Z dziennika tłumaczki. Rozważania o RODO

Odcinek 14 - środki techniczne i organizacyjne

Środa 30 maja 2018 r. - 5 dni po RODO

Drogi Dzienniku!

Wczoraj była mowa o ryzyku. W trzynastym odcinku o RODO. Czy pechowym? Nieee… Ja nie jestem przesądna. Nie wiem, jak Ty. :)

Ryzyko ryzykiem, wdrożę odpowiednie środki organizacyjne i techniczne i powinnam mieć ryzyko pod kontrolą. Hmmm, przynajmniej w miarę… Nigdy nie wiadomo, co się wydarzy. A na razie nikt nie jest w stanie podać mi pełnej listy odpowiednich środków bezpieczeństwa. Zajrzę do rozporządzenia i sprawdzę, co tam jest napisane o tych środkach technicznych i organizacyjnych.

Artykuł 25 wymaga ich od administratora:

> *Artykuł 25 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.*
> *2. 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.*
> *3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.*

I artykuł 28 od podmiotu przetwarzającego:

> *Artykuł 28 Podmiot przetwarzający*
> *3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy (...) Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:*
> *f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;*

Tutaj jest odwołanie do artykułu 32-36. Szczególnie artykuł 32 mnie interesuje, bo omawia bezpieczeństwo:

> *Artykuł 32 Bezpieczeństwo przetwarzania*
> *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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:*
> *a) pseudonimizację i szyfrowanie danych osobowych;*
> *b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*
> *c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*
> *d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*
> *2.Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.*
> *3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.*

I artykuł 32 też mówi o osobie działającej z upoważnienia:

> *Artykuł 32 Bezpieczeństwo przetwarzania*
> *4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.*

Czyli to administrator ma podjąć działania, abym ja, jako osoba upoważniona, przetwarzała dane osobowe zgodnie z rozporządzeniem? Jednak w praktyce, moim zdaniem, sama będę za to odpowiedzialna i sama będę musiała wdrożyć odpowiednie środki techniczne i organizacyjne. Jeżeli w ogóle będę przetwarzała dane osobowe na podstawie upoważnienia, na przykład dla organów wymiaru sprawiedliwości. Na razie Ministerstwo nie zajęło stanowiska w tej sprawie. Ale nie wyobrażam sobie, żeby specjalny wysłannik OWS przychodził sprawdzić u mnie w biurze, czy mam wszystko zorganizowane, jak trzeba.

Zauważyłeś, że w artykule 32 jest znowu mowa o kodeksach postępowania i mechanizmach certyfikacji? Będą konkretne wytyczne, co trzeba zrobić, żeby dostać taki certyfikat zgodności z RODO. Oby tylko te wytyczne mieściły się w granicach rozsądku.

Na razie muszę radzić sobie sama. Oto mój plan działania.
Nie jestem informatykiem, nie jestem specem od bezpieczeństwa technicznego czy organizacyjnego. To co piszę, to podsumowanie wszystkich zaleceń, które otrzymałam w ostatnich miesiącach plus dawka zdrowego rozsądku. Pewne zasady już od dawna stosuję, ale muszę je wpisać do dokumentacji, więc są na liście. Nowe zasady i rozwiązania wdrożę i też wpiszę do dokumentacji, niektóre jako „planowane”. Jeżeli ktoś mi coś jeszcze podpowie, uzupełnię dokumentację.

W tej chwili najważniejsze to wyrobienie odpowiednich nawyków i dyscyplina.

