Ochrona danych w 2025

Prognoza i porady

W TYM WYDANIU:

Patrycja Żarska-Cynk
Data Protection Expert

Wyzwania dla ochrony danych osobowych w 2025

W 2025 roku organizacje działające w Unii Europejskiej muszą zmierzyć się z nowymi wymogami prawnymi wynikającymi z RODO oraz przepisów takich jak Akt o Sztucznej Inteligencji (AI Act), Dyrektywa o Bezpieczeństwie Sieci i Informacji 2 (NIS 2), Cyber Resilience Act (CRA) oraz DORA (Digital Operational Resilience Act). Harmonijne wdrożenie tych regulacji wymaga również od ekspertów ds ochrony danych osobowych zrozumienia ich wzajemnych powiązań i współzależności.

Dla przypomnienia:

- **Rozporządzenie o Ochronie Danych Osobowych (RODO)**
  Rozporządzenie unijne, które reguluje przetwarzanie danych osobowych osób fizycznych przez organizacji publiczne i prywatne na obszarze UE. Weszło do stosowania 25 maja 2018 roku.

- **Akt o Sztucznej Inteligencji (AI Act)**
  Rozporządzenie unijne, które reguluje zasady korzystania z systemów opartych na sztucznej inteligencji, klasyfikując je według poziomu ryzyka i określając odpowiednie wymogi dla każdego z nich. Pierwsze obowiązki wchodzą w życie już 2 lutego 2025 r.

- **Dyrektywa o Bezpieczeństwie Sieci i Informacji 2 (NIS 2)**
  Państwa członkowskie UE miały czas do 17 października 2024 r. na implementację przepisów dyrektywy, która ma na celu wzmocnienie cyberbezpieczeństwa w Unii Europejskiej poprzez nałożenie obowiązków na podmioty świadczące usługi kluczowe dla gospodarki i społeczeństwa. W Polsce dyrektywa zostanie wdrożona poprzez nowelizację Ustawy o krajowym systemie cyberbezpieczeństwa.

- **Cyber Resilience Act (CRA)**
  Rozporządzenie unijne, które wprowadza wymogi w zakresie cyberbezpieczeństwa dla producentów sprzętu i oprogramowania, mające na celu zapewnienie bezpieczeństwa produktów cyfrowych na rynku UE. Rozporządzenie weszło w życie 20 dni po opublikowaniu w Dzienniku Urzędowym Unii Europejskiej, czyli 12 listopada 2024 roku, ale główne obowiązki nałożone przez CRA zaczną obowiązywać od 11 grudnia 2027

roku, dając producentom i innym podmiotom czas na dostosowanie się do nowych wymogów. Mimo to wspominam o nim ju dziś ze względu na synergię obowiązków między aktami prawa.

- **Digital Operational Resilience Act (DORA)** Rozporządzenie UE, które ma na celu wzmocnienie odporności cyfrowej instytucji finansowych, takich jak banki czy firmy ubezpieczeniowe, poprzez ustanowienie jednolitych standardów w zakresie zarządzania ryzykiem ICT. Usługi ICT (Information and Communication Technology) to usługi związane z technologiami informacyjnymi i komunikacyjnymi – czyli wszystkie usługi, które pomagają przetwarzać, przechowywać, przesyłać i udostępniać informacje za pomocą komputerów, internetu i sieci. DORA wchodzi w życie 17 stycznia 2025r.

Procedury notyfikacji incydentów i naruszeń bezpieczeństwa

Każda ze wspomnianych regulacji wprowadza własne definicje i wymogi dotyczące zgłaszania incydentów, co wymaga spójności w ich wdrażaniu:

1. RODO: Naruszenie danych osobowych (artykuły 33-34) – skupia się na ochronie danych osobowych, w tym obowiązku zgłaszania naruszeń bezpieczeństwa danych osobowych w związku z dokonaną oceną jego wagi w ciągu 72 godzin.

2. NIS 2: Znaczący incydent sieciowy (artykuł 23) – rozszerza zakres bezpieczeństwa sieci i informacji, wymagając od podmiotów szybkiego zgłaszania incydentów mających wpływ na ich zdolność do świadczenia usług krytycznych.

3. CRA: Poważny incydent mający wpływ na bezpieczeństwo produktu cyfrowego (artykuł 14) – koncentruje się na bezpieczeństwie produktów cyfrowych, nakładając obowiązek zgłaszania aktywnie wykorzystywanych podatności i incydentów.

4. AI Act: (artykuły 73, 55) – wprowadza zasady raportowania poważnych incydentów związanych z systemami AI, szczególnie tymi wysokiego ryzyka, które mogą naruszać prawa podstawowe.

W obliczu tak wielu regulacji wskazana wydaje się **harmonizacja** środków organizacyjnych w poszczególnych podmiotach z wykorzystaniem już obowiązujących zasad notyfikacji incydentów bezpieczeństwa i naruszeń ochrony danych osobowych. Kluczowe znaczenie będzie miała współpraca Inspektorów Ochrony Danych lub działów ochrony danych organizacji z działami IT, co pozwoli na efektywne zarządzanie ryzykiem w cyfrowym środowisku poszczególnych organizacji.

AI Literacy - edukacja dotycząca bezpieczeństwa pracy w cyfrowym środowisku

Art. 4 AI Act nakłada na dostawców i użytkowników systemów sztucznej inteligencji obowiązek organizowania i udziału w szkoleniach dla osób odpowiedzialnych za projektowanie, wdrażanie oraz nadzór nad systemami AI. Szkolenia te mają

zapewnić odpowiednią wiedzę i umiejętności w zakresie bezpiecznego i zgodnego z prawem korzystania z systemów AI z uwzględnieniem ochrony danych osobowych i praw podstawowych.

