Informatyk czyta GDPR/RODO

Wersja uzupełniona po Seminarium

Dr inż. Wacław Iszkowski

Ekspert PIIT, PTI

Kilka danych osobowych o sobie

1972-1990 Adiunkt w Inst. Informatyki Politechniki Warszawskiej

[programowanie, prog. współbieżne, systemy operacyjne]

[programowanie – od asemblera do AutoLispa - 14 języków]

1990-2000 Praca dla ORACLE'a, DIGITALA, EDS, TPSA

[Business Development Manager, Consultant]

1993-2016 Prezes Polskiej Izby Informatyki i Telekomunikacji

[łączenie informatyki z telekomunikacją oraz system prawnym]

[udział w opracowywaniu ustaw dotyczących teleinformatyki]

2017 Napisanie oprogramowania własnej witryny (HTML, CSS)

www.iszkowski.eu/rodo

Standardy tłumaczenia dyrektyw i rozporządzeń

W rozporządzeniach unijnych w definiowaniu pojęć stosowane są dwa standardowe wzorcowe zapisy w wersji angielskiej, które jednolicie powinny być tłumaczone na język polski:

‘xxx’ means any vvvv …. who ….. w tłumaczeniu na polski:
„xxx” oznacza każde vvvv ….., które ……

‘xxx’ means vvvv …. who.... w tłumaczeniu na polski:
„xxx” oznacza vvvv ….., które …..

zamiast starszego zapisu: *shall mean any -> oznacza wszelkie*

Dane osobowe

EN16	1) ‘personal data’ [shall mean any] means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
PL16	1) „dane osobowe” oznaczają [wszelkie] informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Dana osobowa

W definicjach ustaw, rozporządzeń, dyrektyw definiujemy obiekty w liczbie pojedynczej, a więc gdy po ang. *data* jest w liczbie mnogiej, to polsku może być tłumaczona na *daną* w liczbie pojedynczej lub *dane* w liczbie mnogiej:

Personal data - dana osobowa, ale zależnie od kontekstu może być
Personal data - dane osobowe.

Dlatego też proponuję skróconą wersję definicji danej osobowej:

„dana osobowa" oznacza każdą informację, która samodzielnie lub w połączeniu z innymi danymi osobowymi pozwala zidentyfikować tożsamość osoby fizycznej oraz określić jej cechy.

Ta wyliczanka przykładów identyfikatora jest niepotrzebna!

UWAGA 1. O danej osobowej

Po prezentacji zwrócono mi uwagę, że dana osobowa oznacza informację o osobie, a nie to że pozwala zidentyfikować jej tożsamość. Dlatego też skrócona wersja definicji powinna być następująca:

„dana osobowe” oznacza informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Ta definicja (również jej wersja z RODO) oznacza, że mając informację mogącą być daną osobową, a nie mogąc na jej podstawie zidentyfikować osoby do której powinna być ona przypisana, nie możemy jej dalej traktować jako danej osobowej. W takim przypadku wraz z taką daną musimy mieć inną daną osobową identyfikującą taką osobę, a wtedy dopiero możemy tę informację właściwie przypisać do zidentyfikowanej osoby.

Jest to ciekawa konstatacja.

Przetwarzanie

N16	2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
PL16	2) „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Przetwarzanie – „dotknięcie danej”

W wyliczance brakuje takich operacji, jak: *gromadzenie, zapisywanie, konsolidowanie, archiwizowanie, sortowanie, porównywanie, zestawianie, kompresowanie, itd…* -

Proponuję skróconą wersję tej definicji:

„przetwarzanie” oznacza operację lub zbiór operacji wykonywanych na danych osobowych lub zbiorach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany.

System archiwizacji

N16	(6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
PL16	6) „zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Zbiór danych jest złym tutaj tłumaczeniem, gdyż filing system jest systemem archiwizacji zawierającym zbiór plików danych o określonych strukturach zawierających zbiory danych osobowych i ich wzajemnych powiązaniach, stąd definicja ta powinna być następująca:

„system archiwizacji” oznacza dowolny uporządkowany zbiór danych osobowych, dostępnych według określonych kryteriów, niezależnie czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie oraz geograficznie.

Odpowiedzialny administrator

EN16	7) ‘controller’ ..... 8) ‘processor’ ....
PL16	7) „administrator” .... 8) „podmiot przetwarzający” ..

