Procedura uwzględniania ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych

Realizowanie zasad privacy by design i privacy by default, jest jednym z podstawowych obowiązków RODO, dlatego UIK uwzględnia je w każdym procesie związanym z przetwarzaniem danych osobowych. Zasada ochrony danych w fazie projektowania ma za zadanie ochronę prywatności już na etapie kreowania danego projektu, narzędzia, aplikacji, funkcjonalności. Jest to też związane z zasadą celowości RODO czyli rozważeniem jaki cel ma być realizowany poprzez wykorzystywanie danych osobowych oraz w związku z tym jakie dane osobowe będą nam potrzebne.

Zasada domyślnej ochrony danych osobowych dotyczy przewidywania możliwych zabezpieczeń danych osobowych w ramach danego projektu, narzędzia, aplikacji, funkcjonalności i wdrażania takich rozwiązań. Chodzi o to, aby użytkownik który przyłącza się do danego systemu był już domyślnie (bo ktoś o tym pomyślał wcześniej) chroniony w zakresie danych osobowych, które będzie udostępniał.

Mając to na uwadze UIK wprowadza następujące zasady:

1. Zastanów się jaki cel ma realizować proces, system, aplikacja itp. nad którymi pracujesz.
2. Jeśli cel zakłada wykorzystanie danych osobowych, zastanów się nad tym:
   a. jakie konkretne rodzaje tych danych musisz zebrać, czy będą to dane zwykłe np. imię, nazwisko, adres e-mail itp., czy może dane szczególnych kategorii np. informacje o zdrowiu, nałogach, orientacji seksualnej itp.,
   b. jak długo będziesz je musiał przechowywać i dlaczego,
   c. komu będziesz je udostępniać i dlaczego,
3. Zrealizuj cel projektując rozwiązanie tak, żeby zebrać tylko te dane, które faktycznie będą niezbędne dla jego zrealizowania.
4. Realizując cel nie zbieraj danych na „zapas", możesz mieć wówczas problemy.
5. Realizując cel unikaj rozwiązań obarczonych ryzykiem organizacyjnym lub technicznym. Jeśli nie umiesz sobie z tym poradzić zgłoś się do działu IT.
6. Realizując cel stosuj rozwiązania, które będą minimalizowały jakiekolwiek ryzyko naruszenia zbieranych danych osobowych np. realizujesz cel on-line stosuj protokół SSL itp. Przygotowując zestawienia i raporty zastanów się czy na pewno musisz wpisywać imię i nazwisko pracownika (może akurat w tym raporcie te dane są zbędne).