Dane osobowe na nośnikach papierowych - środki organizacyjne i techniczne

- Strefa biurowa jest odpowiednio wydzielona i oznaczona: u mnie jest to o tyle proste, że mam wydzielone pomieszczenie biurowe w domu, więc mogę je zamknąć. Pewnie niektórym tłumaczom pracującym przy stole kuchennym będzie trudniej ;-(.
- Stosuję zasadę „czystego biurka”: gdy nie ma mnie w biurze, żadne ważne dokumenty, w szczególności te zawierające dane osobowe, nie znajdują się na biurku czy w zasięgu ręki.
- Klienci nie mają wglądu w dokumenty, które leżą na biurku.
- Dokładnie sprawdzam, czy dokumenty zawierające dane osobowe są wydawane osobom upoważnionym. Nie mogę dopuścić do żadnych pomyłek przy wydawaniu dokumentów.
- Dbam o to, by przesyłki zawierające dokumenty z danymi osobowymi były bezpiecznie dostarczane do urzędu pocztowego.
- Poza godzinami pracy wszystkie ważne dokumenty, w tym dokumenty zawierające dane osobowe, są chowane w szafie zamykanej na klucz/sejfie.
    - Szafa na klucz/sejf: w tej chwili mam szafkę na klucz, ale chyba nie jest to całkiem bezpieczne miejsce na dokumenty zawierające dane wrażliwe. Już od dawna rozważam zakup małego sejfu, niekoniecznie ze względu na RODO, więc teraz mam dobrą motywację, żeby w końcu go kupić. Szafka będzie na mniej wrażliwe dokumenty, które jednak powinny być przechowywane pod kluczem.

- W miarę możliwości będę skanować wszystkie dokumenty źródłowe otrzymane od klienta i niezwłocznie oddawać mu oryginały.
- Niszczę niepotrzebne dokumenty za pomocą niszczarki odpowiedniej klasy.
    - Niszczarka: dawno planowany zakup, ale trzeba się w końcu zmobilizować. Tak jak pisałam, teraz palę wszystkie niepotrzebne papierki w piecu.

Dane osobowe na nośnikach elektronicznych - środki organizacyjne i techniczne

- Komputery:
    - Stosuję zasadę „czystego ekranu”: kiedy nie ma mnie w biurze, nikt nie zagląda do mojego komputera. Wyloguję się za każdym razem, kiedy zostawiam komputer bez opieki.
    - Klienci nie mają wglądu w to, co jest wyświetlane na ekranie mojego komputera.
    - Dzieci mają bezwzględny zakaz zbliżania się do mojego komputera, a oprócz tego nie znają hasła do logowania.
    - Korzystam z odpowiedniego programu antywirusowego.
    - Zaszyfrowałam twardy dysk komputera: daje to pewność, że dane nie dostaną się w niepowołane ręce, nawet jeżeli ktoś ukradnie mi komputer.
- Serwer (mam domowy serwer stacjonarny):
    - Osoby nieupoważnione (w tym moje dzieci) mają zakaz dostępu do serwera albo jego wydzielonej partycji.
    - Serwer jest odpowiednio zabezpieczony przed dostępem osób nieupoważnionych.
    - Zdalny dostęp do serwera jest odpowiednio zabezpieczony: to zadanie dla informatyka.
    - Regularnie wykonuję kopię zapasową wszystkich danych przechowywanych na serwerze.
- Urządzenia mobilne:
    - Telefon komórkowy: haha, przyznam, że jestem starej daty i nie mam smartfona! To akurat plus w przypadku dostosowania do RODO ;-) Pewnie kupię w najbliższej przyszłości, trzeba będzie go zabezpieczyć, jeżeli zechcę np. sprawdzać pocztę na telefonie. Nie zapisuję numerów klientów pod imieniem i nazwiskiem (pseudonimizuję albo używam nazwy firmy).
    - Tablet: jak wyżej.
    - Dzieci nie mają dostępu do moich urządzeń mobilnych, jeżeli używam ich do celów firmowych (oj oj, pewnie będzie z tym ciężko, gdy w końcu się zdecyduję na ten smartfon).
    - Odpowiednio zaszyfrowałam pamięci USB i przenośne dyski twarde.
- Oprogramowania:
    - Zadbam o to, by na wszystkich urządzeniach oprogramowanie było na bieżąco aktualizowane.
    - Będę z ostrożnością korzystać z bezpłatnego oprogramowania.
    - Nie używam nielegalnego oprogramowania.

