Z dziennika tłumaczki. Rozważania o RODO

Odcinek 15 - zgłoszenie naruszenia

Piątek 9 listopada 2018 r. – RODO jest z nami od pięciu miesięcy

Drogi Dzienniku!

Ale ten czas leci… Dopiero był koniec maja, a już minęły wakacje i dawno wróciliśmy do „normalnego" trybu pracy.

Jak tam u mnie z tym RODO? Powiem Ci, że mimo moich najlepszych chęci dalej nie wszystko jest tak, jak bym chciała.

Na pewno mam już jednak zaliczone kilka punktów:

- komputery zaszyfrowane;
- w skrzynce mailowej porządek;
- podstawowa dokumentacja z zestawieniem procesów i analizą ryzyka przygotowana;
- koncepcja z połączonym rejestrem czynności wdrożona i sprawdza się dobrze w moich warunkach pracy.

Z sekretarką mamy wyrobioną rutynę obsługi klientów. Każdy klient indywidualny, który przychodzi do biura, podpisuje jednostronicową umowę świadczenia usługi tłumaczeniowej i powierzenia przetwarzania danych. Jako załącznik daję klientowi warunki ogólne, które bardziej szczegółowo opisują zasady świadczenia usługi i przetwarzania danych. Nikt do tej pory nie marudził, że nie chce podpisywać (ale też nikt nie przeczytał [przy mnie] 10 stron warunków…).
Gorzej z biurami tłumaczeń: dostałam kilka umów powierzenia, których nie podpisałam, ponieważ mam wątpliwości co do pewnych ich postanowień… Za to już kilka razy wysłałam wraz z odpowiedzią na zapytanie moją standardową umowę z warunkami ogólnymi i bez problemu dostałam ich potwierdzenie.

Dziwi mnie jednak, że tak wiele biur dalej przesyła bez żadnych skrupułów dokumenty zawierające wrażliwe dane osobowe, nie dbając o odpowiednie formalności czy zabezpieczenia. I to do nieokreślonej liczby odbiorców… Jednak powinna się zapalać jakaś czerwona lampka, nawet jeżeli nie bardzo się przyjmujemy tym RODO. No cóż, dopiero jak będzie pierwsza wpadka wszyscy staną na baczność.

Co zostało mi jeszcze do zrobienia?
Na pewno opracowanie procedur:

- zgłoszenia naruszenia;
- odpowiedzi na żądanie osoby, której dane dotyczą.

W ostatnich dniach zagłębiłam się trochę w ten pierwszy temat i przygotowałam odpowiednie dokumenty wzorcowe.

Przypominam Ci, że zgodnie z artykułem 33 RODO zarówno jako administrator, jak i podmiot przetwarzający mamy obowiązek zgłosić naruszenia ochrony danych osobowych:

> *Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu*
> *1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.*
> *2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.*

Ale pierwsze pytanie brzmi: co stanowi naruszenie?
Muszę rozróżnić dwa rodzaje naruszenia:

- naruszenie ochrony danych;
- naruszenie praw i wolności osób fizycznych.

Zgodnie z tym artykułem zgłaszam naruszenie ochrony danych tylko jeżeli skutkuje ono ryzykiem naruszenia praw i wolności osób fizycznych. Krótko mówiąc, tylko wtedy, kiedy może ono komuś zaszkodzić. To, co należy przez to rozumieć, jest bardziej szczegółowo omówione w motywie 75 rozporządzenia:

> *Motyw (75) Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:*
>
> - *jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa;*
> - *jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji*

ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;
- *lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.*

Bardzo szeroki zakres…

Drugi aspekt to naruszenia zasad ochrony danych osobowych bezpośrednio wynikających z rozporządzenia. W szczególności chodzi o:
- Naruszenie poufności: dane osobowe zostaną udostępnione osobom nieupoważnionym;
- Naruszenie dostępności: dane osobowe są z różnych powodów niedostępne w odpowiednim momencie;
- Naruszenie integralności: dane osobowe zostały zmienione, zniszczone, utracone, skradzione.