Umiejętność korzystania ze sztucznej inteligencji stanie się podstawowym filarem strategii AI. **Samo zapewnienie pracownikom dostępu do najnowocześniejszych narzędzi sztucznej inteligencji i oczekiwanie transformacyjnych postępów w zakresie wydajności, produktywności i innowacji nie wystarczy.**

Aby wesprzeć organizację w przygotowaniu się do terminu wejścia w życie pierwszych obostrzeń związanych z AI Act (które obowiązują już od 2 lutego 2025), oraz zmaksymalizować bezpieczeństwo należy budować proosobowe umiejętności posługiwania się sztuczną inteligencją. W tym celu działy ochrony danych osobowych powinny uzupełnić szkolenia z zakresu ochrony danych osobowych o następujące elementy:

1. **Zrozumienie systemów AI:**

   Wyjaśnienie mechanizmów działania systemów sztucznej inteligencji, w tym uczenia maszynowego i algorytmów oraz ich wpływu na przetwarzanie danych osobowych.

2. **Ocena ryzyka AI:**

   Nauka identyfikacji ryzyk związanych z wykorzystaniem AI, takich jak naruszenia prywatności, dyskryminacja czy niezgodność z RODO oraz omijanie tych ryzyk podczas pracy z systemami AI.

3. **Transparentność i wyjaśnialność AI:**

   Przekazywanie wiedzy o konieczności zapewnienia, aby wyniki działania systemów AI były zrozumiałe i możliwe do wyjaśnienia, co jest szczególnie istotne w procesach przetwarzania danych osobowych. Edukacja w zakresie budowania promptów ograniczających halucynacje w systemach AI.

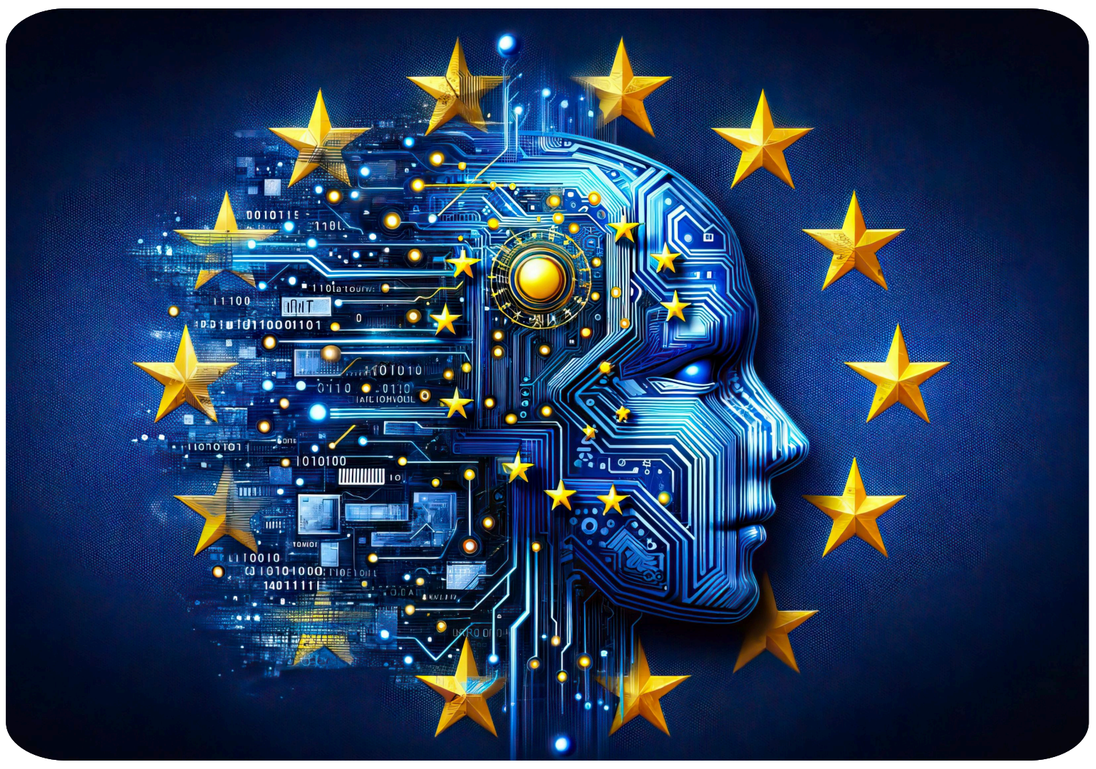
4. **Reagowanie na incydenty związane z AI:**

   Tworzenie procedur postępowania w przypadku naruszenia ochrony danych osobowych przez systemy AI.

Polityka Train Your Own AI (TYOAI) w uzupełnieniu BYOD

Wiele organizacji latami stosowało politykę BYOD (przynieś własne urządzenie). W 2025 r. organizacje będą musiały zacząć myśleć o zasadach BYOAI, a może lepiej TYOAI (train your own AI). Nie minie wiele czasu, zanim pracownicy nietechniczni będą mogli trenować i dostosowywać modele sztucznej inteligencji do własnej pracy, dokumentów i komunikacji, tak aby były one zoptymalizowane do generowania treści, które są bardzo podobne do ich własnych. Jeśli dodasz do tego narzędzia do tworzenia agentów AI bez kodu (np. przeciągnij i upuść), pracownicy będą mogli również zintegrować swoje osobiście wyszkolone modele AI z aplikacjami „zewnętrznymi”, takimi jak poczta e-mail, kalendarz i oprogramowanie zwiększające produktywność, dzięki czemu będą mogli autonomicznie „zlecać” określone zadania, takie jak odpowiadanie na e-maile i planowanie spotkań.

