Rozliczalność a zasady przetwarzania w RODO

Tematem dzisiejszego artykułu będzie przybliżenie Wam tematu zasad przy przetwarzaniu danych osobowych, ze szczególnym zwróceniem uwagi na rozliczalność, czy właściwie zasadę rozliczalności, w kontekście przepisów o ochronie danych osobowych. Jest to jedna z najważniejszych zasad, która w sposób jednoznaczny wpływa na ukształtowanie, zrozumienie ale, co przede wszystkim nas jako administratorów danych powinno zainteresować, na kształtowanie w praktyce i właściwe zastosowanie przepisów ochrony danych osobowych. Czym jest zasada rozliczalności? Wymogiem wobec administratora, aby w każdej sytuacji był w stanie wykazać, że w prawidłowy sposób realizuje przepisy RODO. I tylko tyle? Nie tylko, bowiem za tym krótkim stwierdzeniem kryje się cały ciąg obowiązkowych działań, podejmowanych zarówno w zakresie administratora jak i organizacji, pracowników, klientów. Konsekwencją tych działań jest opracowanie i wdrożenie przez administratora odpowiednich procedur, polityk, instrukcji oraz zastosowanie adekwatnych środków organizacyjnych i technicznych. Wszystko po to, aby administrator był w stanie potwierdzić, że ochrona danych osobowych w jego organizacji funkcjonuje prawidłowo. I pomimo tego, że jak pisaliśmy o tym wcześniej, przepisy RODO w większości nie narzucają administratorowi konkretnych rozwiązań, nie wskazują jak powinna wyglądać konkretna dokumentacja, to jednak z zasady rozliczalności jednoznacznie wynika obowiązek administratora, udowodnienia przestrzegania zasad przetwarzania danych osobowych. Bez posiadania odpowiedniej dokumentacji, potwierdzającej przyjęcie w organizacji konkretnych rozwiązań, zasad i regulacji w zakresie ochrony danych osobowych oraz dokumentów potwierdzających, że zasady te zostały przyjęte i we właściwy sposób wdrożone, funkcjonują w ramach bieżącej działalności i są znane i respektowane w trakcie realizowania obowiązków służbowych przez pracowników, administrator nie jest w stanie wykazać spełnienia obowiązku rozliczalności.

Zasada rozliczalności odnosi się do wszystkich zasad określonych przez RODO przy przetwarzaniu danych osobowych. Administrator ma obowiązek, na każdym etapie przetwarzania móc wykazać, że w pełni przestrzega wszystkich zasad przetwarzania określonych przepisami. Dokładnie zakres tych zasad, których przestrzeganiem musi wykazać się administrator określa art. 5 ust.1 RODO. Krótko opiszemy czym charakteryzują się poszczególne zasady:

1. Ograniczenie celu - czyli zbieranie danych tylko i wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach. Warunkiem jest także, że administrator, po zebraniu danych osobowych, nie może ich wykorzystywać do innych celów,
2. Integralność i poufność czyli zabezpieczenie danych osobowych przez wdrożenie adekwatnych, odpowiednich środków organizacyjnych i technicznych aby zabezpieczyć te dane przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem,
3. Przejrzystość i rzetelność czyli przetwarzanie w taki sposób aby dla każdej osoby, której to dotyczy przetwarzanie było jasne i czytelne, a informacje w tym zakresie przekazywane prostym i zrozumiałym językiem w łatwo dostępnej i zrozumiałej formie,
4. Minimalizacja danych czyli wymóg aby administrator gromadził minimum danych osobowych niezbędnych mu do realizacji celu, w ramach którego te dane są zbierane. Z zasadą minimalizmu powiązane są pojęcia anonimizacji i pseudonimizacji,
5. Merytoryczna poprawność danych czyli wymóg aby dane były poprawne i w razie potrzeby uaktualniane. Tym samym administrator, w zakresie danych osobowych, które zebrał, ma obowiązek dopilnować ich aktualizacji lub sprostowania,
6. Ograniczenie przechowywania czyli przechowywania danych w formie, która umożliwia identyfikację osoby, tylko i wyłącznie przez okres niezbędny do realizacji celów bądź okres wskazany konkretnym przepisem prawa,
7. Privacy by design (nazywanej też „zasadą prywatności w fazie projektowania") czyli zasada, w myśl której administrator danych będzie zobowiązany zapewnić, aby już na etapie

projektowania systemu, a następnie na etapie wykorzystywania go, do przetwarzania danych wprowadzone do niego zostały odpowiednie środki techniczne i organizacyjne, które zapewnią ochronę danych użytkowników i ich przetwarzanie zgodnie z RODO.

