1

JAKIE DANE OSOBOWE MOŻE PRZETWARZAĆ PRACODAWCA I JAK DŁUGO

1.1 WSTĘP

Unijne rozporządzenie o ochronie danych osobowych jest stosowane we wszystkich krajach członkowskich i wiąże je bez potrzeby implementacji do prawa krajowego. Jednak nie oznacza to braku przepisów uszczegóławiających, czy precyzujących obszar ochrony danych w prawie polskim. Podstawa prawna będąca uzupełnieniem do rozporządzenia jest niewątpliwie ustawa z 10 maja 2018 r. o ochronie danych osobowych, ale nie tylko. Dla zapewnienia zgodności przepisów krajowych z przepisami RODO konieczne było dokonanie zmian w wielu aktach prawnych. Ustawodawca kompleksowo znowelizował właściwe przepisy prawa Ustawą o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) z dnia 21 lutego 2019 r. Zmiany dotyczyły 162 ustaw, w tym Kodeksu pracy oraz Ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych. Ustawy te w szerokim zakresie regulują katalog danych osobowych jaki jest zobligowany przetwarzać pracodawca będący Administratorem Danych. Zmiany objęły także zagadnienie monitoringu wizyjnego poprzez wprowadzenie nowych przepisów do Kodeksu pracy. Pracodawca przetwarzając dane osobowe jako Administrator Danych musi pamiętać również o retencji danych, a więc okresie przechowywania i terminach usuwania danych osobowych.

1.2 ZAKRES GROMADZONYCH DANYCH OSOBOWYCH

Pracodawca jako Administrator Danych przetwarza dane osobowe zwykłe, dane szczególnej kategorii oraz dane o wyrokach skazujących. Dane osobowe mogą być przetwarzane zgodnie z zasadą legalności tylko wtedy, gdy spełniony jest co najmniej jeden warunek przewidziany w art. 6 ust. 1 lit. a-f lub w art. 9 ust. 2 lit. a-j RODO. Dane zwykłe to informacje o zidentyfikowanej lub możliwej do

zidentyfikowania osobie fizycznej (osobie, której dane dotyczą): imię, nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej [2]. Dane zwykłe przetwarzane są przez Administratora Danych na podstawie przesłanek zawartych w art. 6 ust. 1 RODO:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, podyktowanego prawem Unii lub państwa członkowskiego;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą , lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów maja interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba , której dane dotyczą jest dzieckiem.

Jakie dane osobowe zwykłe może przetwarzać pracodawca określa bardzo szczegółowo Kodeks pracy w art. 22^1 określa katalog danych osobowych, których pracodawca żąda od osoby ubiegającej się o zatrudnienie jak i pracownika. Przy rekrutacji pracodawca żąda następujących danych: imię (imiona) i nazwisko, datę urodzenia, dane kontaktowe wskazane przez taką osobę, wykształcenie, kwalifikacje zawodowe, przebieg dotychczasowego zatrudnienia. Podanie przez osobę ubiegającą się o pracę danych związanych z wykształceniem, kwalifikacjami zawodowymi i przebiegiem zatrudnienia jest zasadne tylko wtedy gdy jest to niezbędne do wykonywania określonej pracy na określonym stanowisku. Zatrudniony pracownik zobligowany jest uzupełnić dane o adres zamieszkania, numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość. Ponadto pracodawca może żądać od pracownika innych danych, a także danych osobowych dzieci i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy. Pytanie o wykształcenie i przebieg dotychczasowego zatrudnienia jest zasadne wtedy, gdy nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie. Żądanie numeru rachunku płatniczego jest uzasadnione, jeżeli

pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych [4]. Zwrócić uwagę należy na fakt, że jeżeli pracodawca podczas rekrutacji nie zapyta o kwalifikacje zawodowe, traci taką możliwość przy zatrudnieniu pracownika.
Pracodawca żąda od pracownika innych danych osobowych niż wymienionych w kodeksie pracy, gdy jest to niezbędne do zrealizowania uprawnienie lub spełnienia obowiązku wynikającego z przepisu prawa [4]. Udostępnienie pracodawcy danych następuje w formie oświadczenia osoby, której dane dotyczą. Pracodawca jako Administrator Danych może również przetwarzać dane biometryczne pracownika ale tylko 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.
Przetwarzanie danych szczególnej kategorii co do zasady jest na gruncie RODO zabronione. Do katalogu tych danych zaliczamy dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane dotyczące zdrowia, seksualności lub orientacji seksualnej jak również dane genetyczne oraz dane biometryczne. Pracodawca może przetwarzać te dane tylko i wyłącznie w przypadku, gdy wystąpi co najmniej jedna z przesłanek wskazanych w art. 9 ust. 2 RODO:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie tych danych;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonania prawa w związku z zatrudnieniem pracownika w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osób, których dane dotyczą , bądź innej osoby fizycznej, która jest fizycznie bądź prawnie niezdolna do wyrażenia zgody;
- przetwarzanie wyłącznie w stosunku do członków organizacji (fundacji, stowarzyszenia, inne niezarobkowe podmioty ocelach politycznych, światopoglądowych, religijnych lub związkowych) oraz osób utrzymujących z nimi stałe kontakty (np. współpracownicy, wolontariusze);
- przetwarzanie danych będzie możliwe gdy osoba, której dane dotyczą, w sposób oczywisty je upubliczni;
- przetwarzanie danych niezbędne do ustalenia i dochodzenia roszczeń, w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- przetwarzanie danych podyktowane jest ważnym interesem publicznym wyrażonym w prawie krajowym lub unijnym;
- przetwarzanie danych w celach profilaktyki zdrowotnej lub medycyna pracy: ocena zdolności pracownika do pracy, dokonywanie diagnozy medycznej, zapewnienie opieki zdrowotnej lub zabezpieczenia społecznego, leczenie

pacjentów i zarzadzanie systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego zgodnie z przepisami prawa krajowego;

- przetwarzanie danych podyktowane jest ważnym interesem publicznym w dziedzinie zdrowia publicznego (ochrona przed transgranicznymi zagrożeniami zdrowotnymi lub o zapewnienie wysokich standardów jakości bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych);
- przetwarzanie jest niezbędne do celów archiwalnych, badań naukowych oraz celów statystycznych zgodne z prawem krajowym i nie może naruszać istotnych prawa do ochrony danych [1].

Wśród danych szczególnie chronionych pracodawca przetwarza takie dane jak: orzeczenie lekarskie stwierdzające brak przeciwwskazań do pracy na danym stanowisku, informacje o przynależności związkowej w celu odprowadzania składek członkowskich, ewentualne dane medyczne dotyczące postępowania powypadkowego, informacje o zawartości alkoholu we krwi, dane zawarte w zwolnieniach lekarskich oraz dane niezbędne do realizacji świadczeń socjalnych.

Pracodawca musi pamiętać, że udostępniane dane przez osobę uprawnioną do korzystania z Funduszu w celu przyznania ulgowej usługi i świadczenia oraz dopłaty i ustalenia ich wysokości następuje tylko i wyłącznie w formie oświadczenia. Pracodawca może żądać udokumentowania tych danych w zakresie niezbędnym do ich potwierdzenia. Potwierdzenie może odbywać się w szczególności na podstawie oświadczeń i zaświadczeń o sytuacji życiowej (w tym zdrowotnej), rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu [5].

Dane dotyczące wyroków skazujących Administrator Danych może przetwarzać wyłącznie na podstawie art. 6 ust. 1 RODO jedynie pod nadzorem władz publicznych lub jeżeli takie przetwarzanie jest dozwolone prawem Unii lub państwa członkowskiego. Do danych tych zaliczamy np. dane z Krajowego Rejestru Karnego z którego pracodawca uzyskuje informacje dotyczące m. in. członków zarządu w celu wzięcia udziału w przetargu regulowanym przez prawo zamówień publicznych.

