ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.5

DOMINIKA DÖRRE-KOLASA
ORCID: 0000-0002-4134-741X
Uniwersytet Jagielloński

PRZETWARZANIE DANYCH OSOBOWYCH PRACOWNIKÓW W RAMACH TAK ZWANYCH INNYCH FORM MONITORINGU

Abstrakt: Powszechna dostępność nowych technologii pozwala pracodawcom na stosowanie dotychczas niewystępujących w środowisku pracy rodzajów monitorowania aktywności pracowników. Co więcej — upowszechnienie się pracy zdalnej, w połączeniu z pojawieniem się nowej regulacji w kodeksie pracy, w naturalny sposób zwiększa zainteresowanie pracodawców procesami przetwarzania danych na temat aktywności pracowników *online*, jak również danych o lokalizacji. Technologie wykorzystywane w ramach innych form monitoringu mogą być bardzo skuteczne w wykrywaniu naruszeń obowiązków pracowniczych, ochronie informacji poufnych czy też służyć zwiększaniu efektywności pracy, lecz jednocześnie stwarzają poważne zagrożenia dla ochrony prywatności i danych osobowych. Aplikacje służące do cyfrowej analizy danych mogą bowiem działać w sposób niezauważalny dla użytkowników urządzeń, przez co zagrażają ich prywatności bardziej niż na przykład kamery CCTV. W związku z tym uzasadniona jest ponowna rewizja oceny skutków dla ochrony danych oraz baczna analiza podejmowanych działań z uwzględnieniem zasad wynikających zarówno z kodeksu pracy, jak i RODO. Skorzystanie przez pracodawców z danych pozyskanych w sposób niezgodny z przepisami może się spotkać z poważnymi konsekwencjami prawnymi.

Słowa kluczowe: monitoring, praca zdalna, GPS, kontrola pracowników, inne formy monitoringu

UWAGI WPROWADZAJĄCE

Ustawą[1] z dnia 10 maja 2019 roku wprowadzono do kodeksu pracy przepisy dotyczące różnych rodzajów monitoringu, to jest monitoringu wizyjnego (art. 22^2 k.p.), monitoringu poczty elektronicznej (art. 22^3 § 1 k.p.) oraz innych form monitoringu (art. 22^3 § 4 k.p.). Skorzystano w ten sposób z przewidzianej w RODO możliwości uszczegółowienia w przepisach krajowych zasad ochrony praw i wolności jednostek w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem.

[1] Ustawa o ochronie danych osobowych z dnia 10 maja 2019 r., Dz.U. z 2018 r. poz. 1000.

© for this edition by CNS

Zgodnie z art. 88 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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)[2] — dalej: RODO — państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy. Przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.

Zawarta w kodeksie pracy regulacja dotycząca monitoringu jest zatem tą „bardziej szczegółową regulacją" w stosunku do przepisów RODO, która precyzuje ten aspekt przetwarzania danych osobowych w kontekście zatrudnienia. Nie można jednak zapominać, że do przetwarzania danych osobowych w ramach każdej z form monitoringu powinny być stosowane nie tylko przepisy kodeksu pracy, ale także przepisy RODO. Podejmując decyzję o wprowadzeniu monitoringu, jak również dokonując okresowej oceny jego funkcjonowania, należy mieć na uwadze zwłaszcza zasady przetwarzania danych osobowych określone w art. 5 RODO, a więc: zasadę rzetelności i legalności (zgodności z prawem), zasadę ograniczenia celu, zasadę minimalizacji danych, zasadę prawidłowości (poprawności danych), zasadę ograniczenia przechowywania, zasadę integralności i poufności (bezpieczeństwa danych) oraz zasadę rozliczalności.

Zgodnie z zasadami przetwarzania danych osobowych, które powinny być przez pracodawców stosowane niezależnie od stosowanej technologii[3], dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu"). Dane te powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

[2] Dz.Ur.UE. L 119 z 4.05.2016 r. ze zm., s. 1.

