Warszawa, dn. 9.12.2025 r.

Privacy by design w praktyce - 5 błędów, które trzeba koniecznie przestać popełniać

Wstęp

Privacy by design wielu administratorom danych wciąż kojarzy się z teorią lub formalnym wymogiem RODO. Tymczasem art. 25 mówi jasno – ochrona danych osobowych ma być **wbudowana w procesy, produkty i usługi już od etapu projektowania (cyt.: „… przy określaniu sposobów przetwarzania…")**. W praktyce oznacza to, że prywatność nie może być „dodatkiem" do gotowego projektu. Powinna być jednym z jego fundamentów – iść wspólnie z bezpieczeństwem, użytecznością czy zgodnością techniczną. Mimo to, po wejściu RODO, wiele organizacji dotychczas popełnia te same błędy.
Przyjrzyjmy się zatem pięciu wybranym błędom z praktyki – i zobaczmy, jak ich uniknąć.

❌ Błąd #1: Privacy by design na papierze w segregatorze

W wielu przypadkach *privacy by design* jak i ogólnie wdrożenie zgodności z RODO sprowadza się do przyjęcia ogólnej polityki lub wzoru procedury. Problem w tym, że takie dokumenty często nie mają przełożenia na codzienną pracę zespołów m.in. IT, marketingu, sprzedaży czy HR.
Bez prostych narzędzi – podstawowych checklist zgodności, formularzy oceny ryzyka, instrukcji dla deweloperów i przede wszystkim szkolenia i punktów kontrolnych stosowania przyjętych polityki i procedur – koncepcja pozostaje martwa.

💡 **Rozwiązanie:**

- Włącz zasady prywatności do istniejących procesów – minimalizacja i bezpieczeństwo danych rzeczywiście mają działać.
- Dodaj do każdego nowego projektu obowiązkowe punkty związane z ochroną danych osobowych m.in. „Czy uwzględniono i oceniono ryzyka dla podmiotów, których dane są przetwarzane w danym projekcie?", „Czy jest podstawa prawna do ich przetwarzania?", Czy zaciągnięto opinię IOD, specjalisty ds. ochrony danych osobowych?".

❌ Błąd #2: IOD włączany do projektu zbyt późno

W wielu organizacjach Inspektor Ochrony Danych jest informowany o projekcie… tuż przed jego wdrożeniem, a najlepiej jeszcze w duecie z prośbą o akceptację. To moment, gdy trudno już coś zmienić bez opóźnień i kosztów.
IOD powinien być obecny **na etapie planowania**, a nie „gaszenia pożarów". Dzięki temu może pomóc ocenić ryzyka, dobrać właściwe zabezpieczenia i uniknąć błędów, które później mogą kosztować firmę reputację lub karę.

💡 **Rozwiązanie:**

- Wprowadź zasadę: każdy projekt z elementem przetwarzania danych musi być wcześniej skonsultowany z IOD. **UWAGA**: nie powinien to też być etap, kiedy nie wiadomo zupełnie jakie procesy związane z przetwarzaniem danych są planowane. Przyjdź z konkretem, ale jeszcze zanim on ostatecznie zostanie zatwierdzony przez Zarząd. A to prowadzi do następnej rekomendacji, a mianowicie:
- Ustal w procedurze, w którym momencie projekt trafia do IOD i jakie informacje są mu przekazywane.

❌ Błąd #3: Brak realnej oceny ryzyka i DPIA

Ocena skutków dla ochrony danych (DPIA) to jedno z najważniejszych narzędzi *privacy by design*.
Niestety, często jest wykonywana tylko „dla formalności" albo pomijana, bo „projekt nie wydaje się ryzykowny i po co opisywać procesy taj szczegółowo". Wbrew pozorom UODO właśnie poprzez brak rzetelnej oceny ryzyka z uwzględnieniem możliwych konsekwencji nawet przy niskim ryzyku wydaje najwyższe kary.
Tymczasem nawet prosta aplikacja czy formularz zbierający adresy e-mail do newsletteru może przetwarzać dane w sposób wymagający oceny ryzyka – zwłaszcza przy użyciu nowych technologii czy zewnętrznych dostawców.

💡 **Rozwiązanie:**

- Wprowadź krótki formularz wstępnej oceny (tzw. *screening*), który pomoże szybko ustalić, czy DPIA jest potrzebna i włącz do procesów projektowych Twojego project managera i przeprowadź podstawowe szkolenia jak go wypełnić.
- Prowadź DPIA wspólnie – prawnik, IT i biznes powinni być przy „wspólnym stole", wtedy nic nie umknie.

❌ Błąd #4: Przechowywanie danych nadmiarowo i dłużej niż jest wskazane w procedurze

To klasyka. Procedura została spisana, przyjęta, wrzucona do folderu „Procedury RODO" na sharepoincie i koniec 😊 Systemy i formularze wciąż proszą o dane, które nie są potrzebne: PESEL w ankiecie, adres korespondencyjny w konkursie online czy numer telefonu w zapisie na newsletter. Takie przypadki łamią zasadę **minimalizacji danych**, a przy okazji zwiększają ryzyko wycieku i odpowiedzialność administratora.

💡 **Rozwiązanie:**

- Regularnie przeglądaj formularze i bazy danych – usuń pola, które nie są niezbędne wobec celu.
- Włącz zasadę minimalizacji do standardów UX/UI – zespół projektujący formularze powinien wiedzieć, jakie dane są naprawdę potrzebne.

❌ Błąd #5: Brak testów i audytów „po wdrożeniu"

Privacy by design to proces ciągły, nie jednorazowa czynność na początku projektu. Niestety, wiele firm **wdraża nowe rozwiązanie i na tym kończy temat**. Nikt już nie sprawdza, czy

dane rzeczywiście są chronione, czy dostęp mają tylko uprawnieni, czy logi bezpieczeństwa są analizowane.

💡 **Rozwiązanie:**

- Zrób audyt *privacy by design*, idealnie raz w roku lub po każdej większej zmianie w procesie.
- Testuj procesy – sprawdź, czy np. usunięcie danych użytkownika faktycznie usuwa je z kopii zapasowych.

Podsumowanie

Privacy by design to jak najbardziej praktyka, a nie teoria. **Pomocne narzędzie identyfikacji i eliminacji ryzyk** oraz budowania zaufania klientów. Warto pamiętać, że najskuteczniejsze wdrożenia to te, które łączą ludzi, procesy i technologię – a nie generuje kolejne dokumenty. Jeśli Twoja organizacja dopiero zaczyna wdrażać zasady *privacy by design* w swoje procesy, zacznij od prostych kroków: checklist, konsultacji z IOD i przeglądu istniejących procesów.

Kateryna Stryhina – specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.