Czego należy się spodziewać?

- wzrostu kosztów związanych z zapewnieniem zgodności z przepisami
- rozszerzenia obowiązków informacyjnych i sprawozdawczych
- wzmocnienia pozycji organów nadzorczych (GIODO)
- ryzyka nałożenia sankcji

(do 100 000 000 Euro lub 5% rocznego globalnego obrotu)

- ograniczenia w możliwości promowania swoich produktów i usług (?)
- rozszerzenie praw podmiotów danych.

OBOWIĄZKI ADMINISTRATORA DANYCH

PRZED ROZPOCZĘCIEM PRZETWARZANIA

- Opracowanie „*zwięzłych, przejrzystych, jasnych i łatwo dostępnych polityki*” dotyczące przetwarzania danych osobowych i wykonywania praw podmiotów danych (art. 11(1) LIBE);
- przeprowadzić analizę szczególnego ryzyka (PE)
- przeprowadzić ocenę skutków w zakresie ochrony danych osobowych (*privacy impact assesment)*
- weryfikacja zgodności (*compliance review*)- co 2 lata- PE
- mianować Administratora Bezpieczeństwa Informacji

(4/2 letnia kadencja, trudno odwoływalny, podlegający bezpośrednio kierownictwu)

- konsultacja z GIODO (*prior consultation*)- jeśli szczególne ryzyka

UPRZEDNIA KONSULTACJA

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Jeśli wysoki stopień ryzyka przetwarzania danych

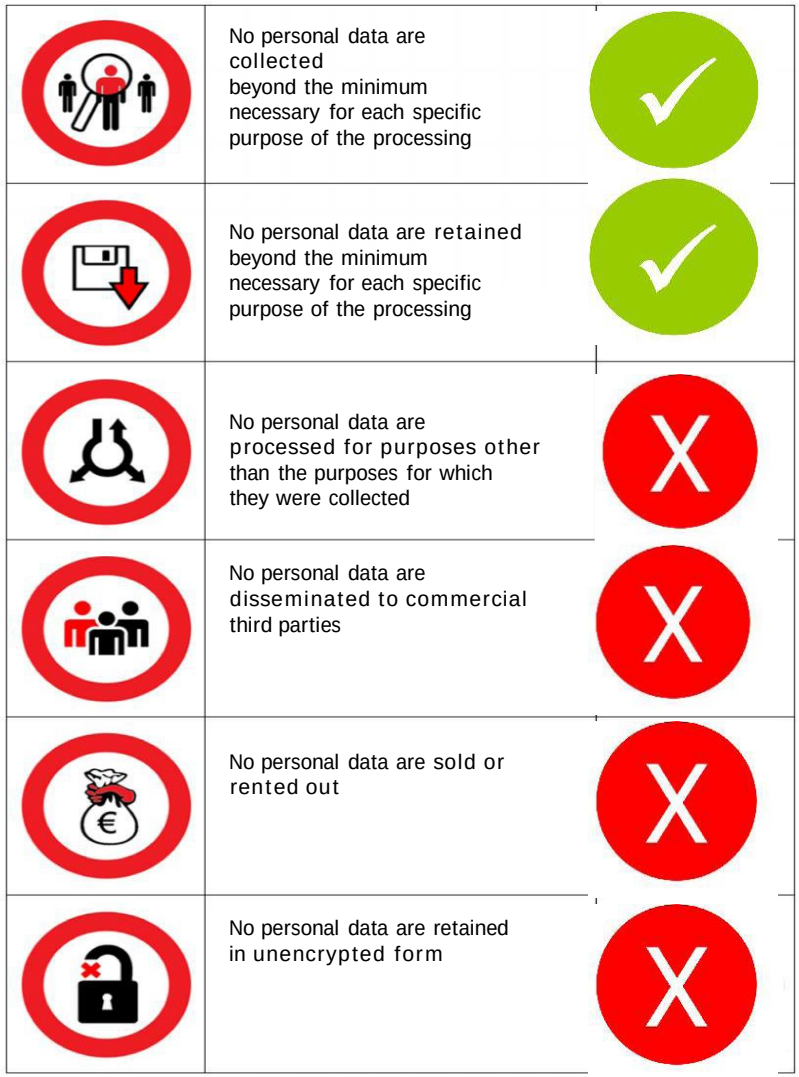
(przetwarzanie danych wrażliwych, danych dzieci w wielkoskalowych systemach informatycznych, profilowanie znacznie oddziaływujące na podmioty danych)