8. Privacy by default (nazywanej też „zasadą prywatności w ustawieniach domyślnych") czyli przyjęcie założenia ochrony prywatności, jako domyślnego ustawienia każdego programu (systemu). Zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie użytkownika programu. W praktyce funkcjonowania systemu użytkownicy, chcąc zrezygnować z części swej prywatności powinni podjąć aktywne działania w tym kierunku, a nie powinno to być efektem samodzielnego działania twórców systemu, ingerującym w prywatność użytkownika. Zasada ta nakazuje administratorowi dokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, gdy 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.

W praktyce stosowania ochrony danych osobowych zasadę rozliczalności nie należy traktować jako dodatkowego obciążenia administratora, tak naprawdę bowiem, ta zasada jest pewną formą podpowiedzi, wskazania jak stosować przepisy RODO, żeby prawidłowo wywiązać się ze wszystkich obowiązków w tych przepisach wskazanych. W ten sposób wracamy też do kwestii wcześniej już omawianej, a mianowicie jakie działania, w tym jaki zakres dokumentacji, powinien prowadzić oraz jakie działania powinien podjąć administrator, aby móc prowadzić działalność w przekonaniu, że jest w stanie wykazać prawidłowość przetwarzania danych osobowych w jego organizacji. Nie rozpisując się już nadmiernie, wskazać należy, że ten niezbędny, podstawowy zakres posiadanej dokumentacji i zrealizowanych działań to:

- Dokumentacja ochrony danych osobowych (Polityka bezpieczeństwa, Instrukcja zarzadzania systemami informatycznymi, polityka bezpieczeństwa fizycznego, procedury dotyczące miedzy innymi monitoringu, identyfikacji i postępowania z incydentami i naruszeniami),
- Odpowiedni zabezpieczony system informatyczny i wykorzystywane programy,
- Wdrożone dokumenty: upoważnienia, zobowiązania do zachowania poufności, umowy powierzenia, rejestry (upoważnień, umów powierzeń, udostępnień),
- Systematyczne prowadzenie szkoleń pracowników z zakresu ochrony danych osobowych,
- Szacowanie ryzyka i ocena skutków dla ochrony danych osobowych.

Bez tego niezbędnego minimum trudno jest mówić o prawidłowym przetwarzaniu i jego udokumentowaniu w organizacji, a jeszcze trudniej o przekonaniu, że tak jest organu nadzoru, w przypadku, gdy zdarzy się nieszczęście i z różnych powodów, jesteśmy zmuszeni odpowiadać na szczegółowe pytania tego organu.

I w tym temacie trochę więcej w drugiej części artykułu. W przypadku konieczności odpowiadania na pytania PUODO, czy to wskutek naszego samozgłoszenia naruszenia, czy w przypadku, gdy wpłynęła na nas skarga, podstawą jest świadomość w jaki sposób funkcjonuje w takich wypadkach polski organ nadzoru czyli PUODO. Po pierwsze, nie należy działań organu lekceważyć i zdecydowanie dochowywać wskazanych przez organ terminów czy to odpowiedzi czy realizacji wskazanych działań. PUODO jest urzędem świadomym swojej ważnej misji, nie lubi być lekceważony, a jeśli już ktoś się na to odważy to urząd posiada środki sankcjonujące takie działanie, z których, jak pokazuje praktyka ostatnich miesięcy, potrafi zrobić użytek. Po drugie, nie lekceważmy PUODO opisem jak to u nas wszystko, pomimo naruszenia, jest świetnie i ile to nie zrobiliśmy, żeby przywrócić właściwie przetwarzanie danych osobowych. Jak wskazuje bowiem i nasza praktyka, jak i opis podobnych spraw, przygotowanie i wysłanie do PUODO pisma opisującego jakie to prawidłowe działania firma podjęła kiedy stwierdzono

