6) kryptograficzne środki ochrony danych osobowych;
7) wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
8) mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności użytkownika.

§ 7. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:
1) osoby zatrudnione przy przetwarzaniu danych są zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
2) osoby zatrudnione przy przetwarzaniu danych osobowych są przeszkolone w zakresie zabezpieczeń systemu informatycznego;
3) osoby zatrudnione przy przetwarzaniu danych osobowych są obowiązane do zachowania ich w tajemnicy;
4) monitory komputerów, na których przetwarzane są dane osobowe, są ustawione w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
5) kopie zapasowe zbioru danych osobowych są przechowywane w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Rozdział 4
Procedura DPIA
(Data Protection Impact Assessment)

§ 8. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych z wykorzystaniem załącznika nr 3.

§ 9. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie.

§ 10. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Rozdział 5
Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 11. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie z wykorzystaniem załącznika nr 4a i 4b.

§ 12. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.

§ 13. Na podstawie wyników przeprowadzonej analizy ryzyka wskazani przez administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.

§ 14. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.

§ 15. Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów zgodnie z załącznikiem nr 4b, lub ryzyka w stosunku do zasobu biorącego udział w procesie wysokiego ryzyka stosownie do wyniku DPIA zgodnie z załącznikiem nr 3.

Rozdział 6
Procedura współpracy z podmiotami zewnętrznymi

§ 16. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 6.

§ 17. Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z Rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej zgodnie z załącznikiem nr 7.

Rozdział 7
Procedura domyślnej ochrony danych

§ 18. Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza DPIA w stosunku do tego procesu.

§ 19. W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

Rozdział 8
Procedura zarządzania incydentami

§ 20. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

§ 21. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.

§ 22. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.

§ 23. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych, zgodnie z załącznikiem nr 10.

Rozdział 9
Procedura realizacji praw osób

§ 24. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w Rozporządzeniu administrator danych rozpatruje indywidualnie zgodnie z procedurą opisaną w załączniku nr 9, 9a i 9b.

§ 25. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

1) prawo dostępu do danych,
2) prawo do sprostowania danych,
3) prawo do usunięcia danych,
4) prawo do ograniczenia przetwarzania danych,
5) prawo do przenoszenia danych,
6) prawo do sprzeciwu wobec przetwarzania danych,
7) prawo do niepodlegania decyzjom opartym wyłącznie na profilowaniu.

§ 26. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 27. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów Rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z Rozporządzenia.

Rozdział 10
Procedura odbierania zgód oraz informowania osób

§ 28. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z załącznikiem nr 8.

§ 29. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikiem nr 8.

§ 30. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z załącznikiem nr 8.

Rozdział 11
Postanowienia końcowe

§ 31. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

§ 32. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

Załączniki:

Załącznik nr 1 – rejestr czynności przetwarzania,

Załącznik nr 2 – powołanie IOD,

Załącznik nr 3 – arkusz DPIA,

Załącznik nr 4a – arkusz inwentaryzacji zasobów,

Załącznik nr 4b – arkusz analizy ryzyka,

Załącznik nr 5 – upoważnienie do przetwarzania danych osobowych,

Załącznik nr 6 – umowa powierzenia przetwarzania danych osobowych,

Załącznik nr 7 – lista kontrolna dla podmiotu przetwarzającego,

Załącznik nr 8 – klauzule obowiązku informacyjnego i klauzule zgody,

Załącznik nr 9 – arkusz realizacji praw,

Załącznik nr 9a – wniosek o realizację praw,

Załącznik nr 9b – odpowiedź na wniosek osoby,

Załącznik nr 10 – rejestr incydentów.

Powyższa dokumentacja ochrony danych osobowych musi zostać uzupełniona o stan faktyczny. Na potrzeby niniejszego opracowania opisano przykładowe zabezpieczenia, które organizacja mogłaby, ale których oczywiście nie musi posiadać. Opisane procedury mogą jednak pasować do większości organizacji (choć zapewne nie do wszystkich).