[3] *Opinia 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy, WP 249*, Archiwum GIODO, 21.02.2018, https://archiwum.giodo.gov.pl/pl/file/13179 (dostęp: 24.10.2022).

© for this edition by CNS

W k.p. ustawodawca dokonał dychotomicznego podziału dopuszczalnych form monitoringu, przyporządkowując do nich określone cele, które mogą uzasadniać wprowadzenie „szczególnego nadzoru" czy też „kontroli". Elementem, który pojawia się w obydwu przypadkach, jest uzależnienie decyzji pracodawcy o wprowadzeniu monitoringu od tego, czy ocenił podjęte działania jako niezbędne do osiągnięcia tych celów. Zarówno art. 22^2, jak i art. 22^3 k.p. rozpoczynają się od sformułowań „jeżeli jest to niezbędne do zapewnienia". Oznacza to, że decyzji o wprowadzeniu, czy też kontynuowaniu stosowanego wcześniej monitoringu powinna bezwzględnie towarzyszyć ocena, czy monitoring jest niezbędny do osiągnięcia wskazanych w przepisach celów. Wydaje się, że ową niezbędność można rozumieć szerzej niż tylko niemożność osiągnięcia tych celów bez zastosowania monitoringu. W mojej ocenie mieści się w tym zakresie również racjonalność działania, która jest uzasadniona pod względem organizacyjnym i kosztowym.

Stosując monitoring, pracodawca przetwarza dane osobowe pracowników na podstawie art. 6 ust. 1 lit. f RODO, to jest do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, z wszystkimi tego konsekwencjami.

Zamieszczenie regulacji dotyczącej monitoringu w przepisach k.p. z jednoczesnym wskazaniem na wyraźnie ustalone cele, które ustawodawca uznaje za wynikające z prawnie uzasadnionych interesów, nie zwalnia pracodawcy z obowiązku przeprowadzenia tak zwanego testu równowagi. Test ten składa się z trzech części[4]. W ramach części pierwszej należy ustalić, czy istnieje cel, dla którego podstawą prawną przetwarzania danych może być prawnie uzasadniony interes. Częścią drugą testu powinna być ocena niezbędności przetwarzania danych dla realizacji tego celu. W części trzeciej należy ocenić, czy nie jest spełniona przesłanka o charakterze negatywnym w postaci występowania w danym stanie faktycznym interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej. W przypadku spełnienia tego warunku nie będzie można powołać się na przepis art. 6 ust. 1 lit. f RODO jako uzasadnienia dla przetwarzania danych osobowych. Należy wskazać, że zgodnie z zasadą rozliczalności fakt przeprowadzenia testu równowagi powinien być udokumentowany celem wykazania, że pracodawca przed wprowadzeniem określonej formy monitoringu dokonał weryfikacji, czy nie sprzeciwia się temu ochrona praw i wolności osób, które mają być w ten sposób kontrolowane. Co więcej: należy rozważyć, jakie środki powinny być wdrożone aby zapewnić ograniczenie ewentualnego ryzyka naruszenia praw i wolności podmiotów danych. Warto o tym przypominać, gdyż praktyka pokazuje, że wielu pracodawców trwa w mylnym przeświadczeniu, że skoro ustawodawca włączył

[4] Więcej na ten temat M. Więckowska, *Przetwarzanie danych na podstawie prawnie uzasadnionego interesu*, „ABI Expert" 2018, nr 3, s. 10–14.

© for this edition by CNS

przepisy o monitoringu do kodeksu pracy, to nie ma potrzeby dokonywać analizy zgodności tego procesu z przepisami RODO, a co za tym idzie, w ogóle nie przeprowadzają oceny skutków dla ochrony danych.

INNE FORMY MONITORINGU W PRZEPISACH K.P.