Chociaż wszystko to nie musi stać się rzeczywistością w 2025 roku, to z pewnością jest na horyzoncie i dlatego musi stać się przedmiotem zainteresowania specjalistów ds. zarządzania sztuczną inteligencją w przedsiębiorstwach. W świecie, w którym wszyscy możemy trenować własną sztuczną inteligencję, umiejętność korzystania z AI nie będzie podlegać negocjacjom.



Privacy by Design i Privacy by Default w systemach AI

Głębokie powiązanie między unijną ustawą o sztucznej inteligencji a RODO nie jest przypadkowe. Z ponad 30 odniesieniami do RODO w całym swoim tekście ustawa o sztucznej inteligencji uznaje ten kluczowy związek. Ta integracja ma sens, gdy weźmiemy pod uwagę, że systemy sztucznej inteligencji często przetwarzają dane osobowe, czy to poprzez zbiory danych szkoleniowych, czy interakcje użytkowników podczas wdrażania. **Zarówno ustawa o sztucznej inteligencji, jak i RODO odzwierciedlają podejście UE do regulacji cyfrowych, dzieląc podstawowe zasady, takie jak przejrzystość, uczciwość i odpowiedzialność, z zakresem ochrony praw podstawowych.**

Podczas gdy oceny skutków dla ochrony danych RODO koncentrują się na zagrożeniach dla prywatności osób fizycznych, oceny zgodności/ryzyka lub wpływu na prawa podstawowe ustawy o sztucznej inteligencji badają szersze skutki społeczne systemów sztucznej inteligencji. Organizacje mogą zintegrować te procesy, aby stworzyć bardziej kompleksową i skuteczną strategię zgodności, która dotyczy zarówno ochrony danych, jak i odpowiedzialnego rozwoju sztucznej inteligencji.

Systemy sztucznej inteligencji stawiają wyjątkowe wyzwania. Złożoność modeli sztucznej inteligencji, skala przetwarzania danych i potencjał nieoczekiwanych korelacji wymagają ponownego przemyślenia sposobu wdrażania podstawowych zasad wskazanych w art. 5 RODO w kontekście rozwoju i wdrażania sztucznej inteligencji. Różne poziomy ryzyka wymagają różnych wymogów dla systemów sztucznej inteligencji lub modeli, również w zależności od odpowiedniej roli (tj. dostawcy, podmiotu wdrażającego, importera, dystrybutora). W związku z tym również "podmioty wdrażające" muszą przestrzegać ogólnego obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia, że korzystają z systemów sztucznej inteligencji wysokiego ryzyka zgodnie z instrukcjami użytkowania dołączonymi do takich systemów.

W praktyce organizacje będą musiały pamiętać o wdrażaniu wymogów obu aktów prawnych dla kolejnych faz życia systemów:

1 Faza projektowania

- ☑ dokładne zrozumienie sposobu działania systemów i przepływu danych
- ☑ dokumentowanie wyborów projektowych i potencjalnych zagrożeń wpływających zarówno na prywatność, jak i zgodność ze sztuczną inteligencją
- ☑ analiza możliwości wykorzystania/wdrożenia technik ochrony prywatności, takich jak: Federated Learning, Differential Privacy, Secure Model Deployment
- ☑ przeprowadzenie wstępnej oceny skutków w zakresie ochrony danych (art. 35 RODO) wraz z oceną zgodności/ryzyka lub oceną skutków w zakresie praw podstawowych zgodnie z ustawą o AI (art. 9 i 27 ustawy o AI)

2 Faza rozwoju

- ☑ wdrożenie protokołów minimalizacji danych, okresów przechowywania danych i domyślnych ustawień ochrony prywatności przy przetwarzaniu danych osobowych
- ☑ wdrożenie mechanizmów rejestrowania i powiadamiania, które uwzględniają zarówno wymogi RODO, jak i ustawy o sztucznej inteligencji
- ☑ tworzenie procedur testowania dokładności i stronniczości modeli (wymóg ustawy o sztucznej inteligencji) oraz niezawodności/ bezpieczeństwa systemu (art. 32 RODO, art. 15 ustawy o sztucznej inteligencji)
- ☑ przestrzeganie obowiązków w zakresie dokumentacji: tworzenie rejestrów czynności przetwarzania (art. 30) obok lub w oparciu o dokumentację techniczną systemu AI (art. 11, 18 ustawy o AI)

3 Faza monitorowania

- ☑ regularne oceny zgodności z obiema ramami i usprawnienia
- ☑ ciągłe monitorowanie wydajności systemu i wpływu na prywatność; zapewnienie nadzoru i kontroli ze strony człowieka (art. 22 RODO, art. 14 ustawy o sztucznej inteligencji)
- ☑ prowadzenie dokumentacji i aktualizacja rejestrów i dokumentacji (technicznej)
- ☑ wdrożenie procedur reagowania na incydenty obejmujących zarówno prywatność (art. 33 RODO), jak i incydenty związane ze sztuczną inteligencją (art. 73 ustawy o sztucznej inteligencji). Regularna weryfikacja skuteczności ustawień domyślnych i podejmowanie niezbędnych działań naprawczych (art. 20 ustawy o sztucznej inteligencji).