Sprawdzając wersje tej definicji w innych językach – tylko w polskim, bułgarskim, czeskim (správce) angielskie ***controller*** przetłumaczono na *administrator*. Nie zdziwił tłumaczy fakt, że przecież w angielskim istnieje pojęcie *administrator,* a użyto pojęcia *controller.*

Na pytanie dlaczego w wersji angielskiej użyto *controller* - odpowiedź przynoszą tłumaczenia na język niemiecki, francuski, hiszpański czy włoski – gdzie przetłumaczono to jako ***odpowiedzialny.***

Istota RODO

informacje zbierane od i o obywatelu niezbędne do uzasadnionej z nim relacji muszą być chronione, a następnie na jego życzenie usunięte lub przekazane do innego zbioru – dopuszczalne są wyjątki związane z działalnością i bezpieczeństwem Państwa.

[brakuje informacji o karach!]

Nieco informatyki


```
pesel:  string ;                                    /* łańcuch znaków - "51021602057"
pesel : array  [1..11] of char:                     /*tablica znaków - pesel[1]="5",…
pesel : array [enum( rok, mc, dzien, nrkol, płeć, kontr)] of integer ;
                                                    /* tablica z elemetami wyróżnionymi
pesel: record
      rok: word ;
      mc : enum (sty,lut, mar, kwi, maj, cze, lip, się, wrz, paz, lis, gru) ;
      dzien: byte ;
      nrkol: integer ;
      plec: enum (kob, mez);
      kontr: integer ;
end;

pesel: file of byte ;      /*dla zapisania pliku z obrazem numeru pesel w jakimś formacie
```

Co może być daną osobową?

DANA OSOBOWA (wystarczająca)

- Numer PESEL/ZUS
- Numer DO /Paszportu
- Zdjęcie
- Odcisk palca
- DNA/dana biometryczna
- Numer telefonu komórkowego

DANA OSOBOWA (niewystarczająca)

- Nazwisko
- Imię Nazwisko
- Adres (zam., koresp.)
- Adres mejlowy
- Numer telefonu
- Numer IP

Uwagi o identyfikacji wg danej osobowej

Uwaga 1. Przy pojęciu identyfikacji osoby zaznacza się, że taka identyfikacja powinna być łatwa bez ponoszenia specjalnych kosztów. Zawsze przy tym powinno być sprecyzowane dla kogo ma to być łatwe, gdyż w większości przypadków odpowiednie urzędy i służby mogą bardzo łatwo dowiedzieć się kto ma taki numer Pesel, DO, Paszportu, dokumentu ZUSu, rej. pojazdu, itp.

Uwaga 2. Praktycznie dla każdej informacji – danej - konieczne jest uwzględnienie okresu jej ważności. Nazwisko, numer dowodu, paszportu, telefonu, samochodu, adres mejlowy może być zmienione – ba nawet płeć i numer Pesel też. Dlatego też istotnym jest notowanie czasu, kiedy było dokonywana operacja, aby można było potwierdzić jej z zgodność z aktualnymi danymi.

Prawnicy & Informatycy

Pan TI [PRAWNIK] pisze - … *Porównywanie matematycznego świata binarnego z naukami społecznymi, w mojej ocenie nie ma najmniejszego sensu (przynajmniej nie tym językiem, którym się posługujemy obecnie). To co w matematyce można oznaczyć "jest/nie ma" w naukach społecznych, tym bardziej w prawie, nie da się zastosować. Po to każda nauka ma swoje zasady, swoją siatkę pojęć, aby w ramach konkretnej dziedziny rozumieć podobnie znaczenie określonych słów, pojęć.* ***Dla mnie nie ma w prawie "danej osobowej", jest tylko liczba mnoga, bo na podstawie pojedynczej informacji nie da się ustalić tożsamości osoby fizycznej….***

W RODO nie ma informatyka !?

Formalnie zadania tego informatyka, nie nazywając go, opisuje motyw (83) RODO:

W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko [??]. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

UWAGA 2: O szyfrowaniu

- Przywołane w motywie szyfrowanie informatykom niewiele wyjaśnia. O jakim szyfrowaniu jest tu mowa? O prostym typu „Szyfr Cezara”? Raczej nie ze względu na ocenę ryzyka bezpieczeństwa. Wtedy zapewne wchodzą do zastosowania szyfry Algorytmu RSA z kluczami co najmniej 2048 bitowymi.
- Ale pytaniem jest czy rzeczywiście baza danych osobowych zlokalizowana w pamięci serwera musi być zaszyfrowana, gdy jest stale wykorzystywana? A może tylko przesyłanie tych danych lub umieszczenie ich na przenośnym nośniku?
- Tak na marginesie mutacja szyfru Cezara – szyfr Vernama może być lepszym w zastosowaniu.
- I jeszcze jedno – niebawem pojawią się komputery kwantowe i wszystkie te szyfry będą bardzo łatwymi do natychmiastowego złamania.
- Oczywiście, zawsze pojawia się stwierdzenie. Na ile ktoś chce dostać się do takich zaszyfrowanych danych osobowych, że jest w stanie poświęcić znaczące środki na złamanie szyfru.
- W praktyce to się rzadko zdarza. A ci których na to stać – środków nie liczą.