naruszenie oraz jakie wcześniej przyjęto rozwiązania w zakresie monitorowania bezpiecznego przetwarzania danych osobowych, to dopiero początek. Problem w tym, że PUODO nie zadowala się ogólnymi stwierdzeniami i deklaracjami, lecz żąda konkretnych dokumentów potwierdzających podjęte działania lub przedstawione okoliczności. Nie wystarcza sama deklaracja, że przeprowadzony został audyt wewnętrzny i zewnętrzny, że podjęto odpowiednie działania na systemie i bazach danych. W kolejnym piśmie urząd żąda konkretnych dokumentów, w tym z systemów informatycznych, jednoznacznie potwierdzających, że firma faktycznie zrealizowała opisane działania i że ma na to dowody i odpowiednią dokumentację w zakresie ochrony danych osobowych oraz, że wdrożyła opisane procedury. Zasadnym więc wydaje się posiadanie takiej dokumentacji i wdrożonych procedur, których przestrzeganie na bieżąco jest monitorowane, by w sytuacji naruszenia móc przywrócić, bez szkody dla firmy, jej prawidłowe funkcjonowanie, ale też prawidłowo dokonać zgłoszenia do organu nadzorczego. W razie konieczności uzupełnienia zgłoszenia będziemy mogli wykazać to co rzeczywiście jest realizowane, a nasze działania okażą się satysfakcjonujące dla PUODO to pozwoli nam to uniknąć dodatkowych konsekwencji.

Jeśli uważnie przeczytaliście tekst powyżej, to zwróciliście uwagę, że dane osobowe muszą być przetwarzane w sposób zapewniający ochronę przed przypadkową utratą, zniszczeniem lub uszkodzeniem. Czyli zgodnie z zasadą integralności i poufności. Jeżeli w naszej firmie nastąpi naruszenie ochrony danych np. poprzez zaszyfrowanie danych to znaczy, że nie jesteśmy w stanie z tych danych korzystać ani umożliwić korzystanie naszym klientom, a to narusza przepisy RODO. Nie dość więc, że mamy ogromny kłopot z bieżącym funkcjonowaniem firmy to jeszcze musimy zmierzyć się z działaniami PUODO, zresztą wynikającymi z naszego obowiązku zgłoszenia naruszenia. Prawidłowa realizacja zasad przetwarzania danych osobowych opracowana i wdrożona u danego administratora pozwala na przygotowanie wyjaśnień, które będą satysfakcjonujące dla PUODO, a jednocześnie stanowi ogromnie ważny element pozwalający na szybkie przywrócenie w firmie stanu sprzed ataku hackerskiego czy innego uszkodzenia systemu czy bazy danych. Należy też zwrócić uwagę na dopracowanie prawidłowych procedur wykonywania pracy zdalnej i wykorzystywania w tym zakresie bezpiecznych narzędzi, bo wszystko wskazuje na to, że oprócz wielu korzyści wynikających z tego systemu wykonywania pracy, jednym z zagrożeń jest właśnie możliwy atak hackerski i zaszyfrowanie bazy danych całej firmy. Tych przypadków ostatnio lawinowo przybywa. Realizacja zasad zawartych w RODO, w szczególności zasada rozliczalności, daje nam pewne gwarancje, że prawidłowo przetwarzamy dane w firmie, ale też pozwalają w sytuacjach naruszenia ochrony danych zrealizować właściwe procedury i zakończyć sukcesem postępowanie przed PUODO. Bez względu na stosowane środki bezpieczeństwa musimy pamiętać, że naruszenie może przydarzyć się w każdej firmie i na tą okoliczność chcemy byście byli przygotowani.

etaxar

Janusz Dębowski
Ochrona Danych Osobowych
tel. 502 434 909
biuro@etaxar.pl

mp
Magdalena Piekuś
OCHRONA DANYCH OSOBOWYCH