Ogromnie istotny w tym przypadku jest wymiar edukacji po stronie pionu ds. prywatności w organizacji – Inspektora Ochrony Danych, który zgodnie z kierunkiem rozwoju apetytu na stosowanie nowych technologii przez organizację musi rozwijać i własne kompetencje.

Dziś już mamy kilka pomocnych źródeł informacji, takich jak Opinia Europejskiej Rady Ochrony Danych nr 28/2024 w sprawie kluczowych aspektów ochrony danych osobowych w odniesieniu do opracowywania i wdrażania modeli sztucznej inteligencji, publikacje stanowisk i rekomendacji takich organów ochrony danych jak niemieckie organy z regionu Badenii-Wirtembergii czy Bawarii, jak i stanowiska CNIL czy ICO mimo iż organ ten znajduje się już poza RODO jurysdykcją.

Mamy też pierwsze kary administracyjne (decyzja organu włoskiego Garante dotycząca Open AI). Uważam, że nie tylko 2025 r. ale i rzeczywistość kolejnych lat wymaga od specjalistów ds. prywatności ciągłego pogłębiania wiedzy profilowanej w kierunku w jakim podążają organizacje, które wspieramy ekspercką opinią.

Akt o usługach cyfrowych

Digital Services Act (DSA), czyli Akt o Usługach Cyfrowych, to unijne rozporządzenie mające na celu uregulowanie funkcjonowania platform cyfrowych w Europie. Od 17 lutego 2024 r. wszystkie podmioty objęte zakresem DSA muszą być w pełni zgodne z przepisami tego rozporządzenia.

Choć jego główny cel dotyczy ochrony użytkowników i transparentności w środowisku cyfrowym, wprowadza również szereg obowiązków, które pośrednio wpływają na ochronę danych osobowych. Najważniejsze punkty wspólnych działań zobowiązanych przez DSA platform w obu obszarach regulacyjnych:

1. Platformy muszą dostosować działania reklamowe do obydwu regulacji, co wymaga:
   - uzyskiwania wyraźnej zgody na przetwarzanie danych wrażliwych (RODO);
   - wykluczania wrażliwych kategorii danych z algorytmów reklamowych (DSA).

2. Platformy muszą wypracować procedury, które będą zarówno zgodne z DSA w zakresie przejrzystości moderacji, jak i z RODO w kwestii ograniczania przetwarzania danych osobowych.

3. Platformy muszą łączyć obowiązki wynikające z raportowania naruszeń danych (RODO) i treści nielegalnych (DSA), co może powodować konieczność stworzenia odrębnych procesów i zespołów odpowiedzialnych za każdy obszar.

Akt w sprawie danych

Akt w sprawie danych (Data Act) to unijna propozycja legislacyjna mająca na celu uregulowanie dostępu, udostępniania i wykorzystania danych w Unii Europejskiej. Jego głównym celem jest umożliwienie sprawiedliwego podziału wartości generowanej przez dane pomiędzy przedsiębiorstwa, konsumentów i administrację publiczną, wspierając jednocześnie innowacje i konkurencyjność gospodarki cyfrowej. Rozporządzenie będzie stosowane od 12 września 2025 r.

Data Act obejmuje dane osobowe i nieosobowe, o ile są generowane w ramach użytkowania produktów lub usług opartych na technologii IoT. Rozporządzenie w istotny sposób wpływa na zarządzanie danymi osobowymi i nieosobowymi, mimo że jego głównym celem jest uregulowanie wykorzystania danych generowanych przez urządzenia IoT i inne systemy. Jego przepisy są komplementarne wobec RODO, które pozostaje kluczowym aktem prawnym regulującym ochronę danych osobowych.

Nowością wprowadzoną przez Data Act jest określenie, kto ma prawo dostępu do danych (zarówno osobowych, jak i nieosobowych) i jakie warunki muszą być spełnione przy ich udostępnianiu. Gdy dane osobowe są udostępniane w ramach Data Act, muszą być przetwarzane według zasad RODO, takich jak zgoda użytkownika, przejrzystość i celowość przetwarzania. Data Act rozszerza ochronę na dane nieosobowe, które nie są objęte RODO, ale mogą być krytyczne z punktu widzenia prywatności (np. dane dotyczące urządzeń IoT używanych w domu).

W przypadku technologii i urządzeń IoT rozróżnienie między danymi osobowymi a danymi nieosobowymi może nastręczać problemów, co będzie stanowić wyzwanie dla podmiotów zobowiązanych na gruncie Aktu w sprawie danych. Dla przedsiębiorców znajdujących się w kręgu adresatów Data Act oznaczać to będzie konieczność dostosowania praktyk udostępniania danych do zasad minimalizacji i anonimizacji oraz rozwijania narzędzi umożliwiających łatwe zarządzanie dostępem do danych i ich wymianą zgodnie z przepisami.

ISO 27701 jako samodzielny system zarządzania informacjami o prywatności (PIMS)

Zaktualizowana wersja normy ISO 27701 przeszła już do fazy „zatwierdzania” przez ISO - Międzynarodową Organizację Normalizacyjną. Jest to teraz wersja ostateczna i czeka tylko na formalne zatwierdzenie. Jest to ekscytujące wydarzenie dla tych, którzy czekają na nowy standard, który przekształca ISO 27701 z „bolt-on” ISO 27001 (ISMS) w samodzielny system zarządzania. Pozwoli to organizacjom na certyfikację ich PIMS, nawet jeśli nie posiadają certyfikowanego ISMS.

Możemy spodziewać się, że nowy standard zostanie opublikowany jeszcze w pierwszym kwartale 2025 roku.

Gotowy na zmiany w 2025?

