Warszawa, dnia 1 lutego 2019 r.

Pan
Piotr Drobek
Dyrektor Zespołu Analiz i Strategii
UODO

Szanowny Panie Dyrektorze,

W odpowiedzi na zaproszenie do wzięcia udziału w konsultacjach publicznych dotyczących umów powierzenia przetwarzania danych, Związek Pracodawców Branży Internetowej IAB Polska przedstawia swoje stanowisko i propozycje dotyczące standardowych klauzul umownych:

1. **Jak dokumentować polecenia administratora dotyczące przetwarzania danych?**

Administrator może polecić przetwarzającemu szeroki wachlarz operacji przetwarzania danych. Z tego względu, naszym zdaniem, dopuszczone powinny zostać wszelkie formy dokumentowania poleceń administratora, o ile na ich podstawie możliwe będzie jednoznaczne wskazanie jego intencji. Taka instrukcja powinna wskazywać co najmniej kategorię danych, które mają zostać przetworzone oraz wskazywać rodzaj czynności, które mają zostać podjęte przez przetwarzającego. Jeżeli te warunki są spełnione, to faktyczna forma może być dowolna, np.:

- postanowienia umowy;
- postanowienia zamówień lub zleceń składanych w związku z realizacją umowy ramowej;
- polecenia składane środkami komunikacji bezpośredniej, o ile będzie możliwość ich utrwalenia;
- polecenia wydawane za pośrednictwem systemu informatycznego, o ile będą one zapisywane w formie np. logów.

W tym zakresie, zasadnym wydaje się posłużenie się analogicznymi rozwiązaniami jak w przypadku "wyraźnego działania potwierdzającego", które stanowi jedną z form udzielenia zgody na przetwarzanie danych osobowych. W obu sytuacjach administrator powinien mieć możliwość "odtworzenia" treści oświadczenia, które zostało złożone.

Związek Pracodawców Branży Internetowej IAB Polska
ul. Puławska 39 lok. 77 02-508 Warszawa tel. +48 22 415 54 44 fax +48 22 212 87 74
www.iab.org.pl

2. **Jak weryfikować zobowiązania do zachowania tajemnicy przez osoby upoważnione do przetwarzania danych?**

Uważamy, że podmiot przetwarzający powinien przyjąć na siebie umowne zobowiązanie do zapewnienia, że osoby upoważnione do przetwarzania danych są zobowiązane do zachowania ich w tajemnicy. Dodatkowo, fakt ten mogą potwierdzać ewentualne audyty zewnętrzne przeprowadzane u przetwarzającego.

Zbyt daleko posuniętym uprawnieniem wydaje się zaś, możliwość żądania przez administratora dostępu np. do umów o pracę osób mających dostęp do powierzonych danych. Natomiast podmiot przetwarzający powinien w umowie zobowiązać się do ponoszenia odpowiedzialności za działania i zaniechania takich osób.

3. **Jak precyzyjnie powinny być w umowie wskazane środki bezpieczeństwa wymagane na mocy art. 32 RODO?**

Naszym zdaniem opis środków bezpieczeństwa powinien być na tyle dokładny, żeby administrator mógł dokonać oceny, czy są one wystarczające, zważywszy na kryteria wskazane w art. 32 RODO. Nie powinien jednak narażać podmiotu przetwarzającego na dodatkowe ryzyko związane z nieuprawnionym wykorzystaniem takich informacji. Dla przykładu, wystarczające wydaje się wskazanie, że obiekty, gdzie przetwarzane są dane są chronione przez strażników. Zbyt daleko idącym, będzie natomiast wskazanie ich liczby, tras i częstotliwości patroli.

Przy sporządzaniu opisu środków bezpieczeństwa pomocne może być posłużenie się normą ISO 27001.

4. **Jak skutecznie wywiązywać się z obowiązków związanych z realizacją żądań osoby, której dane dotyczą?**

W pierwszej kolejności należy zaznaczyć, że to administrator jest zobowiązany do realizacji praw podmiotu danych. Jednak i w tym przypadku, można skorzystać z usług podmiotu przetwarzającego. W takiej sytuacji kluczowe wydaje się, aby jednoznacznie wskazać, że adresatem żądania jest właśnie administrator oraz że jest ono realizowane na jego rzecz. Przetwarzający, spełniając np. obowiązek informacyjny w imieniu administratora, nie powinien być zobowiązany by ujawniać, że jest innym podmiotem. Nie ma również przeszkód, aby przetwarzający dostarczył administratorowi rozwiązania techniczne, z których będą mogły korzystać osoby, których dane są przetwarzane.

Najważniejsze jest jednak jednoznaczne określenie zasad, który z podmiotów odpowiada za spełnienie tych obowiązków.

W praktyce szczególnie istotne okazują się postanowienia umowy pomiędzy administratorem a podmiotem przetwarzającym dotyczące zachowania podmiotu przetwarzającego po otrzymaniu żądania osoby, której dane dotyczą. Możliwe w tym względzie są co najmniej trzy scenariusze: (i) podmiot przetwarzający ma obowiązek przekazać wniosek do administratora, (ii) podmiot przetwarzający powinien zwrócić wniosek wnioskodawcy, wskazując właściwego adresata (administratora), (iii) podmiot przetwarzający powinien rozpatrzeć wniosek. Ze względu na doniosłość prawną działania podejmowanego na skutek wniesienia żądania podmiotu danych, umowa pomiędzy administratorem a podmiotem przetwarzającym powinna zawierać uregulowanie określonego sposobu postępowania podmiotu przetwarzającego po otrzymaniu takiego żądania.

5. **Jak realizować obowiązek udostępnienia informacji niezbędnych do wykazania spełnienia obowiązków ciążących na administratorze (m.in. art. 28, 32-36 RODO)?**

Podmiot przetwarzający może legitymować się przed administratorem różnego rodzaju certyfikatami lub spełnieniem powszechnie uznanych standardów. Administrator powinien mieć również zapewnione prawo audytu podmiotu przetwarzającego. Zalecanym powinno być, aby strony ustaliły zasady (w tym rozliczenie ewentualnych kosztów) jego przeprowadzenia.

Z praktyki stosowania wskazanych przepisów wynika też, że zasadnym jest ustalenie w umowie terminu, w jakim podmiot przetwarzający powinien przekazać administratorowi żądane informacje, a także sposobu (środka komunikacji) ich przekazania.

6. **Jak zapewniać zgodność działań innego podmiotu przetwarzającego z postanowieniami umowy zawartej z administratorem?**

Podmiot przetwarzający, który jest stroną umowy z administratorem, powinien ponosić pełną odpowiedzialność za działania i zaniechania dalszych przetwarzających. Dodatkowo, powinien dysponować procedurą weryfikacji i kontroli tych podmiotów. Administrator powinien mieć możliwość zapoznania się z powyższymi procedurami.

Z poważaniem,

PREZES ZARZĄDU
Włodzimierz Schmidt

Związek Pracodawców Branży Internetowej IAB Polska
ul. Puławska 39 lok. 77 02-508 Warszawa tel. +48 22 415 54 44 fax +48 22 212 87 74
www.iab.org.pl