- Kopia zapasowa:
    - Regularnie wykonuję kopię zapasową wszystkich dokumentów, które standardowo trzymam na serwerze domowym. Robię bieżącą, lustrzaną kopię na komputerze, na którym pracuję, oraz regularnie kopię zapasową na dysku zewnętrznym, który przechowuję w bezpiecznym miejscu. Poproszę informatyka, aby mi doradził, jak sprawnie robić kopie zapasowe.
- Szyfrowanie:
    - Komputery, serwer i wszystkie nośniki danych są szyfrowane: wolę to zadanie zostawić informatykowi, niech on to zrobi dobrze. Pewnie ktoś bardziej zorientowany zrobiłby to sam, ale ja nie jestem asem informatycznym ;-).
    - Nauczę się sprawnie szyfrować dokumenty (w szczególności załączniki do poczty elektronicznej), zainstaluję odpowiednie oprogramowanie i udostępnię klucz publiczny do szyfrowania, za pomocą którego klient będzie mógł szyfrować pliki przed wysłaniem do mnie.
    - Jeżeli klient prześle mi pliki zawierające wrażliwe dane osobowe bez szyfrowania, uczulam na ryzyko i odsyłam pliki z tłumaczeniem w formie szyfrowanej tylko na jego wyraźnie żądanie.
- Hasła:
    - Wszystkie hasła są odpowiednio mocne.
    - Przechowuję wszystkie hasła za pomocą aplikacji typu KeePass, co pozwoli ograniczyć liczbę haseł do zapamiętania (czyli już nie w zeszycie ;-)).
    - Okresowo zmieniam hasła: co to znaczy okresowo? Z lenistwa w ogóle nie zmieniam haseł (czerwienię się). I chyba nie tylko ja jestem taka leniwa… Trzeba się zdyscyplinować!
- Poczta elektroniczna:
    - Korzystam tylko ze skrzynek pocztowych, które przechowują pocztę na serwerze w Unii Europejskiej i bez mojej wiedzy nie przekierowują poczty poza UE (przyznam, że nie wiem, jak to sprawdzić, ale się dowiem).
    - Jeżeli klient zażąda ode mnie przesłania plików w formacie szyfrowanym, to tak zrobię. Jeżeli nie zażąda, to jego problem, bo on jest administratorem i powinien oceniać poziom ryzyka. Ale uczulam na ryzyko.
    - Do podwykonawców przesyłam pliki zawierające dane osobowe i inne wrażliwe informacje tylko w formie zaszyfrowanego załącznika. W miarę możliwości ograniczam przesyłanie takich plików i anonimizuję je przed udostępnianiem innym.
- Chmura:
    - Korzystam tylko z takich rozwiązań w chmurze, które zapewniają zgodność z RODO. Nie korzystam z bezpłatnych usług przechowywania dokumentów w chmurze, typu google dysk.
    - Nie korzystam z bezpłatnych czy niezabezpieczonych rozwiązań do przesyłania dużych plików typu Dropbox albo serwerów ftp. Jeżeli klient stosuje takie praktyki, uczulam na ryzyko i korzystam z takich rozwiązań tylko na jego wyraźnie żądanie.
- Router i biurowa sieć bezprzewodowa:
    - Dopilnuję, aby sieć biurowa (czyli domowa) była odpowiednio zabezpieczona, a komputery biurowe były widoczne tylko dla osób upoważnionych: to zadanie dla informatyka.