Dynamicznie zmieniające się otoczenie prawne stanowi wyzwanie dla przedsiębiorców, którym stawiane są coraz to nowe obowiązki, wymuszając zmianę sposobu funkcjonowania, modelu biznesowego czy zasad obsługi klienta. Wspierając przedsiębiorców w tych złożonych zadaniach jako doradcy-eksperci w obszarze ochrony danych osobowych nie jesteśmy zwolnieni od dostrzegania potrzeb i obowiązków w otoczeniu prawnym. Wspieramy rozwiązania optymalne regulacyjnie i biznesowo. To podejście powinno charakteryzować każdego specjalistę w zakresie ochrony danych osobowych nie tylko w 2025 roku.

Źródła:

1. Tech Law Trends in 2025: AI and Tech Regulation (Again)
   https://kempitlaw.com/insights/tech-law-trends-in-2025-ai-and-tech-regulation-again/
2. 5 Trends to Watch: 2025 EU Data Privacy & Cybersecurity | Insights
   https://www.gtlaw.com/en/insights/2025/1/published-articles/5-trends-to-watch-2025-eu-data-privacy-cybersecurity
3. A comprehensive EU AI Act Summary [2025 update] - SIG
   https://www.softwareimprovementgroup.com/eu-ai-act-summary/
4. EU AI Act and NIS2 Directive 2025 Compliance Challenges
   https://natlawreview.com/article/5-trends-watch-2025-eu-data-privacy-cybersecurity
5. How will rules and regulations affect cybersecurity and AI in 2025?
   https://www.scworld.com/feature/how-will-rules-and-regulations-affect-cybersecurity-and-ai-in-2025
6. Long awaited EU AI Act becomes law after publication in the EU's ...
   https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal
7. Nowe technologie w ryzach prawnych. Czy w 2025 r. zmierzymy się ...
   https://www.rp.pl/prawo-w-polsce/art41610321-nowe-technologie-w-ryzach-prawnych-czy-w-2025-r-zmierzymy-sie-z-przepisami-na-miare-rodo
8. AI Act | Shaping Europe's digital future - European Union
   https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
9. Data protection 2024: Key trends and predictions for 2025
   https://www.dpocentre.com/data-protection-2024-key-trends-predictions-2025/
10. European Union Artificial Intelligence Act | Deloitte
    https://www.deloitte.com/nl/en/services/risk-advisory/analysis/eu-ai-act.html
11. 5 Trends to Watch: 2025 EU Data Privacy & Cybersecurity
    https://www.gtlaw-dataprivacydish.com/2025/01/5-trends-to-watch-2025-eu-data-privacy-cybersecurity/
12. What to expect from the new EU Parliament and Commission in 2025
    https://www.taylorwessing.com/en/interface/2024/predictions-2025/what-to-expect-from-the-new-eu-parliament-and-commission-in-2025
13. European approach to artificial intelligence
    https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
14. *https://www.iso.org/standard/85819.html*

Aleksander Markiewicz
Legal Counsel

Czy nagrywanie pracowników jest legalne?

Monitoring w miejscu pracy

Monitoring to temat, który wzbudza wiele emocji. Wyjaśniamy kwestie wykorzystania nagrań z monitoringu w pracy, tego, czy rejestrowanie dźwięku jest legalne i sytuacji, w których nielegalny monitoring może zainteresować Urząd Ochrony Danych Osobowych.

Kamery monitoringu - definicja

Zgodnie z definicją słownikową, monitoring to stała obserwacja i kontrola jakichś procesów lub zjawisk. Monitoring może mieć różne cele - zapewnienie bezpieczeństwa pracowników, zapewnienie bezpieczeństwa w miejscu publicznym, weryfikację jakości świadczonych usług czy weryfikację prawidłowości wykonanej pracy. Obecnie monitoring jest narzędziem wykorzystywanym powszechnie, w każdej dziedzinie życia, w sektorze prywatnym oraz w przestrzeni publicznej.

Monitoring może polegać na przetwarzaniu danych w formie wizerunku (wizerunek osoby fizycznej) lub numerów identyfikacyjnych (np. tablice rejestracyjne).

Monitoring w miejscu pracy

Przepisy kodeksu pracy rozróżniają dwie formy monitoringu:

- monitoring wizyjny
- monitoring poczty pracownika

Kodeks przewiduje również inne formy monitoringu, które nie zostały wymienione enumeratywnie.

Do innych form monitoringu można zaliczyć:

- kontrolę położenia pracownika (geolokalizacja);
- kontrolę służbowych rozmów telefonicznych (np. rejestracja czasu połączeń, jakość obsługi klienta);
- monitoring systemów informatycznych (tj. kontrola aktywności pracownika w sieci, np. poprzez wykaz odwiedzanych stron, podgląd pulpitu, cykliczne zrzuty ekranu).

Poza poniżej opisanymi wymogami wynikającymi z kodeksu pracy, w przypadku stosowania monitoringu, a co za tym idzie przetwarzania danych osobowych, na podmiocie, który decyduje o formie monitoringu oraz jego celach i sposobach wykonania (administrator) ciążą obowiązki wynikające bezpośrednio z Rozporządzenia 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) - dalej jako RODO.

Nagrywanie pracowników. Obowiązki pracodawcy

W przypadku gdy pracodawca (administrator) wprowadza np. monitoring wizyjny obejmujący teren parkingu, musi być on świadomy, że nie będzie przetwarzał danych wyłącznie swoich pracowników, ale również dane osób będących kontrahentami, podwykonawcami czy innych osób mogących wejść na teren parkingu.