Ustawodawca dał możliwość pracodawcy oparcie przetwarzanie danych osobowych pracownika na podstawie art. 6 ust. 1 lit a, czyli zgodzie. Zgoda dotyczy tylko i wyłącznie danych osobowych, o których mowa w art. 9 unijnego rozporządzenia, czyli szczególnej kategorii danych. W stosunkach pracowniczych zgoda jako podstawa prawna przetwarzania danych jest podstawą niewystarczająco trwałą m. in. z uwagi na możliwość jej odwołania w każdym czasie i wynikające stąd konsekwencje. Po wycofaniu zgody przez pracownika pracodawca nie może przetwarzać danych, które zostały oparte na jej postawie. Dane te muszą zostać usunięte.

Pracodawca jako Administrator Danych musi pamiętać, że wszystkie osoby dopuszczone do przetwarzania szczególnej kategorii danych muszą posiadać pisemne upoważnienie do przetwarzania danych oraz zostać zobligowane do

zachowania ich w tajemnicy. Nic nie stoi na przeszkodzie, żeby pracodawca taki sam wymóg zastosował do pracowników przetwarzających dane osobowe zwykłe oraz dane dotyczące wyroków skazujących.

1.3 MONITORING WIZYJNY A OCHRONA DANYCH OSOBOWYCH PRACOWNIKA

Stosowanie monitoringu wizyjnego od wielu lat budzi kontrowersje polskiego organu nadzorczego w zakresie ochrony danych osobowych. Prezes Urzędu Ochrony Danych Osobowych określa ten rodzaj kontroli jako „inwazyjną formę przetwarzania danych osobowych" [6]. Dodatkowe wątpliwości budzi brak jednolitych regulacji w tym zakresie. Ustawodawca jedynie fragmentarycznie odnosi się do regulacji zasad, zakresu i celu wykorzystania monitoringu wizyjnego w określonych sferach życia jak np. w sferze pracy zawodowej i relacji z pracodawcą. W ramach monitoringu wizyjnego o przetwarzaniu danych osobowych możemy mówić wówczas, gdy na obrazie monitoringu wizyjnego pojawiają się dane pozwalające na identyfikację osób fizycznych. Dodatkowo, dane te muszą zostać zapisane, a więc utrwalone. Nie można dokonywać jakichkolwiek operacji na danych osobowych, jeżeli nie są one wcześniej zapisane na trwałym nośniku (np. rejestrator cyfrowy wyposażony w dysk twardy). W tym kontekście należy mieć na uwadze, że stosownie monitoringu wizyjnego nie zawsze będzie się wiązało z przetwarzaniem danych osobowych. W przypadku wykorzystania monitoringu wyłącznie do podglądu na żywo konkretnego miejsca, gdy obraz nie jest zapisywany, nie będzie dochodziło do utrwalania danych a tym samym do ich przetwarzania [3]. Najczęściej przetwarzanymi kategoriami danych jest wizerunek osoby przebywającej w obszarze monitorowanym. Wizerunek w wielu przypadkach prowadzi do ustalenia tożsamości konkretnej osoby, a także pozwala określić numer rejestracyjny samochodu jakim się porusza [3]. Pracodawca jako podmiot monitorujący jest Administratorem Danych, a tym samym decyduje o celach, zakresie oraz sposobie zastosowania monitoringu wizyjnego. Informacje te pracodawca jest zobligowany zawrzeć w układzie zbiorowym pracy lub regulaminie pracy albo w obwieszczeniu jeżeli nie jest objęty układem zbiorowym pracy lub nie jest zobowiązany do ustalenia regulaminu pracy [4]. Celem zastosowania monitoringu wizyjnego może być zapewnienie bezpieczeństwa pracowników, ochrona mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Swoim zakresem monitoring może obejmować całość zakładu lub jego najbardziej newralgiczne obszary. Ważnym jest, aby określony został czas przechowywania nagrań, który na dzień dzisiejszy zgodnie z zapisami Kodeksu pracy nie może przekroczyć 3 miesięcy od dnia nagrania – chyba, że nagrania stanowią dowód w sprawie termin ulega przedłużeniu do czasu prawomocnego zakończenia postepowania [4]. Ponadto przydatny dla celów kontrolnych jest opis struktury monitoringu oraz rodzaj

stosowanych kamer a także komu kopie z nagrań monitoringu mogą zostać przekazane. Pracodawca jako administrator danych musi pamiętać o konieczności spełnienia obowiązku informacyjnego dla osób wchodzących na teren objęty monitoringiem.