Na podstawie § 4 art. 22^3 k.p. przepisy dotyczące monitoringu służbowej poczty elektronicznej mają odpowiednie zastosowanie do innych form monitoringu, jeśli ich wdrożenie jest niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. W pozostałych przypadkach, w których prowadzony monitoring służy innym celom wynikającym z prawnie uzasadnionych interesów pracodawcy nietożsamych z celami wskazanymi w art. 22^3 k.p., przepis ten nie znajduje zastosowania. Tylko wówczas, gdy inne formy monitoringu są prowadzone w celach, o których mowa w § 1 art. 22^3 k.p., pracodawca jest zobowiązany zamieścić w układzie zbiorowym pracy, regulaminie lub obwieszczeniu informację o celu, zakresie oraz sposobie zastosowania monitoringu, jak również zastosować się do obowiązków informacyjnych poprzedzających wprowadzenie tej formy kontroli pracowników (przepisy art. 22^2 § 6–10 k.p. stosuje się odpowiednio). Podobnie jak w odniesieniu do monitoringu służbowej poczty elektronicznej inne formy monitoringu nie mogą naruszać dóbr osobistych pracowników (art. 22^3 §2 w związku z art. 22^3 § 4 k.p.).

OBOWIĄZKI INFORMACYJNE PRACODAWCY WZGLĘDEM PRACOWNIKÓW

Do obowiązków pracodawcy należy poinformowanie pracowników o wprowadzeniu monitoringu w sposób przyjęty u danego pracodawcy nie później niż dwa tygodnie przed jego uruchomieniem oraz przekazanie każdemu nowemu pracownikowi przed dopuszczeniem go do pracy informacji o celu, zakresie oraz sposobie zastosowania monitoringu. W mojej ocenie treść tej informacji powinna być zindywidualizowana, a nie stanowić jedynie powtórzenia zapisów zawartych w regulaminie pracy lub układzie zbiorowym. Powinna odnosić się w szczególności do tych form monitoringu, którym ten konkretny pracownik jest (lub będzie) poddawany. Uważam również, że informacja ta powinna być w miarę potrzeby aktualizowana. Pozostaje to w interesie obydwu stron. W sytuacji gdy pracodawca będzie chciał uczynić użytek z danych osobowych pozyskanych dzięki określonej formie monitoringu, o której pracownik nie został należycie poinformowany, może spotkać się z zarzutem naruszenia zarówno przepisów RODO, jak

© for this edition by CNS

i przepisów cywilnych o ochronie dóbr osobistych, w tym przypadku prawa do prywatności. Istnieje też cały szereg orzeczeń Europejskiego Trybunału Praw Człowieka, w których silnie akcentowane jest, że każda forma ingerencji w prywatność wymaga właściwego poinformowania o prowadzonych działaniach. Jedynie tytułem przykładu można wskazać, na kanwie wyroku ETPCz *Bărbulescu przeciwko Rumunii*[5] z 5 września 2017 roku, że pracownikowi należy wskazać różnicę między monitorowaniem przepływu informacji (to jest weryfikacją czy lub jak często korzysta ze skrzynki służbowej do celów prywatnych) a monitorowaniem treści korespondencji. Monitorowanie treści informacji jest oczywiście bardziej inwazyjne, dlatego też wymaga poważniejszego, bardziej pogłębionego uzasadnienia. Pracownikowi każdorazowo należy zapewnić odpowiednie gwarancje, zwłaszcza gdy czynności monitorowania będą miały charakter inwazyjny. Gwarancje te w szczególności powinny zapewniać, że pracodawca nie ma dostępu do treści komunikacji, chyba, że pracownik został z wyprzedzeniem poinformowany o takiej ewentualności.

