Z dziennika tłumaczki. Rozważania o RODO

Odcinek 9 - Analiza stanu obecnego

Poniedziałek 21 maja 2018 r. - Zostały 4 dni do RODO

Drogi Dzienniku!

Zastanawiam się, kiedy do Międzynarodowej Klasyfikacji Chorób zostanie dopisana nowa jednostka chorobowa: RODOza. Albo może ostre zapalenie wyrostka RODOwego. Objawy: napady paniki, RODOwstręt, nadmierna pobudliwość i hiperaktywność związane ze zbliżającym się terminem 25 maja. ;-)

Ja już mam lekarstwo na tę przypadłość. Tabletka. O przepraszam, **tabelka**. Tak, obiecana tabelka. Tym razem nieco większy egzemplarz - porządny plik w excelu.
Już Ci pokazuję. Tu masz link. Ale uwaga - to wersja robocza. Chciałabym ją jeszcze skonsultować z koleżankami i kolegami po fachu, żeby sprawdzić, czy niczego nie przeoczyłam.

Ten plik to próba uporządkowania i udokumentowania tego, co się dzieje z danymi osobowymi w ramach mojej działalności. Docelowo ma też zawierać **dokumentację**, która pokazuje, jakie kroki podjęłam, żeby dostosować moją działalność do wymogów rozporządzenia. A jeżeli nie zdążę zrobić wszystkiego do 25 maja, to też jakie kroki zamierzam podjąć w najbliższej przyszłości.

Dlaczego tworzę taką dokumentację? Przypominam Ci **zasadę rozliczalności**, którą omówiłam w załączniku z głównymi założeniami:

> *Art. 5 Zasady dotyczące przetwarzania danych osobowych*
> *2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i* ***musi być w stanie wykazać ich przestrzeganie*** *(„rozliczalność”).*

Nie tylko muszę dostosować swoją działalność do zasad rozporządzenia, ale też muszę być w stanie wykazać, że przestrzegam tych wszystkich zasad oraz że wdrożyłam odpowiednie środki organizacyjne i techniczne. Czyli ta dokumentacja nie tylko służy moim potrzebom wewnętrznym, ale też jest pewnego rodzaju **zabezpieczeniem w przypadku kontroli**.

Jeżeli jestem administratorem, to wdrożenie odpowiednich środków technicznych i organizacyjnych jest moim obowiązkiem. To wynika m.in. z art. 24.1.

> *Artykuł 24 - Obowiązki administratora*
> *1. **Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia**, **administrator wdraża odpowiednie środki techniczne i organizacyjne**, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te **są w razie potrzeby poddawane przeglądom i uaktualniane**.*
> *2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich **polityk ochrony danych**.*
> *3. Stosowanie zatwierdzonych **kodeksów postępowania**, o których mowa w art. 40, lub zatwierdzonego **mechanizmu certyfikacji**, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.*

Zgodnie z ust. 1 jako administrator muszę wdrożyć środki techniczne i organizacyjne, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Podstawą podjęcia konkretnych działań będzie więc analiza tych poszczególnych elementów, czyli konkretnie **analiza stanu obecnego**. To będzie pierwszy element mojej dokumentacji.

Czy moja dokumentacja to pełna polityka ochrony danych osobowych, o której mowa w ust. 2? Trudno powiedzieć. Rozporządzenie nie daje twardych wytycznych, co do zakresu czy formy takiej polityki ochrony danych osobowych, ani też nie wskazuje kryteriów bądź sytuacji, kiedy wdrożenie takiej polityki jest wymagane. Każdy musi ocenić we własnym zakresie. Ale można powiedzieć, że mój plik to coś w rodzaju „minipolityki” ochrony danych osobowych.

W ust. 3 jest też mowa o kodeksach postępowania i mechanizmach certyfikacji. W tej chwili takich dokumentów dla branży tłumaczeniowej nie ma. Gdyby istniały, to wskazywałyby już bardziej konkretne rozwiązania, które można by wprowadzić, aby działać zgodnie z rozporządzeniem. Ale ich nie ma i nie wiemy, czy i kiedy będą. **Na razie więc każdy musi się dostosować we własnym zakresie i szukać zaleceń w różnych źródłach**. Niestety, powoduje to, że powstaje miszmasz, każdy robi co innego i każdy też co innego doradza.