Informacja taka powinna zawierać dane Administratora Danych, podstawę prawną przetwarzania danych, opis obszaru objętego monitoringiem z wyraźnymi znakami graficznymi (kamery), określenie praw jakie przysługują osobom wchodzącym na teren monitoringu wizyjnego oraz gdzie znajdują się szczegółowe informacje na temat przetwarzania danych oraz przysługujących uprawnień. Jeśli monitoring wizyjny obsługuje podmiot świadczący usługę ochrony, wówczas z takim podmiotem pracodawca powinien zawrzeć umowę powierzenia przetwarzania danych osobowych.

Podczas wprowadzania monitoringu wizyjnego pracodawca musi pamiętać, że monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej ani też pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba, że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu w jakim został monitoring wprowadzony i nie naruszy godności oraz innych dóbr osobistych pracownika. Monitoring pomieszczeń sanitarnych wymaga uprzedniej zgody zakładowej organizacji związkowej. W przypadku jej braku zgodę muszą wyrazić przedstawiciele pracowników wybranych w trybie przyjętym u danego pracodawcy [4].

Jeżeli pracodawca powziął decyzję o wprowadzeniu monitoringu wizyjnego musi o tym fakcie poinformować pracowników nie później niż 2 tygodnie przed jego uruchomieniem. Ponadto pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje dotyczące celu, zakresu i sposobu zastosowania w zakładzie pracy monitoringu wizyjnego [4].

Pracodawcy przysługuje również prawo kontroli służbowej poczty elektronicznej pracownika, a także wprowadzenie GPS w samochodach służbowych pod warunkiem, że jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, zaś monitoring poczty elektronicznej nie narusza tajemnicy korespondencji oraz innych dóbr pracownika.

1.4 RETENCJA DANYCH

Przez retencję danych rozumiemy przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust.1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne

i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania") [2]. Po zakończeniu przetwarzania, dane powinny zostać usunięte, zanonimizowane lub też przekazane podmiotowi uprawnionemu ustawowo do ich przejęcia od administratora (np. przekazane do archiwum państwowego). Retencja danych osobowych jest ściśle związana z obowiązkami informacyjnymi Administratora Danych. Treść obowiązku informacyjnego podyktowana art. 13 i art. 14 RODO obliguje go do podania okresu przechowywania danych. Tak więc niezbędnym staje się przegląd i nadzorowanie zbiorów przetwarzanych danych.

Przesłanki usunięcia danych osobowych:

- cele w których dane były zbierane zostały osiągnięte, np. zakończona rekrutacja;
- brak podstawy prawnej do przetwarzania danych osobowych, np. prawo do bycia zapomnianym;
- zgłoszenie sprzeciwu wobec przetwarzania danych osobowych, np. marketing bezpośredni;
- przetwarzanie danych odbywa się niezgodnie z prawem np. nadmiarowość danych;
- prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator, nałożyło na Administratora danych obowiązek usunięcia danych osobowych;
- brak zgody podmiotu danych na ich przetwarzanie.

Jeżeli pracodawca upubliczni dane osobowe pracowników musi pamiętać że zgodnie z art. 17 jeśli ciąży na nim obowiązek usunięcia danych osobowych, powinien dołożyć wszelkich starań, aby tego dokonać. Ponadto, administrator ma obowiązek poinformowania innych administratorów przetwarzających dane osobowe o konieczności ich usunięcia. Jest to zapis wzmacniający prawo do „bycia zapomnianym" w Internecie.

Warto dodać, że osoba, która udzieliła zgody na przetwarzanie danych osobowych jako dziecko, również ma prawo do ich usunięcia. Wskazuje się, że dziecko nie jest w pełni świadomie ryzyka związanego z przetwarzaniem danych [7].