Jak informatyk ma pomóc administratorowi?

Z Artykułu 25 RODO:

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

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 wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

UWAGA 3: Security & Privacy by design

- Słuchając prezentacji o Privacy by design oraz o bezpieczeństwie systemów teleinformatycznych zdecydowanie stwierdzam, że powinniśmy dać sobie spokój z wdrażaniem Privacy by design, a tylko skupić się na Security by design.
- Oczywiście poprawne zaprojektowanie i implementacja systemu maksymalnie niezawodnego i odpornego na nieuprawnione ingerencje – bezpiecznego, zapewni również odpowiednią ochronę danych osobowych.
- Pełna realizacja wymagań Security by design (w tym Privacy by design) może być wykonana tylko w nowo-projektowanych systemach. W systemach już eksploatowanych można dokonać tylko pewnych poprawek, dokładając warstwę ochronną (programy antywirusowe, weryfikacje dostępu, firewalle, aktualizację oprogramowania, itp.).
- Innymi słowami informatycy mają zapewnioną pracę na najbliższe lata. Wymiana systemów będzie postępować w miarę ujawnianych cyber-ataków.

UWAGA 4: Prawa dla Informatyków

- GDPR/RODO wprowadzając ostrzejsze warunki na zapewnienie ochrony danych osobowych przez odpowiedzialnych (administratorów) za te dane, równocześnie nakłada na przetwarzających (de'facto informatyków) ogromną odpowiedzialność potwierdzoną wysokimi karami finansowymi.
- GDPR/RODO w ogóle nie interesuje się tymi co kradną te dane. Nie zamierza też ich wykrywać i karać – stwierdzono bowiem że jest to bardzo trudne i często niemożliwe. Łatwiej jest ustalić i ukarać tych, którzy „niedopilnowali" i dali sobie ukraść te dane, a nawet dopuścili tylko do wycieku.
- GDPR/RODO nakładając te obowiązku również na informatyków, nie daje im żadnych praw mogących wesprzeć ich działania. A niestety oprócz możliwości eksploatacji systemów, które nie są odpowiednio przygotowane do działania (są „dziurawe"), stając otwartymi dla przestępców, istnieją też możliwości złamania dostępu poprzez szantaż administratora systemu, aby ten sam skopiował wskazane dane. W obu tych przypadkach informatycy (administratorzy systemu) mają małe szanse zapewnienia sobie formalnego wsparcia swoich przeciwdziałań takim praktykom.
- I dlatego proponuję poniższy zestaw praw (jest to niestety tylko propozycja do realizacji, ale w części mogą być wpisane do umowy pomiędzy administratorem danych a podmiotem przetwarzającym).

Prawa dla Informatyków - podstawowe

Prawa te mogą być na przykład sformułowane następująco – prawo do:

- samodzielnego podjęcia decyzji o wyłączeniu systemu lub podobnych działaniach, gdy istnieje zagrożenie wycieku danych,
- uzależnienia dalszej eksploatacji systemu od uzupełnienia go o określony sprzęt, oprogramowanie, aplikację, itp. mające wzmocnić ochronę przed wyciekiem danych osobowych,
- ograniczenia lub wyznaczenia grupy osób mających dostęp do określonych funkcji lub pomieszczeń systemu,
- odmowy wykonania operacji mogących prowadzić do pobrania danych osobowych poza zdefiniowanymi i zatwierdzonymi procedurami (w tym również dotyczącymi pobrań przez uprawnione służby),

Prawa dla informatyków – ich chroniące

Stąd propozycja dodatkowych praw chroniących interesy informatyków:

- ochrony swoich danych personalnych (korzystanie z pseudonimu) w relacjach z częścią pracowników czy też zewnętrznych klientów dla unikania możliwości szantażowania tych osób,
- ochrony swojej osoby oraz rodziny w sytuacji zagrożenia fizycznego spowodowanego szantażem lub innymi działaniami związanymi z uzyskaniem nieuprawnionego dostępu do danych obsługiwanego systemu,
- pomocy prawnej (płatnej przez zakład pracy) w przypadku prawnego rozstrzygania stopnia winy zakładu i zatrudnionych w nim informatyków mogących być odpowiedzialnych za wyciek danych, gdyż z reguły będą to złożone prawnie postępowania o znaczących kwotach odszkodowawczych.
- możliwość ubezpieczenia się

Podziękowanie dla UODO
Podziękowanie dla słuchaczy
Wacław Iszkowski

Treść tej prezentacji jest opisana w esejach na witrynie:

www.iszkowski.eu/rodo