- UPS (nie, nie chodzi o firmę kurierską, tylko o *uninterruptible power supply,* takie zasilanie awaryjne, jakby duża bateria): mam takie urządzenie, ponieważ u nas często występują braki w dostawie prądu i wtedy ten sprzęt zapewnia zasilanie urządzeń biurowych i routera przez kilkanaście, a nawet kilkadziesiąt minut. UPS w pewnym stopniu zabezpiecza też przed przepięciami w sieci, np. wskutek uderzenia pioruna. W świetle RODO jest to forma zabezpieczenia przed utratą danych. Akurat mam, więc dopiszę do stosowanych środków technicznych.
- Serwisowanie sprzętu - upoważnienie/powierzenie:
    - Tylko upoważniona osoba może mieć dostęp do sprzętu: muszę podpisać upoważnienie albo umowę powierzenia z informatykiem. On nie musi mieć wglądu w dokumenty z danymi osobowymi, ale będzie miał do nich fizyczny dostęp.

Pseudonimizacja

Tłumacz stosuje pseudonimizację w przypadku:

- danych osobowych zleceniodawcy: dane osobowe zleceniodawcy są jedynie wykorzystane
    - w korespondencji ze zleceniodawcą,
    - w dokumentacji rachunkowej,
    - w repertorium,
    - w rejestrze zleceń.

  W przypadku oznaczania materiałów przekazywanych do tłumaczenia dane osobowe (imię i nazwisko) zastępowane są numerem zlecenia.
- przekazywania materiałów źródłowych podwykonawcom, o ile jest to możliwe, biorąc pod uwagę to, jaką usługę ma wykonać podwykonawca;
- tłumaczenia za pomocą narzędzi CAT: pseudonimizacja przed załadowaniem plików źródłowych do narzędzi CAT.

Pozostałe środki organizacyjne

Tak naprawdę zasady obsługi zleceń w dużej mierze są już rozpisane w pliku z dokumentacją. Wiem już:

- według jakiego procesu odbywa się obsługa zlecenia,
- gdzie dokumenty są przechowywane,
- w jaki sposób spełniam obowiązek informacyjny,
- jak udokumentować podstawę prawną:
    - podpisuję umowę o świadczenie usług tłumaczeniowych i powierzenia ze zleceniodawcą,
    - podpisuję umowę powierzenia z podwykonawcą,
    - daję upoważnienie sekretarce;
- kto oprócz mnie ma dostęp do danych: tylko osoby upoważnione
    - moja sekretarka;

Pozostaje jeszcze opisać:

- procedurę zgłaszania naruszenia.

To jest taki wstępny plan. I tak niezła rozpiska z tego wyszła. Pewnie można o wiele więcej, ale nie dajmy się zwariować.

Na początku w arkuszu ze środkami organizacyjnymi i technicznymi jeszcze dopiszę zgodnie z art. 32:

Poniższe środki techniczne i organizacyjne zostały wdrożone, 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, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
Środki te zapewniają:

- *zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*
- *zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*

Rozwiązania są regularnie testowanie, mierzone i oceniane.

Wow, chyba przebrnęłam przez najważniejsze tematy związane z RODO. Może wszystko jeszcze nie do końca jest idealne, ale to już solidna podstawa. Teraz muszę to zastosować w życiu. I w praniu pewnie wyjdą jakieś poprawki. Wczoraj trzy razy przeredagowywałam moją formułkę do wiadomości elektronicznych...

Mam szczerą nadzieję, że powstanie prawdziwy poradnik albo jeszcze lepiej kodeks postępowania dla tłumaczy. W tej chwili każdy robi to, co uważa za słuszne. Może z czasem na tej podstawie zostaną opracowane dobre praktyki i zalecenia, zasady współpracy się ujednolicą i za pięć lat będziemy się śmiali, że daliśmy się tak zwariować przez to całe rozporządzenie. Ale to dopiero za pięć lat. Teraz muszę się przyzwyczaić do nowej rzeczywistości. Pewnie jeszcze wiele razy będę Ci pisać o RODO.

Ale już nie w tym tygodniu. Jadę na zasłużony odpoczynek: szkolenie!!! Nie mogę się doczekać ;-).

Do przeczytania wkrótce!

Twoja Tłumaczka