1. Przy retencji danych należy zwrócić uwagę, że w stosunku do tych samych danych mogą mieć zastosowanie różne terminy retencji. W takiej sytuacji należy przechowywać dane zgodnie z tym dłuższym terminem retencji. Może również dojść do sytuacji, w której retencja danych ulegnie wstrzymaniu i przedłużeniu. Do takiej sytuacji może dojść w związku z prowadzonym przez Administratora Danych lub wobec niego postępowaniem, cywilnym, karnym lub administracyjnym, co wymaga zabezpieczenia materiału dowodowego. Takie wstrzymanie biegu terminu retencji następuje na okres trwania postępowania.
2. Pracodawca żeby wywiązać się z obowiązku respektowania obowiązku retencji danych powinien przyjąć w organizacji odpowiednia procedurę, w której określi właściwe zarządzanie danymi osobowymi w tym obszarze.

3. Konsekwencją naruszenia RODO w zakresie dopuszczalnej retencji danych osobowych może być kara, o której mowa w art. 83 ust. 5 lit. a i b RODO, tj. administracyjna kara pieniężna w wysokości do 20000000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Nałożenie na ADO administracyjnej kary pieniężnej nie zwalnia go z ewentualnej odpowiedzialności cywilnej wobec osób, których dane dotyczą, zgodnie z art. 79 ust. 1 RODO.

1.5 PODSUMOWANIE

Unijne rozporządzenie jak i polskie prawodawstwo spowodowały, że dla pracodawcy obszar ochrony danych osobowych stał się wymagający i restrykcyjny. Katalog danych osobowych jakich pracodawca żąda od pracownika jest ściśle określony, a każde inny zakres danych musi mieć własne podstawy prawne przetwarzania. Dodatkowe problemów przysparza regulacja retencji danych w przedsiębiorstwie, która wbrew wytycznym nie jest prosta i jednoznaczna. Administrator Danych usuwając dane osobowe musi pamiętać, że dane podlegające retencji mają zostać zniszczone w sposób trwały i nieodwracalny.

LITERATURA

[1] Dmochowska A., Zadrożny M.: *Unijna reforma ochrony danych osobowych*. Wydawnictwo C.H. BECK. Warszawa 2018.
[2] Sibiga G., Syska K.: *Ogólne rozporządzenie o ochronie danych. Podręczny zbiór przepisów o ochronie danych osobowych, zestawień, schematów, oraz wzorów rejestru czynności przetwarzania*. Wydawnictwo C.H. Beck, Warszawa 2017.
[3] Wezgraj J.: *Monitoring wizyjny a ochrona danych osobowych – wymagania RODO, przepisy sektorowe oraz wytyczne UODO*. Wydawnictwo PRESSCOM Sp. z o.o. Wrocław 2019.
[4] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn. Dz.U. 2019 r. poz. 1040 ze zm.).
[5] Ustawa z dnia 4 marca 199 r. o zakładowym funduszu świadczeń socjalnych (tekst jedn. Dz.U. 2019 r. poz. 1352).
[6] Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego. Warszawa, 2018.
[7] https://www.politykabezpieczenstwa.pl/pl/a/retencja-danych-osobowych-przechowywanie-danych-osobowych-w-ograniczonym-horyzoncie-czasowym

Data przesłania artykułu do Redakcji: 02.2020
Data akceptacji artykułu przez Redakcję: 03.2020

JAKIE DANE OSOBOWE MOŻE PRZETWARZAĆ PRACODAWCA I JAK DŁUGO

Streszczenie: W artykule przedstawiono jakie dane i na jakiej podstawie mogą być przetwarzane przez pracodawcę jako Administratora Danych. Przedstawiono także wskazówki, które należy uwzględnić w wdrażaniu monitoringu wizyjnego. Zwrócono uwagę na konieczność uregulowania obszaru retencji danych oraz problemów w tym zakresie.

Słowa kluczowe: administrator, pracodawca, pracownik, podmiot danych, monitoring, retencja danych

WHAT KIND OF PERSONAL DATA CAN AN EMPLOYER PROCESS AND FOR HOW LONG

Abstract: The article presents what kind of data and on which basis can an employer process as a data controller. The article presents as well the guidelines that should be taken into account in the implementation of video monitoring. Attention was paid to the need of regulating the data retention area and problems in this respect.

Key words: controller, employer, employee, data subject, video monitoring, data retention

Marzena Smolarska
FAMUR S.A.
ul. Armii Krajowej 51, 40-698 Katowice, Polska
e-mail: msmolarska@famur.com
tel: +48 781 550 418