KL&M LAW

Kobylańska · Lewoszewski · Mednis

Zapewnienie bezpieczeństwa danych w fazie projektowania

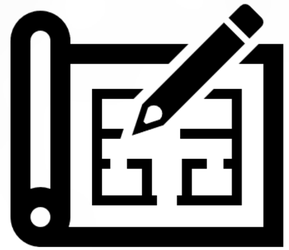
Dr hab. Arwid Mednis (KL&M Law, WPiA UW)

Na jakim etapie powinniśmy rozważyć przyjęcie środków bezpieczeństwa?

Obowiązek uwzględnienia ochrony prywatności w fazie projektowania:

Administrator wdraża odpowiednie środki techniczne i organizacyjne zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania.

Odpowiednimi środkami technicznymi mogą być:
szyfrowanie i pseudonimizacja danych.



Ochrona danych w fazie projektowania – cel i kryteria

Kryteria:
należy uwzględnić 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 wynikające z przetwarzania.

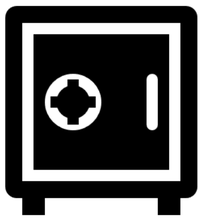
Cel:
skuteczna realizacji zasad ochrony danych (w tym zasady integralności i poufności) oraz nadanie przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

Zasada integralności i poufności:
dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Ocena skutków przetwarzania (DPIA)

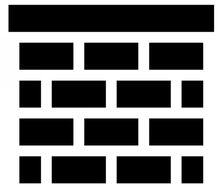
Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Ocena zawiera m. in. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.



Domyślna ochrona danych

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.



KL&M LAW
Kobylanska · Lewoszewski · Mednis

Wytyczne EROD

Wytyczne nr 4/2019 dotyczące artykułu 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Wersja 2.0

Przyjęte 20 października 2020 r.

Szyfrowanie a *privacy by design*

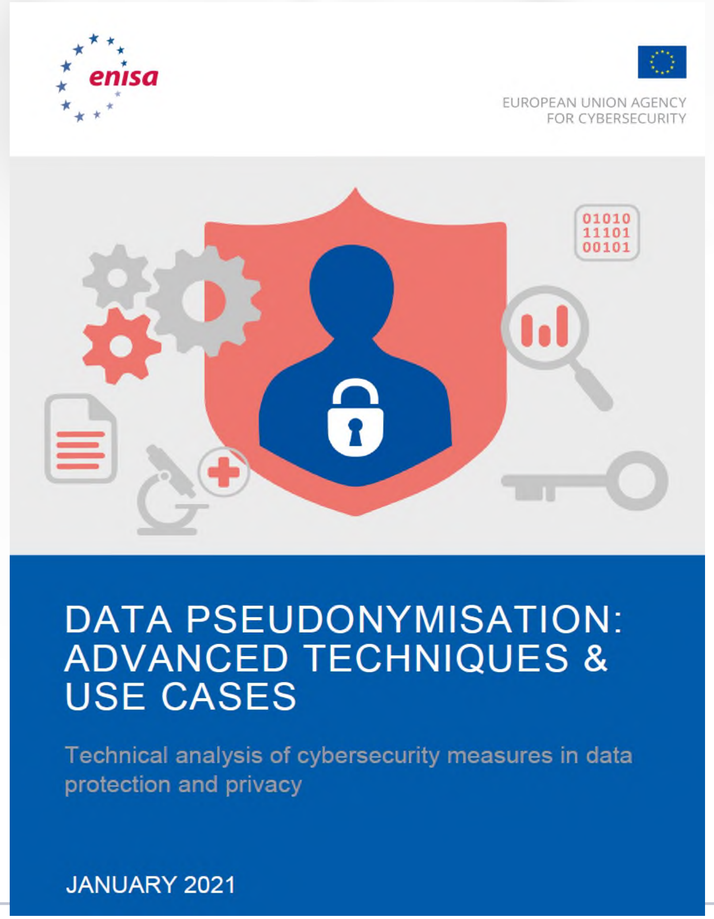
Kluczowe elementy uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych mogą obejmować przede wszystkim:

Integralność i poufność poprzez m. in. kontrolę dostępu – szyfrowanie może być wykorzystane w celu ograniczenia dostępu do określonych danych osobowych (przykład EROD z wykorzystaniem danych medycznych w celu kontroli jakości) oraz w ogólnym celu zabezpieczenia danych (EROD rekomenduje pseudonimizację m. in. kopii zapasowych);

Ograniczenie celu poprzez m. in. ograniczenie ponownego wykorzystania – *administrator powinien stosować środki techniczne, w tym haszowanie i szyfrowanie, w celu ograniczenia możliwości ponownego wykorzystania danych osobowych w innym celu* (wytyczne EROD)

KL&M LAW
Kobylanska · Lewoszewski · Mednis

ENISA



KL&M LAW
Kobylanska · Lewoszewski · Mednis

Dziękuję za uwagę

arwid.mednis@klmlaw.pl

KL&M LAW

Kobylanska · Lewoszewski · Mednis