Ja stwierdziłam, że na razie przygotuję **niezbędne minimum**. Nie będę tworzyć obszernej dokumentacji, która potem może się okazać niepotrzebna, albo nie do końca zgodna z zaleceniami kodeksów czy mechanizmów certyfikacji. Niech będzie praktycznie i do rzeczy.

No właśnie. Zajrzyjmy teraz do załączonego pliku. Zawiera on kilka arkuszy. Pierwszy arkusz to wykaz poszczególnych części dokumentacji. Jest tam też informacja o ostatniej aktualizacji. W wyżej cytowanym artykule jest przecież mowa o tym, że:

> *Artykuł 24 - Obowiązki administratora*
> *1. (...) Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.*

Rozporządzenie nakłada na mnie obowiązek okresowego sprawdzenia, czy moje procedury są odpowiednie i w razie potrzeby zaleca ich aktualizację. **Co roku** przejrzę więc dokumentację i sprawdzę, czy wszystko się zgadza, a jakby się coś zmieniło w ciągu roku, to też zapiszę. Jeżeli pewnych rzeczy nie zdążę zrobić do 25 maja albo coś okaże się niewystarczające, to też będę to **stopniowo aktualizować**.

Drugi arkusz „Firma" zawiera dane mojej firmy i krótki opis mojej działalności. Tyle ;-)
Przejdźmy do trzeciego arkusza „Zbiory_procesy". Nie przestrasz się, na pierwszy rzut oka wygląda to okropnie.
To jest tabelka prezentująca moją sytuację: jestem tłumaczem przysięgłym, prowadzę biuro, mam sekretarkę, podzlecam od czasu do czasu tłumaczenia czy korekty, przyjmuję zlecenia nie tylko od biur tłumaczeń i organów wymiaru sprawiedliwości, ale także klientów indywidualnych, którzy przychodzą do biura. To tak w skrócie.

Inni tłumacze może mają swoją działalność zorganizowaną inaczej, ale pewnie wiele elementów jest wspólnych. Każdy jednak musi dostosować dokumentację do charakterystyki swojej sytuacji. Lista czynności może być dłuższa, krótsza, w innej kolejności itd.

Jak zauważyłeś, mam tutaj nie tylko opis zbiorów danych osobowych, ale także opis procesu przetwarzania danych osobowych - od momentu, kiedy wchodzą one w moje posiadanie, do momentu, kiedy je trwale usunę. Jest to bardzo istotne, bo filozofia rozporządzenia skupia się nie na zbiorach, tylko na procesach: co dokładnie z tymi danymi robimy, jak je przetwarzamy.

Pierwsza kolumna zawiera więc opis poszczególnych etapów i czynności, podczas których przetwarzam dane osobowe. Od momentu zapytania po wykonanie tłumaczenia, rozliczenie z klientem i archiwizację.
Druga kolumna wskazuje zbiory danych, a trzecia miejsce ich przechowywania. To miejsce się zmienia na każdym etapie procesu przetwarzania.

Widzisz też, że podzieliłam np. skrzynkę pocztową na różne zbiory, m.in. wg rodzaju zleceniodawcy i wg stanu obsługi zapytania/zlecenia. Będzie to ważne ze względu na dalsze kolumny: moja rola (administrator/podmiot przetwarzający), okres przechowywania, cel, podstawa prawna itd. Tak samo zrobiłam ze zbiorem bieżących zleceń.
Wychodzi bardzo szczegółowa tabela, ale mam nadzieję, że obejmuje ona wszystkie rodzaje danych osobowych, z którymi mam do czynienia w mojej działalności i wszystkie procesy ich przetwarzania. Jak mi coś jeszcze wpadnie do głowy, to uzupełnię.

Pytasz, **dlaczego tak szczegółowo opisałam korespondencję mailową**? No właśnie. Różne wiadomości i ich załączniki mają różne okresy przechowywania. Jak nie zacznę oddzielać zapytań od zleceń potwierdzonych, to powstanie problem z usuwaniem wiadomości ze zleceniami, których nie przyjęłam. Nieprzyjętych zleceń nie będę mogła przechowywać tak długo jak przyjętych, bo nie będę miała do tego podstawy prawnej. Na razie wpisałam miesięczny okres przechowywania, więc pod koniec następnego miesiąca po prostu zamierzam usunąć wszystkie przeterminowane wiadomości w folderze Zapytania. Muszę też dopilnować, żeby przenosić wiadomości wysłane do odpowiedniego folderu. Jak już tłumaczenie jest potwierdzone, to przeniosę je do potwierdzonych, podzielonych z kolei na trzy rodzaje klientów. Niezła zabawa, prawda? Zobaczymy, czy to pomoże mi pilnować terminów usunięcia. Nie wyobrażam sobie, że będę ciągle musiała przeglądać całą skrzynkę, żeby usuwać przeterminowane maile. Jeżeli są już uporządkowane w folderach, wystarczyć skasować maile w danym folderze.

