Załącznik Nr 4
do Polityki Ochrony Danych Osobowych

Toruń, dnia 25 maja 2018 r.

ZBIÓR ZASAD DOMYŚLNEJ OCHRONY PRYWATNOŚCI (PRIVACY BY DEFAULT) ORAZ PROJEKTOWANEJ OCHRONY PRYWATNOŚCI (PRIVACY BY DESIGN)
DRIMER Sp. z o.o. sp.k. z siedzibą w Toruniu

Uwagi ogólne:

Zgodnie z zasadą domyślnej ochrony prywatności (privacy by default) – zakres udostępnionych danych osobowych przez osobę fizyczną powinien być maksymalnie ograniczony i obejmować wyłącznie dane niezbędne do wyznaczonych przez Spółkę celów. Innymi słowy, Spółka nie powinna nadmiernie przetwarzać dane, zaś samo przetwarzanie powinno mieć oparcie w podstawie prawnej wynikającej z RODO. To osoba, której dane dotyczą (użytkownik, pracownik, klient) decyduje, czy chce zmniejszyć poziom ochrony swojej prywatności poprzez udostępnienie dalszych danych lub zmianę ustawień prywatności lub podanie informacji niewymaganych do realizacji danej czynności, ale pomocnym np. przy personalizacji produktu lub usług.

Z kolei zasady projektowanej ochrony prywatności (*privacy by design*) zakładają, że Spółka projektując procedury, systemy, procesy, usługi lub produkty powinna wdrażać środki zapewniające bezpieczeństwo przetwarzania danych już w fazie projektowania, a nie dodawać je dopiero po wymyśleniu i zaprojektowaniu danego rozwiązania. Zaletami takiego podejścia są: 1) identyfikacja możliwych problemów już na samym początku procesu lub projektowania, b) większe prawdopodobieństwo spełnienia wymogów prawa w zakresie przetwarzania oraz 3) wzrost świadomości dotyczącej wymogów przetwarzania danych osobowych w organizacji.

Poniżej znajdują się podstawowe zasady związane z domyślną i projektowaną ochroną prywatności.

Zasady domyślnej ochrony prywatności - Privacy by default

Zgodnie z art. 25 ust. 2 RODO Spółka wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (minimalizacja danych). Obowiązek ten odnosi się do:

a. ilości zbieranych danych osobowych (minimalizacja ilości danych),
b. zakresu ich przetwarzania (minimalizacja zakresu danych),
c. okresu ich przechowywania (minimalizacja przechowywania danych),
d. dostępności danych (minimalizacja dostępu do danych),
e. reglamentacji dostępu do danych – ograniczeniu dostępu osób fizycznych

Spółka powinna wiedzieć o osobie fizycznej tylko to, co konieczne z uwagi na dany proces przetwarzania, tak długo jak jest to konieczne, a ponadto w Spółce dostęp do danych powinien być odpowiednio reglamentowany.

Podsumowując, w celu zapewnienia prawidłowego przestrzegania zasady domyślnej ochrony danych należy:

1. zweryfikować stosowane formularze i dokumenty i usunąć z nich pola wymagające podawania przez osobę fizyczną nadmiernych lub zbędnych danych;

2. informować osoby o zakresie danych niezbędnych, których podanie jest konieczne dla danego procesu lub usługi oraz danych podawanych dobrowolnie i nieobowiązkowych;
3. ustalić, przez jaki czas dane powinny być przetwarzane, biorąc pod uwagę stosunek prawny łączący strony, terminy przedawnienia, terminy wynikające z przepisów prawa (np. dokumenty kadrowe) lub treść umowy pomiędzy stronami
4. ograniczyć dostęp do danych (np. poprzez rozwiązania informatyczne lub faktyczne zabezpieczenia tj. klucze, karty dostępu) jedynie do upoważnionych pracowników lub osób, w szczególności poprzez ograniczenie dostępu nowym pracowników lub pracownikom na niższych stanowiskach w organizacji,
5. chronić dane przed niepowołanym dostępem przez osoby nieupoważnione lub przed wyciekiem danych poprzez narzędzia organizacyjne i techniczne (np. pseudonimizację, szyfrowanie danych).

W praktyce zasada domyślnej ochrony danych wymaga
- przestrzegania architektury informacji w organizacji,
- stosowania zasad zarządzania dostępem, w tym domyślnych uprawnień poszczególnych grup użytkowników do poszczególnych zasobów w ramach architektury informacji,
- zastosowania odpowiednich narzędzi – podstawowe narzędzia można znaleźć w systemach operacyjnych komputerów, ale w praktyce do najczęściej spotykanych należą klucze i karty dostępu;
- korzystania z takich usług informatycznych i nabywania systemów informatycznych, które umożliwiają zarządzanie dostępem i rozliczalność dostępu;
- przydzielenia odpowiednich uprawnień i zobowiązania personelu do korzystania wyłącznie z zasobów niezbędnych dla poszczególnych pracowników;
- zaprojektowania odpowiedniej infrastruktury biura.

Istotne jest zapewnienie kontroli dostępu do danych i niedopuszczenia do sytuacji ich udostępnienia bliżej nieokreślonej liczbie osób. Dla przykładu:
Jeśli udostępniamy zasoby wszystkim pracownikom, to w wyniku rotacji pracowników (zwłaszcza na niższych szczeblach – programy praktyk itp.) ten pozornie zamknięty krąg może zostać uznany za krąg otwarty, do którego zalicza się nieokreślona liczba osób fizycznych. W związku z tym domyślna prywatność powinna tu oznaczać domyślny ograniczony krąg dostępu do danych, a co za tym idzie – nie wydaje się zgodne z przepisami dot. ochrony danych osobowych, by każdy nowy pracownik firmy (czy też nowo ustanowiony użytkownik systemów firmy) miał od razu dostęp do wszystkich zasobów.

Zasady projektowanej ochrony prywatności - Privacy by design
Z samego brzmienia przepisu RODO dotyczącego projektowania prywatności można wyodrębnić trzy elementy, które należy zapewnić:

1. bezpieczeństwo,
2. minimalizację dostępu
3. zaprojektować powyższe przed wdrożeniem lub zaprojektowaniem nowych rozwiązań, zabezpieczeń, produktów lub usług.

Należy dokonać analizy czynników wpływających na zakres obowiązku projektowania, tj. stan wiedzy technicznej, koszt wdrażania, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

Należy jednocześnie zaznaczyć, że żadne względy natury organizacyjno-finansowej nie powinny być traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych. Nie oznacza to jednak, że Spółka zobowiązana jest do zapewnienia w procesie przetwarzania wszelkich dostępnych środków bezpieczeństwa – może ograniczyć się do takich, które są wystarczające i odpowiednie w świetle wymagań stawianych przez przepisy prawa, w tym RODO.

Projektowanie prywatności powinno opierać się o następujące kroki:

1. ocena ryzyka lub ocena skutków przetwarzania dla planowanego procesu przetwarzania,
2. wybór rozwiązań zapewniających większe możliwości ograniczenia dostępu do danych i wypełnienia założeń privacy by default,
3. zakup lub projektowanie narzędzi do zarządzania dostępem,
4. wybór dostawcy usługi oferującego większą odpowiedzialność za naruszenia ochrony danych lub posiadającego odpowiedni certyfikat,
5. Każde projektowanie powinno zawierać weryfikację wpływu działania związanego z wydatkiem na procesy przetwarzania i ochronę danych osobowych.