Ostatnim działaniem, jakie podejmujemy w ramach wdrażania RODO, jest zatwierdzenie przygotowanej w powyższy sposób dokumentacji ochrony danych osobowych oraz jej wdrożenie (a więc należałoby teraz przeszkolić konkretne osoby w zakresie obowiązków zawartych w tej dokumentacji oraz w zakresie korzystania z załączników do dokumentacji). W ramach wdrażania i doskonalenia systemu ochrony danych osobowych nie można rzecz jasna zapominać o testowaniu nowych procedur oraz istniejących zabezpieczeń.

Podsumowanie

Niniejsza publikacja wskazała, jakie kroki należy podjąć oraz jak mogą one przebiegać przy wdrażaniu nowych przepisów o ochronie danych osobowych. Wszelkie dane znajdujące się w formularzach są przykładowe – mają na celu zobrazowanie możliwych stanów faktycznych oraz różnych sposobów postępowania organizacji z punktu widzenia urzędu oraz podmiotu sektora prywatnego.

Największym wyzwaniem dla każdej organizacji jest dodanie nowych obowiązków związanych z ochroną danych osobowych pracownikom, którzy do tej pory nie stykali się na co dzień z obszarem analizy ryzyka. Po wdrożeniu obowiązków wynikających z RODO może się nagle okazać, że muszą się oni zmierzyć nie tylko z analizą ryzyka w stosunku do zasobów biorących udział w procesach, ale również z analizą ryzyka naruszenia prawa do prywatności osób, czyli DPIA. Oprócz tego właściciele procesów będą musieli zmierzyć się z koniecznością spełnienia obowiązku informacyjnego wobec osób, których dane osobowe przetwarzają. Będą musieli zmierzyć się z procesorami danych, by dokonać ich oceny i zawrzeć z nimi umowy powierzenia przetwarzania danych osobowych. Innymi słowy, niemal cały ciężar wdrożenia RODO zostaje nałożony na właścicieli procesów. W praktyce właścicielami procesów najczęściej zostają kierownicy poszczególnych jednostek organizacyjnych, którzy w swoich działach mają również podwładnych – i to im mogą zlecić wykonanie poszczególnych zadań. W ten sposób cały ciężar wdrożenia RODO w praktyce zostaje przeniesiony na wszystkich pracowników organizacji.

Jak pokazuje niniejsza publikacja, wdrożenie RODO w organizacji nie będzie ani proste, ani trudne, jednak z pewnością okaże się czasochłonne i pracochłonne. Warto również pamiętać o tym, że większość organizacji podchodzi do ochrony danych osobowych czy bezpieczeństwa informacji w kategoriach unikania kary za nieprzestrzeganie przepisów prawa. To jedna z największych pułapek. Organizacja zwykle zamierza uczynić tylko tyle,

ile musi, i nic ponadto, a przecież przepisy RODO wymagają ciągłego doskonalenia systemu ochrony danych osobowych oraz sukcesywnego podnoszenia poziomu bezpieczeństwa danych osobowych! Można nie sprostać temu zadaniu, ryzyko polega bowiem na tym, że o ile najwyższe kierownictwo organizacji z reguły będzie w stanie zaakceptować koszty wdrażania RODO, to dalsze doskonalenie systemu pozostanie pod znakiem zapytania.

Niniejszy zbiór dokumentacji wdrożenia i zarazem poradnik nie obejmuje swoim zakresem wszystkich metod wdrażania RODO, ale nie taki był też jego cel. Każda organizacja musi od czegoś zacząć, a celem tej publikacji było właśnie wprowadzenie Państwa krok po kroku w obszary wiedzy na temat tego, jakie działania należy podjąć, by zbudować w organizacji system ochrony danych osobowych zgodny z RODO. Jednak system ten trzeba będzie w kolejnych latach konsekwentnie doskonalić.