No i cóż mogę jeszcze dodać. W ostatnich dniach rozpisałam wszystko, co wiem na temat tych poszczególnych rubryk. I teraz je wypełnię wg mojej najlepszej wiedzy. Po kolei miejsce przechowywania, okres przechowywania, moja rola (administrator/podmiot przetwarzający), cel i powiązana z celem podstawa prawna oraz komu udostępniam dane. Świetne ćwiczenie podsumowujące ;-).

Arkusz „Zbiory_procesy" z analizą stanu faktycznego jest podstawą do dalszych działań, takich jak spełnienie obowiązku informacyjnego, wdrożenie środków organizacyjnych i technicznych, analiza ryzyka i ustalenie, kiedy potrzebna jest umowa powierzenia.
Jak widzisz, do każdego z tych działań jest w pliku odpowiedni arkusz:

- Arkusz *Info*: opis, w jaki sposób zamierzam spełnić obowiązek informacyjny i obsługiwać zapytania dot. przetwarzanych danych osobowych
- Arkusz *Powierzenie*: lista osób czy jednostek, którym powierzam przetwarzanie danych osobowych
- Arkusz *Upoważnienie*: lista osób upoważnionych przeze mnie do przetwarzania danych osobowych
- Arkusz *Ryzyko:* zagadnienia związane z analizą ryzyka
- Arkusz *Środki techniczne i organizacyjne*: środki, które już zostały wdrożone i których wdrożenie jest planowane
- Arkusz *Naruszenia*: zwięzła procedura zgłaszania naruszeń (oby nie była potrzebna, ale coś powinno być ...)

W następnych dniach napiszę Ci więcej o zadaniach związanych z tymi poszczególnymi tematami i uzupełnię arkusze.

Jeszcze jedna uwaga. **Proszę, nie myl tego pliku z dokumentacją z rejestrem czynności przetwarzania danych osobowych ani z polityką prywatności**. O rejestrze czynności napiszę Ci za kilka dni. O polityce prywatności pewnie jutro, kiedy omówię obowiązek informacyjny.

Czy to tyle na dzisiaj? Hmm, zastanawiam się, czy przypadkiem czegoś w tym pliku nie przeoczyłam. Jak mi się coś jeszcze przypomni, to go uzupełnię. Może eksperci jeszcze coś podpowiedzą? Najważniejsze, że jestem w stanie wykazać, że dokładam wszelkich starań, aby pracować zgodnie z RODO. Dużo rzeczy wyjdzie w praniu, kiedy powstaną standardowe rozwiązania, mechanizmy certyfikacji i kodeksy.

Posiadanie takiej dokumentacji jest ważne. Będzie on nie tylko podkładką w przypadku kontroli, ale także będę mogła ją przedstawić, gdy administrator zażąda ode mnie gwarancji przestrzegania przepisów w zakresie ochrony danych osobowych. Administrator bowiem powinien wybrać taki podmiot przetwarzający, który zapewnia przestrzeganie wymogów RODO:

> *Artykuł 28 - Podmiot przetwarzający*
> *1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora,* ***korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych****, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.*

Póki nie ma mechanizmów certyfikacji ani kodeksów stosowna dokumentacja może być taką gwarancją. Dobrze jest włożyć trochę wysiłku, aby zawierała ona odpowiednie informacje. Poza tym nie zamierzam podpisywać z klientami umów powierzenia, jeżeli nie jestem odpowiednio przygotowana do tego, żeby spełnić wymagania klienta w zakresie ochrony danych osobowych. Moje przygotowania na pewno się przydadzą, kiedy zgłosi się do mnie taki wymagający klient.

Ale teraz naprawdę już dosyć na dzisiaj. Do jutra!

Twoja Tłumaczka