5. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych (zasady "privacy by design" oraz "privacy by default")

1. Administrator danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.

2. Projektowane rozwiązania techniczne i organizacyjne muszą, w szczególności zapewnić, aby zakres i ilość przetwarzanych danych był ograniczony do tego co jest niezbędne dla osiągnięcia określonego celu przetwarzania danych („minimalizacja danych").

3. Administrator danych stosuje, w szczególności środki techniczne i organizacyjne takie jak pseudonimizacja danych (odwracalne szyfrowanie danych).

4. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator danych uwzględnia:

4.1. stan wiedzy technicznej,

4.2. koszt wdrażania,

4.3. charakter, zakres, kontekst i cele przetwarzania danych,

4.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

5. Administrator danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.

6. W szczególności stosowane środki techniczne i organizacje muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.

7. W pierwszej kolejności, Administrator danych powinien rozważyć czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak należy wybrać takie rozwiązanie.

8. Administrator danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-7 powyżej (tzw. zasady „privacy by design" i „privacy by default") było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.

9. Niezależnie od postanowień pkt 8 realizacja zasad „privacy by design" i „privacy by default" może być także wykazana poprzez stosowanie przez Administratora danych mechanizmów certyfikacji zatwierdzonych na warunkach określonych we właściwych przepisach RODO.

10. Zasady „privacy by design" i „privacy by default należy uwzględniać zarówno w fazie projektowania nowych rozwiązań, jak również wprowadzania modyfikacji do już istniejących.

11. Do postępowania zgodnie z zasadami „privacy by design" i „privacy by default zobowiązany jest w szczególności pracownik Administratora danych, który merytorycznie odpowiada za wdrożenie rozwiązań, z którymi wiąże się przetwarzanie danych osobowych.

12. W przypadku, gdy stworzenie lub zaprojektowanie nowego rozwiązania zlecane jest podmiotom trzecim (w ramach outsourcingu usług) Administrator danych zobowiązuje te podmioty, aby tworzone lub projektowane przez nie rozwiązania były zgodne z zasadami „privacy by design" i „privacy by default". W tym

celu Administrator danych stosuje, w szczególności odpowiednie zapisy w zapytaniach ofertowych oraz umowach o współpracy.

13. Administrator danych informuje IOD o planowanym wdrożeniu nowego rozwiązania, z którym wiąże się przetwarzanie danych osobowych. W razie potrzeby, na wniosek Administratora danych, IOD opiniuje zgodność projektowych rozwiązań z zasadami „privacy by design" i „privacy by default".