Wyobraźmy sobie teraz przykładową sytuację, w której dochodzi do naruszenia zasad bezpieczeństwa: ktoś mi ukradł komputer.
Zastanówmy się, czy to jest:
- Naruszenie poufności: jeżeli komputer jest odpowiednio zaszyfrowany, złodziej lub jakakolwiek inna osoba nie uzyska dostępu do danych osobowych;
- Naruszenie dostępności: jeżeli regularnie robię kopię zapasową, to nie doszło do naruszenia dostępności, ponieważ mogę odzyskać wszystkie dane osobowe z kopii zapasowej;
- Naruszenie integralności: złodziej nie będzie miał możliwości wprowadzenia zmian do danych osobowych lub uszkodzenia danych, bo nie ma do nich dostępu.

Wniosek: nie było naruszenia zasad bezpieczeństwa, ale tylko i wyłącznie dlatego, że stosowałam odpowiednie środki bezpieczeństwa.
Drugi wniosek: warto szyfrować komputer i regularnie robić kopie zapasowe!

A jeśli komputer nie był szyfrowany i nie mam kopii zapasowej? No to jest problem. Jest to naruszenie wszystkich trzech zasad…
Następne pytanie: czy to naruszenie skutkuje naruszeniem praw i wolności?
To wszystko zależy od tego, co miałam na tym komputerze. Wyroki sądowe, akta prokuratorskie, dane wrażliwe w dokumentacji medycznej... Tutaj bez wielkich wątpliwości powiedziałabym, że to podpada pod obowiązek zgłoszenia, bo ryzyko jest duże.
W tym momencie znowu muszę oceniać ryzyko, tak jak zrobiłam to przy analizie. Jeśli więc oznaczyłam w analizie pewne kategorie dokumentów wysokim ryzykiem, a dokumenty te były na komputerze, to w przypadku naruszenia powyższych trzech zasad bezpieczeństwa „technicznego” zgłoszenie będzie nieuniknione.

Jeżeli mimo wszelkich moich starań dojdzie (odpukać) do naruszenia ochrony danych osobowych, muszę postąpić zgodnie z artykułem 33.

Najpierw sprawdźmy, co administrator musi zgłosić. Przypominam, że dane osobowe, które przetwarzamy jako administrator, raczej nie powodują ryzyka naruszenia praw i wolności osób fizycznych w przypadku naruszenia zasad bezpieczeństwa.

Jeszcze raz artykuł 33

> *Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu*
> *1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki –w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia –zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.*
> *[…]*
> *3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:*
> *a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;*
> *b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;*
> *c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych; d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.*

Mam tylko 72 godziny na zgłoszenie. Dobrze jest więc mieć przygotowaną procedurę. Tutaj UODO ułatwia nam zadanie. Na stronie https://uodo.gov.pl/pl/134/233 czytamy:

1. Zgłoszenia naruszenia dokonuje się elektronicznie **za pomocą odpowiedniego formularza dostępnego poniżej**, który należy wypełnić a następnie...
2. ...załączyć do **pisma ogólnego dostępnego na platformie biznes.gov.pl**
3. bądź wysłać przez elektroniczną skrzynkę podawczą ePUAP: **/UODO/SkrytkaESP**

Nie trzeba wymyślać własnego pisma czy formularza, wszystko jest gotowe do pobrania. Warto przejrzeć ten formularz już teraz, żeby mieć świadomość tego, jakie informacje będą wymagane w razie naruszenia. Skoro jest to oficjalny formularz UODO, to mogę być pewna, że odpowiada wszystkim wymogom z ust. 3 artykułu 33, w którym opisano zgłoszenie.

Tak przy okazji, ciekawe są np. rodzaje naruszenia wymienione w rubryce „Na czym polegało naruszenie?” To na pewno pomoże uświadomić sobie, jakie zdarzenia mogą być traktowane jako naruszenie.