Wobec tych osób administrator musi przekazać następujące informacje:

- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela
- gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych
- cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania
- jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych
- jeżeli przetwarzanie odbywa się na podstawie zgody - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem
- jeżeli przetwarzanie odbywa się na podstawie zgody - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem
- informacje o prawie wniesienia skargi do organu nadzorczego, czyli Urzędu Ochrony Danych Osobowych
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Monitoring wizyjny w zakładzie pracy

Kodeks pracy reguluje dwie formy monitoringu: monitoring wizyjny oraz monitoring poczty elektronicznej pracownika. Należy pamiętać, że przepisy kodeksu pracy w zakresie monitoringu nie wyłączają stosowania przepisów RODO w tym zakresie.

Monitoring wizyjny dopuszczalny jest w przypadku, gdy jest niezbędny do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

Monitoring nie może obejmować pomieszczeń udostępnianych zakładowej organizacji związkowej. Ponadto monitoring nie może obejmować pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji dopuszczalnego celu (zapewnienie bezpieczeństwa, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji) i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób.
Dodatkowym wymogiem objęty jest monitoring pomieszczeń sanitarnych, który wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.

Kodeks pracy wskazuje również dokładny maksymalny okres przetwarzania danych, który wynosi 3 miesiące od dnia nagrania obrazu. Termin

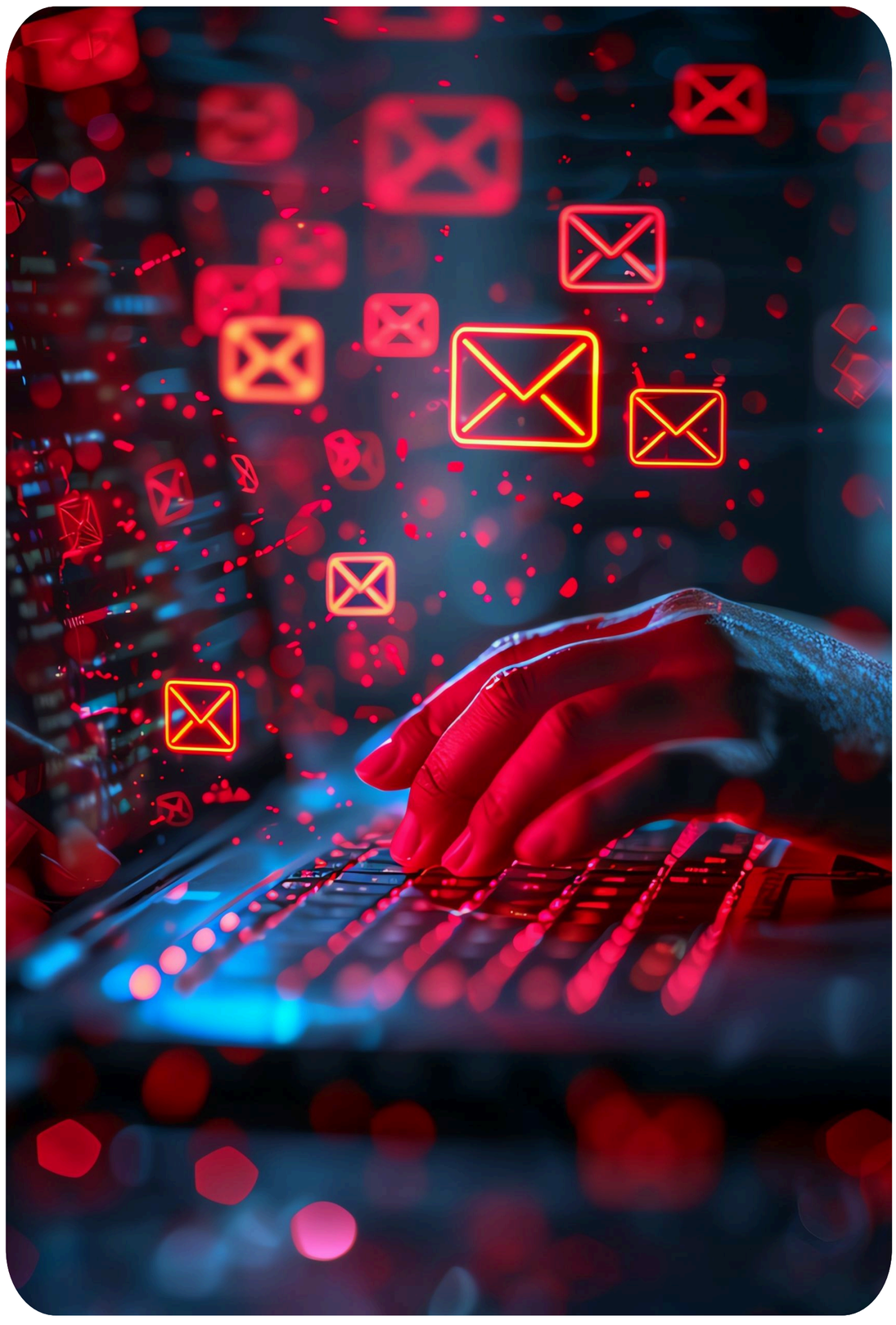
3 miesięcy ulega przedłużeniu w przypadku gdy nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, wówczas termin ulega przedłużeniu do czasu prawomocnego zakończenia postępowania. Wprowadzenie monitoringu wiąże się po stronie pracodawcy z określonymi w kodeksie obowiązkami:

- cele, zakres oraz sposób zastosowania monitoringu należy ustalić w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy;
- pracodawca ma obowiązek poinformować pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem;
- pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o których mowa powyżej;
- pracodawca zobowiązany jest również do oznaczenia pomieszczeń i terenu monitorowanego w sposób widoczny i czytelny – przy użyciu odpowiednich znaków.