OKRES RETENCJI DANYCH

Na zakończenie uwag ogólnych godzi się zaakcentować, że do innych form monitoringu, takich jak monitoring poczty elektronicznej, nie znajduje zastosowania trzymiesięczne ograniczenie przechowywania danych, które ustawodawca przewidział wyłącznie odnośnie nagrań z tak zwanego monitoringu wizyjnego, polegającego na nadzorze nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (art. 22^2 § 3 k.p.). Brak takiego ustawowego ograniczenia stanowi groźną pokusę dla pracodawców, aby zgromadzone w ramach innych form monitoringu dane osobowe przechowywać „na wszelki wypadek", gdyby na przykład wystąpiła potrzeba uzasadnienia rozwiązania umowy o pracę. Należy w tym miejscu raz jeszcze podkreślić, że zgodnie z zasadą ograniczenia przechowywania dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Jeżeli tym celem jest zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, wydaje się być oczywistym, że okres przechowywania danych nie może być nieograniczony. Wyrażam pogląd, że pracodawca może go ustanowić w dowolny sposób, na przykład odnosząc się do obowiązujących u niego okresów rozliczeniowych czy też okresów oceny pracowniczej. W sytuacji, gdy dane pozyskane z monitoringu staną się podstawą określonych czynności prawnych wobec pracownika oczywistym jest, że okres przechowywania tych da-

[5] Wyrok ETPCz z 05.09.2017 r., *Bărbulescu vs. Rumunia*, skarga nr 61496/08.

© for this edition by CNS

nych będzie podlegał automatycznemu wydłużeniu, przynajmniej do okresu przedawnienia roszczeń pracowniczych.

STOSOWANE W PRAKTYCE INNE FORMY MONITORINGU

Jak trafnie zauważono w opinii Grupy Roboczej art. 29 z dnia 8 czerwca 2017 roku, „przyjęcie nowych technologii informacyjnych w miejscu pracy pod względem infrastruktury, aplikacji i urządzeń inteligentnych pozwala na stosowanie nowych rodzajów systematycznego i potencjalnie inwazyjnego przetwarzania danych w miejscu pracy”[6]. Coraz bardziej zaawansowane technologicznie formy przetwarzania danych, w szczególności takie jak te odnoszące się do danych osobowych na temat korzystania z usług online lub danych dotyczących lokalizacji, są znacznie mniej widoczne dla pracowników niż inne tradycyjne formy przetwarzania, takie jak jawne monitorowanie kamerami CCTV. W takich przypadkach szczególnego znaczenia nabiera właściwe spełnienie obowiązku informacyjnego przez pracodawcę gdyż pracownicy mogą nie być świadomi tego, że są w ten sposób monitorowani, ani tym bardziej faktu, jaki zakres ich danych osobowych jest pozyskiwany dzięki tym metodom kontroli. Na długo przed pandemią koronawirusa Grupa Robocza dostrzegła, ze coraz bardziej zacierają się granice między domem a pracą. Gdy pracownicy pracują zdalnie (na przykład z domu) możliwe jest monitorowanie ich czynności poza fizycznym środowiskiem pracy[7]. Ten aspekt monitoringu będzie bez wątpienia stanowił dla pracodawców największe wyzwanie wobec ukończenia prac legislacyjnych oraz wprowadzenia pracy zdalnej do kodeksu pracy i zastąpienia nią istniejącej obecnie telepracy.

INNE FORMY MONITORINGU A PRACA ZDALNA

Z uwagi na upowszechnienie się w ostatnim czasie pracy zdalnej, nadzwyczaj aktualne stały się uwagi Grupy Roboczej dotyczące korzystania przez pracowników z ICT (*information and communication technologies*) poza miejscem pracy. Chodzi o technologie informacyjno-telekomunikacyjne gromadzące, przetwarzające i przesyłające informacje w formie elektronicznej. Możliwości oferowane przez te technologie mogą stwarzać realne ryzyko dla życia prywatnego pracowników, ponieważ w wielu przypadkach systemy monitorowania istniejące w miejscu pracy zostają w praktyce rozszerzone na sferę domową pracowników w przypadku, gdy korzystają oni z tego rodzaju urządzeń w domu[8]. Pracodawca udostępnia

[6] *Opinia 2/2017 Grupy Roboczej art. 29…*, s. 3
[7] *Ibidem*, s. 4–5.
[8] *Ibidem*, s. 18.