- PE: 6 (+4) tygodni „na udzielenie porady”
- Rada UE: zakaz rozpoczęcia przetwarzania i przedstawienie środków usunięcia zagrożeń.

OBOWIĄZKI INFORMACYJNE

Przed rozpoczęciem przetwarzania (PE)

- Niezależnie od sposobu pozyskiwania danych
- dodatkowy obowiązek informacyjnych
- „niezgodność” mimo legalnego działania



DALSZE OBOWIĄZKI INFORMACYJNE

- tożsamości i danych kontaktowych administratora oraz ABI;
- celach przetwarzania danych, do których przeznaczone są dane,
- bezpieczeństwie przetwarzania danych, w tym o warunkach umowy, na podstawie której będą przewarzane dane, a także informacje na temat sposobu ich realizacji i spełnienia wymagań wskazanych w art. 6 (1) (f) LIBE;
- okresie, w którym dane osobowe będą przechowywane, lub jeśli nie jest to możliwe, o kryteriach stosowanych do określenia tego okresu;
- prawie do żądania dostępu do danych i ich poprawiania lub usunięcia danych, prawie do sprzeciwu wobec przetwarzania tych danych, lub uzyskania danych;
- prawie do złożenia skargi do organu nadzoru oraz danych kontaktowych organu nadzoru;
- odbiorcach lub kategoriach odbiorców danych;
- o profilowaniu, środkach opierających się na profilowaniu, oraz przewidywanym wpływie profilowania na prawa osoby, której dane dotyczą;
- o algorytmach związanych z każdym automatycznym przetwarzaniem danych;
- wszelkie inne informacje, które są niezbędne w celu zagwarantowania rzetelnego przetwarzania danych, uwzględniające szczególne okoliczności, w których dane osobowe są gromadzone i przetwarzane, w szczególności istnienie niektórych czynności przetwarzania, których ocena wskazuje, że mogą wiązać się z wysokim ryzykiem w zakresie ochrony danych;
- w stosownych przypadkach, informację, czy dane osobowe były dostarczone do władz publicznych w ostatnim okres kolejnych 12 miesięcy

NOWE OBOWIĄZKI

Obowiązek notyfikacji naruszeń

- definicja naruszenia
- termin notyfikacji (24/72h)
- katalog informacji
- jawny rejestr naruszeń (?)
- informowanie podmiotu danych o naruszeniach

Podmiot przetwarzający

- „cele i warunki przetwarzania”
- obowiązki i odpowiedzialność
- sankcje

PRAWA PODMIOTÓW DANYCH

Prawa podmiotów danych

Dotychczasowe:

- prawo dostępu do danych – częściej niż raz/6 mies.
- prawo do sprostowania danych
- prawo usunięcia danych
- prawo sprzeciwu (PE: bezwarunkowe)

Nowe:

- prawo do przenoszenia danych
- prawo do bycia zapomnianym

PRAWO DO PRZENOSZENIA DANYCH

KE:

1. (...) jeśli dane osobowe są przetwarzane w sposób elektroniczny oraz w zorganizowanym i powszechnie używanym formacie, (podmiot danych ma prawo) do uzyskania od administratora kopii danych podlegających przetwarzaniu w formacie elektronicznym i zorganizowanym, który jest powszechnie używany i umożliwia dalsze wykorzystywanie przez podmiot danych.