Monitoring poczty pracownika

Monitoring poczty elektronicznej pracownika jest dopuszczalny, jeśli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.

Monitoring poczty elektronicznej pracownika nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.



Wprowadzenie monitoringu poczty wiąże się po stronie pracodawcy z określonymi w kodeksie obowiązkami:

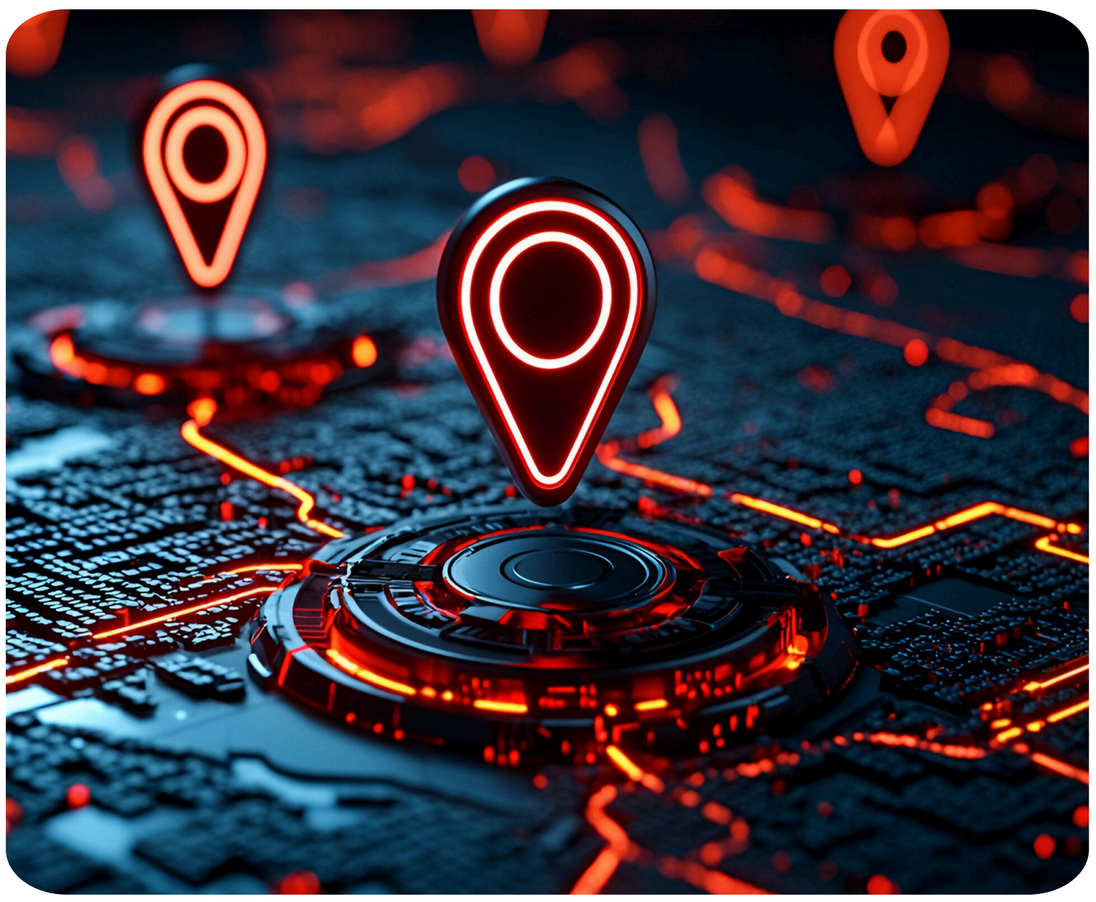
- cele, zakres oraz sposób zastosowania monitoringu należy ustalić w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy
- pracodawca ma obowiązek poinformować pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem
- pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o których mowa powyżej
- pracodawca zobowiązany jest również do oznaczenia pomieszczeń i terenu monitorowanego w sposób widoczny i czytelny – przy użyciu odpowiednich znaków.

Inne formy monitoringu w zakładzie pracy

Jeżeli dla zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, niezbędne jest wprowadzenie innych form monitoringu, wówczas analogiczne zastosowanie mają przepisy dotyczące monitoringu poczty elektronicznej pracownika.

Do innych form monitoringu można zaliczyć:

- kontrolę położenia pracownika (geolokalizacja)
- kontrolę służbowych rozmów telefonicznych (np. rejestracja czasu połączeń, jakość obsługi klienta)
- monitoring systemów informatycznych (tj. kontrola aktywności pracownika w sieci, np. poprzez wykaz odwiedzanych stron, podgląd pulpitu, cykliczne zrzuty ekranu)



Stosowanie monitoringu wizyjnego dla zapewnienia bezpieczeństwa pracowników

Jedną z przesłanek wprowadzenia monitoringu przez pracodawcę na terenie zakładu pracy jest zapewnienie bezpieczeństwa pracowników. Argumentem przemawiającym za stosowaniem systemu monitoringu dla bezpieczeństwa może być cykl produkcyjny stwarzający niebezpieczeństwo i wymagający ciągłego monitorowania lub przypadki incydentów (np. bójka pracowników) do jakich doszło na terenie zakładu pracy.

Dla poprawy bezpieczeństwa, pracodawca w swojej firmie za pomocą kamer może rejestrować obraz. Musi jednak pamiętać konieczności oznaczenia takiego terenu np. poprzez informację "obiekt monitorowany', co stanowi dla pracowników informację o obecności kamer w miejscu pracy.