© for this edition by CNS

pracownikowi sprzęt ICT lub oprogramowanie, które — po jego zainstalowaniu w domu lub na należących do pracownika urządzeniach — pozwala mu uzyskać taki sam poziom dostępu do sieci, systemów i zasobów pracodawcy, jakim dysponowałby wówczas, gdyby znajdował się w miejscu pracy, w zależności od stopnia wdrożenia odpowiednich rozwiązań. Praca zdalna może zatem stwarzać dla pracodawcy szczególnego rodzaju ryzyko spowodowane tym, że pracownicy dysponujący dostępem do jego infrastruktury nie podlegają jednocześnie analogicznym środkom bezpieczeństwa jak te, które są stosowane w pomieszczeniach należących do pracodawcy.

Zagrożenia te zdaje się dostrzegać polski prawodawca, wskazując w nowelizacji kodeksu pracy[9] na konieczność określenia przez pracodawcę procedur ochrony danych osobowych na potrzeby wykonywania pracy zdalnej oraz przeprowadzenia, w miarę potrzeby, instruktażu i szkolenia w tym zakresie. W porozumieniu lub regulaminie dotyczącym pracy zdalnej mają zostać określone zarówno zasady kontroli wykonywania pracy przez pracownika wykonującego pracę zdalną, jak również zasady kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedury ochrony danych osobowych. Zgodnie z treścią wprowadzonej regulacji pracodawca będzie zobligowany dostosować sposób przeprowadzania kontroli do miejsca wykonywania pracy zdalnej i jej rodzaju. Wykonywanie czynności kontrolnych nie będzie mogło naruszać prywatności pracownika wykonującego pracę zdalną i innych osób ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem.

Pracodawcy mają obecnie do dyspozycji cały szereg rozwiązań technologicznych, w tym oprogramowania umożliwiające ciągłe rejestrowanie naciśnięć klawiszy lub ruchów myszy, przechwytywanie ekranu (w losowych albo regularnych odstępach czasu), rejestrowanie uruchamianych aplikacji oraz czasu korzystania z nich, a także włączanie kamer internetowych. Należy podkreślić, iż zadeklarowanie przez pracodawcę, że przetwarzanie danych osobowych za pomocą wybranego narzędzia jest mu niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy nie jest wystarczające dla stwierdzenia, iż odbywa się ono zgodnie z prawem. Pomijając wielokrotnie już wspominany obowiązek informacyjny, koniecznym będzie ograniczenie ryzyka związanego z pracą zdalną w sposób proporcjonalny. Jak wskazuje Grupa Robocza art. 29, prawdopodobieństwo, że uzasadniony interes pracodawcy będzie wystarczający

[9] Rządowy projekt ustawy o zmianie ustawy — Kodeks pracy oraz niektórych innych ustaw, druk sejmowy 2335. W dniu 16 stycznia 2023 r. ustawę uchwaloną w dniu 1 grudnia 2022 r., po odrzuceniu poprawek Senatu przekazano do podpisu Prezydenta — *Przebieg prac przed skierowaniem projektu do Sejmu*. *Rządowy projekt ustawy o zmianie ustawy — Kodeks pracy oraz niektórych innych ustaw*, Sejm Rzeczpospolitej Polskiej, 14.06.2022, https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=2335 (dostęp: 23.01.2023). Po jej opublikowaniu w Dzienniku Ustaw przepisy dotyczące pracy zdalnej wejdą w życie w terminie dwóch miesięcy.

© for this edition by CNS

do uzasadnienia stosowania metod takich jak permanentne rejestrowanie klawiszy naciskanych przez pracownika lub wykonywanych przez niego ruchów myszą jest bardzo niewielkie.