2. Jeżeli (...) przetwarzanie opiera się na zgodzie lub umowie, podmiot danych ma prawo do przekazania tych danych osobowych i innych informacji przez siebie przekazanych i przechowywanych w systemie automatycznego przetwarzania danych, do innego systemu, w powszechnie używanym formacie elektronicznym, bez przeszkód ze strony administratora, z którego baz dane osobowe zostają wycofane.

3. Komisja może opracować format elektroniczny, o którym mowa w ust. 1 oraz techniczne standardy, sposoby i procedury przekazywania danych osobowych na mocy ust. 2. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

PRAWO DO PRZENOSZENIA DANYCH

PE art. 15 ust. 2a

Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.

Rada art. 18 ust 2:

Where the data subject has provided personal data and the processing, (...) based on consent or on a contract, is carried on in an automated processing system provided by an information society service, the data subject shall have the right to withdraw these data in a form which permits the data subject to transmit them into another automated processing system without hindrance from the controller from whom the personal data are withdrawn .

PRAWO DO BYCIA ZAPOMNIANYM

KE: Art 17 ust 2

- w przypadku upublicznienia danych:

obowiązek poinformowania stron trzecich, „że podmiot danych wnioskuje o usunięcie linków do danych, kopii lub replikacji tych danych”

Rada: bez zmian

PE:

- tylko w sytuacji kiedy dane zostały upublicznione bez podstawy prawnej

(!) art. 17 ust 2 (c) i art. 19 ustęp 2
jeśli podmiot sprzeciwił się dalszemu przetwarzaniu (prawo bezwarunkowe)

KOSZTY

KOSZTY

- powołanie ABI
- sporządzenie obszernych polityk i dokumentacji
- realizacja nowych praw podmiotów danych

(przenoszalność danych, prawa odbiorców)

- umowy powierzenia
- wzrost kosztów marketingowych
- realizacja obowiązków informacyjnych
- sankcje

PODSTAWY PRZETWARZANIA DANYCH

Podstawy przetwarzania danych

zgoda

- wyraźna
- *significant imbalance*
- usługa uzależniona od danych (art. 7 ust 4 EP)
- zgoda dziecka

uzasadniony interes administratora

- przetwarzanie zgodne z „rozsądnymi oczekiwaniami podmiotu danych” (PE)
- bezwarunkowe prawo sprzeciwu
- uzasadniony interes strony trzeciej/administratora, której/emu dane są udostępniane

SANKCJE

SANKCJE ADMINISTRACYJNE

Organ uprawniony do nakładania sankcji
Rada: organ właściwy
PE: każdy organ nadzorczy

Podstawy nałożenia sankcji
KE- niejasne dyspozycje
PE- „za niespełnienie obowiązków nałożonych rozporządzeniem”

Na kogo ?
Rada: administrator danych/ podmiot przetwarzający/przedstawiciel
PE: każdy, kto nie spełnia obowiązków

Sankcje karne
Regulowane w prawie krajowym

WYSOKOŚĆ SANKCJI

KE
- max. 100 000 EUR lub w przypadku przedsiębiorstwa do 2% rocznego światowego obrotu
-działanie umyślne lub niedbalstwo
- brak możliwości odstąpienia od wymierzenia kary

PE
- max. 100 000 000 EUR lub do 5% rocznego światowego obrotu
- odpowiedzialność obiektywna
- „za niewypełenienie obowiązków nałożonych rozporządzeniem”

Rada
- obecnie brak kwot
- działanie umyślne lub niedbalstwo

TERMIN STOSOWANIA PRZEPISÓW ?

- 24/25.10.2013 Rada Europejska: „*timely adoption*” (...) by 2015”
- koniec kadencji PE – 1 lipca
- głosowanie na sesji plenarnej
- stanowisko Rady
- 2 lata od przyjęcia
- zasada dyskontynuacji ?

Dziękuję za uwagę

Magdalena Piech
mpiech@konfederacjalewiatan.pl