Inną przesłanką uzasadniającą wprowadzenie monitoringu może być kontrola produkcji lub ochrona mienia pracodawcy.

Monitoring wizyjny w miejscach publicznych

Monitoring w miejscach publicznych prowadzony przez jednostki samorządu terytorialnego (gmina, powiat, województwo) został szczegółowo uregulowany w ustawach samorządowych. Ustawa o samorządzie gminnym wskazuje, że gmina w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej może stosować środki techniczne umożliwiające rejestrację obrazu (monitoring) w obszarze przestrzeni publicznej, za zgodą zarządzającego tym obszarem lub podmiotu posiadającego tytuł prawny do tego obszaru lub na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy lub jednostek organizacyjnych gminy, a także na terenie wokół takich nieruchomości i obiektów budowlanych, jeżeli jest to konieczne do zapewnienia porządku publicznego i bezpieczeństwa obywateli lub ochrony przeciwpożarowej i przeciwpowodziowej.

Podobnie jak w kodeksie pracy, również w ustawie o samorządzie gminnym wskazano, że monitoring nie może obejmować pomieszczeń sanitarnych, szatni, stołówek, palarni oraz obiektów socjalnych.

Również analogicznie został określony czas przechowywania nagrań – nagrania obrazu zawierające dane osobowe przetwarza się wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania, z wyjątkiem sytuacji, w których nagrania zostały zabezpieczone, zgodnie z odrębnymi przepisami.
Ponadto nieruchomości i obiekty budowlane objęte monitoringiem należy oznaczyć w sposób widoczny i czytelny informacją o monitoringu, w szczególności za pomocą odpowiednich znaków. Ustawodawca nałożył również na samorząd gminny obowiązek stosowania środków zabezpieczających przetwarzanie danych z monitoringu, w szczególności uniemożliwiających ich utratę lub bezprawne rozpowszechnienie, a także uniemożliwienie dostępu do danych osobom nieuprawnionym.

Analogiczne przepisy dotyczące monitoringu w miejscach publicznych znajdują się w ustawie o samorządzie powiatowym oraz w ustawie o samorządzie województwa.

Pracodawca chce rejestrować dźwięk. Czy monitoring z dźwiękiem jest legalny?

Analizując przepisy kodeksu pracy (art. 22(2)) zgodnie z zasadą celowości oraz literalną wykładnią tego przepisu - nadzór na terenie zakładu pracy lub terenem wokół zakładu pracy może obejmować tylko środki techniczne umożliwiające rejestrację wyłącznie obrazu, a co za tym idzie brak jest podstaw do wykorzystania urządzeń rejestrujących obraz i dźwięk jednocześnie.

Stosowanie rozwiązań rejestrujących jednocześnie obraz i dźwięk może być uznane za nadmierne przetwarzanie danych osobowych i wiązać się z odpowiedzialnością administracyjną, cywilną, a nawet odpowiedzialnością na gruncie przepisów karnych.
Podobnie uregulowane jest korzystanie z monitoringu wizyjnego prowadzonego przez samorządy (gmina, powiat, województwo), przepisy te – jak wyżej zostało wskazane - pozwalają jedynie na wprowadzenie monitoringu wizyjnego – bez możliwości nagrywania dźwięku.

Podsumowanie

Monitoring dopuszczalny jest w różnych formach i różnym celu, jednak jest mocno ograniczony przepisami, nie tylko kodeksu pracy, ale również ustaw samorządowych. Podobnie uregulowane są zasady wprowadzenia monitoringu i wymogi jakie musi on spełniać – zarówno dla pracodawcy, jak i dla samorządów.

Zaplanowanie i wprowadzenie monitoringu wiąże się ze spełnieniem obowiązków wynikających nie tylko z przepisów prawa samorządowego i kodeksu pracy, ale również z licznymi obowiązkami wynikającymi z ochrony danych osobowych.
Jeśli prowadzony monitoring nie spełnia wymagań polskiego prawa istnieje ryzyko, że ktoś może skierować zgłoszenie do Urzędu Ochrony Danych Osobowych.

Plan kontroli sektorowych UODO na 2025

Urząd Ochrony Danych Osobowych opublikował plan kontroli sektorowych na 2025 rok. Wśród priorytetów znalazło się bezpieczeństwo danych medycznych oraz przetwarzanie danych dzieci.

W planie znalazły się sektory, w których coraz częściej pojawiają się zagrożenia naruszania przepisów o ochronie danych osobowych. UODO wziął też pod uwagę obszary, które budzą duże społeczne zainteresowanie.

Plan kontroli sektorowych UODO na 2025 rok przedstawia się następująco:

1. **Organy, które przetwarzają dane osobowe w Wielkoskalowych Systemach Unii Europejskiej,**

   w tym przetwarzanie danych osobowych SIS/VIS na podstawie przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczpospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz.U. z 2023 r. poz. 1355 ze zm.), aktów wykonawczych oraz przepisów Unii Europejskiej).

2. **Podmioty, które przetwarzają dane o stanie zdrowia**

   Kontrolowany jest sposób zapewnienia bezpieczeństwa danych osobowych.

3. **Podmioty, które przetwarzają dane dzieci**

   Kontrolowane jest przetwarzanie wizerunku dzieci, gdy wymagana jest zgoda wyrażona przez rodziców lub opiekunów prawnych.

4. **Administratorzy danych**

   kontrolowana realizacja obowiązku wynikającego z art. 33 ust. 5 rozporządzenia 2016/679, polegającego na dokumentowaniu wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI