Zabezpieczenia fizyczne danych osobowych – jak je stosować?

Jak już wiemy z naszej serii Ocena ryzyka w RODO, kluczową zasadą RODO jest zasada podejścia opartego na ryzyku (ang. *risk-based approach*).

Oznacza to nic innego, jak konieczność wykonania przez administratora **szczegółowych analiz** prowadzonych przez siebie procesów przetwarzania danych osobowych.

Kolejnym krokiem po analizie ryzyka, jest zastosowania środków zabezpieczających **adekwatnych** do oszacowanego ryzyka!

Dzisiaj zastanowimy się w jaki sposób możemy zabezpieczyć fizycznie przetwarzane przez nas dane osobowe.

Zapraszam do lektury!

Co kryje się pod pojęciem zabezpieczenia fizyczne?

Zabezpieczenia fizyczne, to środki mające na celu:

- zapewnienie **odpowiedniego poziomu ochrony** pomieszczeń, budynków, sprzętów, nośników informacji i elementów systemów informatycznych przed zagrożeniami środowiskowymi np. ogień, woda, pył, promieniowanie elektromagnetyczne,
- **ochronę przed nieupoważnionym dostępem** fizycznym, np. kradzież, włamanie.

Na zabezpieczenia fizyczne składają się:

1) **ochrona fizyczna** – odpowiednio przygotowani do tego celu ludzie, czyli warty, patrole, portierzy,
2) **ochrona techniczna** – na którą składają się:
    - **zabezpieczenia mechaniczne** – szacujące czas jakiego potrzebuje intruz, aby dostać się do wnętrza chronionego pomieszczenia. W tym zakresie mamy do zastosowania drzwi, zamki, kraty, przegrody konstrukcyjne (ściany, stropy), oraz szafki, szafy pancerne, etc.,
    - **zabezpieczenia elektroniczne** – to przede wszystkim systemy sygnalizujące o włamaniu i napadzie, monitoring wizyjny, kontrola dostępu, sygnalizacja pożaru oraz gaszenia i oddymiania.

Najefektywniejszym rozwiązanym jest **zastosowanie zabezpieczeń, które będą ze sobą współdziałać**, np. wzmocnienie drzwi powinno być na tyle solidne, aby w przypadku włamania dać możliwość ochronie budynku na pojawienie w odpowiednim momencie na miejscu. Ochrona powinna być powiadomiona o włamaniu za pomocą systemów zabezpieczeń, najlepiej przed tym, jak intruz znajdzie się w chronionym obszarze.

Podsumowując, zabezpieczenia fizyczne chronią dane przed zagrożeniami środowiskowymi i nieupoważnionym dostępem. Ponadto należy pamiętać, że powinny tworzyć z pozostałymi zabezpieczeniami (technicznymi i organizacyjnymi) kompleksowy system ochrony danych osobowych.

Od czego zacząć?

W pierwszej kolejności należy ustalić listę działań koniecznych do podjęcia.

Poniżej przykładowa lista:

1) Przeprowadzenie audytu mającego na celu wskazanie newralgicznych, pod kątem bezpieczeństwa danych osobowych, obszarów.
2) Przeprowadzenie analizy ryzyka.
3) Dobranie zabezpieczeń stosownie do wartości ryzyka.

Należy zwrócić uwagę, że w trakcie przygotowań do audytu może okazać, się, że będą konieczne do podjęcia jeszcze inne działania, np. związane z profilem działalności naszej organizacji i wymogami innych przepisów prawa niż RODO, ale o tym poniżej.

Jak zabezpieczać dane osobowe?

Kluczowym przepisem w tym zakresie będzie art. 32 ust. 1 RODO:

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (…)

Warte podkreślenia jest to, że w przeciwieństwie do wcześniejszych rozwiązań prawnych administratorom nie wskazuje się już konkretnych środków i procedur w zakresie bezpieczeństwa.

Obowiązuje zasada „*zrób to sam*", co oznacza, że dobór zabezpieczeń musi być dokonany przez samego administratora. Wybrane przez niego rozwiązania powinny zapewnić wysoki poziom bezpieczeństwa, a przede wszystkim odpowiednią skuteczność.

Za błędny dobór środków zabezpieczających, będzie odpowiadał administrator. Warto więc przejrzeć dotychczas stosowane zabezpieczenia – sprawdzić je i ulepszyć, jeśli zajdzie taka potrzeba. Jeśli mamy

w planie nowy proces przetwarzania danych osobowych, należy przeprowadzić analizę ryzyka i na podstawie jej wyników dobrać odpowiednie środki zabezpieczające.

Zabezpieczając fizycznie newralgiczne pod kątem danych osobowych pomieszczania (np. serwerownia, archiwum) należy wziąć pod uwagę m.in.:

- lokalizację,
- zastosowanie drzwi o podwyższonej odporności,
- awaryjne zasilanie,
- wyższy poziom zabezpieczeń przeciwpożarowych,
- monitoring środowiska,
- cichy alarm.

Jeśli okaże się, że chcemy wdrożyć kontrolę dostępu, musimy ustalić jaki system kontroli będzie odpowiedni dla przetwarzanych danych osobowych. W tym zakresie mamy do wyboru trzy poziomy:

1) Poziom niski – bazujący na pamięci np. PIN,
2) Poziom średni – bazujący na kluczach np. karta chipowa,
3) Poziom wysoki – bazujący na cechach biometrycznych np. skaner siatkówki oka.

Należy jednak pamiętać, że zgodnie z art. 22^{1b} Kodeksu pracy, tzw. szczególne kategorie danych, w tym dane biometryczne (art. 9 ust. 1 RODO), mogą być przetwarzane:

- za zgodą osoby ubiegającej się o zatrudnienie bądź pracownika wyłącznie, gdy ich przekazanie następuje z inicjatywy tych osób,
- wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.

Dlatego też, ostatni z poziomów zalecamy tylko w przypadku, w którym mamy możliwość powołania się na przepis prawa, np. obiekt jest szczególnie ważny dla bezpieczeństwa i obronności państwa, a także możemy zastosować się do Rozporządzenia Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony.

Kiedy zabezpieczenia wynikają z przepisów prawa?

Kwestia doboru zabezpieczeń fizycznych okazuje się jednak nie taka łatwa. Często mamy w tym zakresie do zastosowania przepisy innych aktów prawnych niż RODO.

Dla przykładu będą to takie akty jak:

- Rozporządzenie Ministra Kultury z dnia 15 lutego 2005 r. w sprawie warunków przechowywania dokumentacji osobowej i płacowej pracodawców
- Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach - całościowo regulująca prawo archiwalne. Razem z przepisami wykonawczymi oraz resortowymi aktami prawnymi tworzy prawo archiwalne.
- Ustawa o ochronie informacji niejawnych – określa zasady ochrony informacji, które stanowią tajemnicę państwową lub służbową. Przepisy ustawy mają zastosowanie do organów władzy

publicznej, sił zbrojnych Rzeczypospolitej Polskiej i ich jednostek organizacyjnych, Narodowego Banku Polskiego i banków państwowych, państwowych osób prawnych, przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych, których działalność związana jest z dostępem do informacji niejawnych.

- Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia
- Rozporządzenie Rady Ministrów z 26 października 2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji
- Rozporządzenie Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony

Podsumowanie

Dobór zabezpieczeń fizycznych jest istotnym elementem w tworzeniu skutecznego systemu ochrony danych osobowych. To proces, który jest ważny dla administratora ze względu na **wykazanie przez niego zgodności z RODO (zasada rozliczalności)**. To administrator wykazuje w przypadku kontroli, zasadność swoich decyzji w zakresie wybranych środków bezpieczeństwa – dlaczego wybrał taki sposób funkcjonowania ochrony fizycznej , taki system monitoringu, czy taką kontrolę dostępu.

Każdy administrator może zastosować inne zabezpieczenia, ponieważ ma **swobodę wyboru w tym zakresie**, którą zapewnia mu RODO. Pomimo to, nie może zapominać o innych aktach prawnych, opisujących wytyczne, do których ma się zastosować przy przetwarzaniu danych osobowych w określonych przypadkach.

Pamiętajmy też o tym, aby sysytematycznie monitorować i dokonywać przeglądów procesów, w których są przetwarzane dane osobowe. Tylko w ten sposób dobrane zabezpieczenia będą gwaratnować efektywną ochronę.

Wszystkie procedury i zastosowane zabezpieczenia powinny być opisane w Polityce ochrony danych osobowych lub innym analogicznym do niej dokumnecie.

Autor artykułu:

Bogna Tchórzewska, starszy specjalista ds. ochrony danych osobowych

Źródła:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- Krzysztof Liderman, Bezpieczeństwo Informacyjne Nowe Wyzwania, Warszawa 2017