APLIKACJE BIUROWE

Pracowników, bez względu na to czy znajdują się w miejscu pracy czy też poza nim, można monitorować z uwagi na fakt, że korzystają oni z aplikacji internetowych udostępnionych im przez pracodawcę, które przetwarzają dane osobowe. Za Grupą Roboczą art. 29 można wskazać, tytułem przykładu, na aplikacje biurowe takie jak edytory dokumentów, kalendarze, wewnętrzne portale społecznościowe bazujące na technologii przetwarzania w chmurze. Gdyby pracodawca zdecydował się na zezwolenie pracownikom na wykorzystywanie tych narzędzi do celów prywatnych, niezbędnym będzie zapewnienie im możliwości wyznaczenia określonych przestrzeni prywatnych, do których pracodawca będzie mógł uzyskać dostęp wyłącznie w wyjątkowych okolicznościach. Ma to szczególne znaczenie w przypadku kalendarzy, które oprócz organizacji czasu pracy są często wykorzystywane również do planowania prywatnych spotkań. Jeżeli praktyka taka będzie uznawana przez pracodawcę za dopuszczalną, wówczas powinna być zapewniona funkcjonalność pozwalająca na określanie zakresu podmiotowego osób, które będą miały dostęp do prywatnych wpisów pracownika z poziomu użytkownika.

KOMUNIKACJA ELEKTRONICZNA

Monitorowanie treści szeroko rozumianej komunikacji elektronicznej pracowników (na przykład połączeń telefonicznych, przeglądanych zasobów internetowych, komunikatów natychmiastowych, połączeń za pośrednictwem telefonii internetowej itp.) uznawane jest za główne zagrożenie dla prywatności pracowników, a co za tym idzie — pracodawcy powinni podchodzić do niego ze szczególną ostrożnością, mając na uwadze rzeczywistą niezbędność prowadzonych działań do zmierzonych celów. W ocenie Grupy Roboczej w sytuacji, w której niedozwolone metody korzystania z usług łączności można zwalczać, blokując określone strony internetowe, powinno się tego dokonywać. Jeżeli w danym przypadku można zablokować strony internetowe zamiast wprowadzać ciągłe monitorowanie całej komunikacji, należy wybrać to rozwiązanie, aby zapewnić zgodność z wymogiem pomocniczości[10].

[10] *Opinia 2/2017 Grupy Roboczej art. 29…*, s. 17.

© for this edition by CNS

MONITORING GPS

Zgodnie z kodeksem pracy (art. 22^3 § 4) monitoring GPS pojazdów służbowych, jak każda inna forma monitoringu, może być prowadzony wówczas, gdy jest on niezbędny do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Narzędziem pracy będzie w tym przypadku samochód służbowy. We wszystkich sytuacjach, w których samochód służbowy nie stanowi narzędzia pracy pracownika, będąc tym samym jednym z benefitów (na przykład dla kadry menadżerskiej), a stosowany w tych samochodach monitoring GPS miałby na celu wyłącznie umożliwienie zlokalizowania pojazdów w dowolnym momencie (na przykład w przypadku zgłoszenia jego kradzieży), nie będziemy mieć do czynienia z monitoringiem, o którym mowa w art. § 4 art. 22^3 k.p. Pracodawca korzystający z rozwiązań GPS instalowanych w pojazdach będzie mógł gromadzić nie tylko dane o pojeździe, lecz także o konkretnym pracowniku, który korzysta z pojazdu służbowego. Dane takie mogą obejmować nie tylko informacje o lokalizacji pojazdu (a tym samym o położeniu pracownika) zgromadzone przez podstawowe systemy śledzenia GPS, ale — w zależności od zastosowanej technologii — również wiele innych informacji, w tym informacje o stylu jazdy.