Procedura zgłoszenia przez administratora opanowana.

Teraz zgłoszenie przez podmiot przetwarzający administratorowi, czyli sytuacja, która jest dla mnie bardziej prawdopodobna, ponieważ przetwarzam wrażliwe dane osobowe dla niektórych klientów.

Przypominam:

> *Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu*
> *2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.*

Tutaj już nie mam określenia czasu, tylko jest sformułowanie „bez zbędnej zwłoki". Hmmm, jak to będzie oceniane przez urzędników, to się jeszcze okaże. Nie określono też, jakie informacje zgłoszenie powinno zawierać. Na stronie UODO nie ma formularza dla podmiotów przetwarzających, ponieważ one zgłaszają naruszenie administratorowi, a dopiero on urzędowi.
Administrator musi być jednak w stanie podać wszystkie informacje w formularzu, więc pewnie będzie ich wymagać od podmiotu przetwarzającego.
Aby sobie ułatwić życie, dostosowałam formularz UODO do moich potrzeb podmiotu przetwarzającego. Usunęłam rubryczki, które dotyczą tylko administratora i gotowe.
Wzór znajdziesz w załączniku.

Najgorsze jest to, że w przypadku naruszenia, np. kiedy mimo wszystkich zabezpieczeń ktoś się włamie do mojego komputera, prawdopodobnie będę musiała się skontaktować z każdym administratorem, który powierzył mi przetwarzanie danych osobowych. Przerażająca myśl...

Ale to jeszcze nie koniec. Muszę prowadzić dokumentację wszelkich naruszeń i podjętych środków zaradczych.

> *Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu*
> *5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.*

Na to przewidziałam miejsce w pliku z dokumentacją w arkuszu Naruszenia. Opisałam tam procedury i założyłam rejestr naruszeń z przykładowymi wpisami:

- Naruszenie z dnia … <opis naruszenia, okoliczności naruszenia, środki zaradcze - patrz formularz zgłoszenia z dnia …>
- Naruszenie z dnia … : <opis naruszenia, okoliczności naruszenia, środki zaradcze - nie zgłoszono, brak ryzyka naruszenia praw i wolności osoby fizycznej>

To już koniec? Nie, jeszcze nie. Jako administrator mam nie tylko obowiązek zgłoszenia naruszenia do Urzędu Ochrony Danych Osobowych, ale zgodnie z artykułem 34 także muszę poinformować osobę, której dane dotyczą.

> *Artykuł 34 Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych*
> *1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.*

Chyba że:

> *Artykuł 34 Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych*
> *3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:*
> *a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;*
> *b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;*
> *[…]*

Jak wspomniałam wyżej, ze względu na rodzaj danych osobowych, które przetwarzam jako administrator, raczej nie będzie wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, więc raczej nie będę musiała spełnić obowiązku zawiadamiania.
Może się natomiast zdarzyć, że jako podmiot przetwarzający będę musiała zawiadomić administratora, a potem administrator osobę, której dane przetworzyliśmy.

Najważniejszy wniosek z tego całego wywodu jest następujący: obowiązkowo i bezwzględnie należy zastosować odpowiednie środki techniczne, które uniemożliwiają osobom nieupoważnionym dostęp do danych (szyfrowanie) i zapewniają ciągły dostęp do danych (kopia zapasowa).
Czyli profilaktyka. Może uchronić mnie przed bolesnymi konsekwencjami w postaci kontroli urzędowej, wypłaty odszkodowań, a przede wszystkim obowiązku kontaktowania się ze wszystkimi osobami, których może dotknąć moja lekkomyślność czy opieszałość… ech.

Moje wczesne życzenia świąteczne: oby żaden tłumacz nie musiał nigdy zgłosić naruszenia.
I równie wczesne postanowienia noworoczne: będę szyfrować i robić kopie zapasowe.

Do usłyszenia!
Twoja Tłumaczka