KORZYSTANIE Z SAMOCHODU SŁUŻBOWEGO DO CELÓW PRYWATNYCH A MONITORING GPS

W przypadkach, gdy pracodawca dopuszcza możliwość korzystania z pojazdu służbowego do celów prywatnych, Grupa Robocza art. 29 rekomenduje, aby pracownikowi zostało umożliwione skorzystanie z opcji tymczasowego wyłączenia mechanizmu śledzenia położenia pojazdu, na przykład w przypadku gdy będzie to uzasadnione szczególnymi okolicznościami mogącymi wystąpić w godzinach pracy, jak chociażby wizyta lekarska. W ten sposób pracownik może z własnej inicjatywy chronić określone dane dotyczące lokalizacji, traktując je jako dane prywatne. Wydaje się jednak, że rekomendowane przez Grupę Roboczą art. 29 rozwiązanie będzie w praktyce technicznie niemożliwe lub znacznie utrudnione. Co więcej, mogłoby ono prowadzić do sytuacji, w której pracownik, po zakończeniu czynności należącej do sfery prywatnej (której podjęcie w godzinach pracy jest konieczne), zapomniałby ponownie włączyć urządzenia, przez co właściwy cel takiego monitoringu byłby niemożliwy do zrealizowania. Nie ulega jednak wątpliwości, że decydując się na tę formę monitoringu, pracodawcy powinni wziąć pod uwagę przede wszystkim to, czy pracownik pracuje w podstawowym czy zadaniowym systemie czasu pracy. Może to bowiem mieć istotne znaczenie dla

© for this edition by CNS

zorganizowania procesów monitoringu GPS służbowego samochodu pracownika z uwzględnieniem sytuacji wyjątkowych, o których była mowa powyżej.

W niektórych przypadkach pracownicy mogą również korzystać z samochodów służbowych poza godzinami pracy w celach prywatnych, w zależności od treści polityki regulującej sposób korzystania z tych pojazdów czy też indywidualnych uzgodnień pomiędzy pracownikiem a pracodawcą. W ocenie Grupy Roboczej art. 29 jest mało prawdopodobne, aby zaistniała podstawa prawna monitorowania lokalizacji pojazdów pracowników poza uzgodnionymi godzinami pracy. Jednak w przypadku wystąpienia takiej konieczności należy rozważyć możliwość wdrożenia środków, które byłyby proporcjonalne do istniejącego ryzyka. W celu zapobieżenia kradzieży samochodu może to oznaczać na przykład odstąpienie od rejestrowania położenia samochodu poza godzinami pracy, o ile nie opuści on szeroko wyznaczonego obszaru (danego regionu lub wręcz państwa). Ponadto informacje o położeniu byłyby w takim przypadku ujawniane wyłącznie na zasadzie „zbitej szyby" — pracodawca mógłby aktywować „widoczność" danej lokalizacji i uzyskać wgląd w dane, które zostały już zgromadzone przez system, po opuszczeniu określonego obszaru przez pojazd. Pracodawca musi również wyraźnie poinformować pracowników o fakcie zainstalowania urządzenia śledzącego w samochodzie służbowym oraz o tym, że urządzenie to rejestruje wszystkie ruchy wykonywane przez nich w trakcie korzystania z pojazdu (a także o tym, że — w zależności od zastosowanej technologii — ich styl jazdy również może być monitorowany). Informacje takie powinny być umieszczone w widocznym miejscu w każdym samochodzie, w zasięgu wzroku kierowcy[11].

REJESTRATORY DANYCH NA TEMAT ZDARZEŃ

Rejestratory danych na temat zdarzeń zapewniają pracodawcy techniczną możliwość przetwarzania znacznych ilości danych osobowych pracowników, którzy prowadzą pojazdy firmowe. Urządzenia takie są coraz częściej instalowane w pojazdach w celu rejestrowania obrazu, a potencjalnie również dźwięku. Z reguły jednak takie systemy zapewniają możliwość zapisywania danych tylko w przypadku, gdy ocenią, że miało miejsce zdarzenie oceniane przez system za krytyczne (takie jak gwałtowny manewr kierowcy, nieoczekiwane hamowanie, a w każdym razie — wypadek), a w przeciwnym razie dane są nadpisywane. Można jednak wybrać również opcję stałego rejestrowania danych. Zgromadzone w ten sposób informacje mogą zostać później wykorzystane do obserwowania i analizowania stylu jazdy danej osoby w celu jego udoskonalenia. Ponadto wiele tych systemów wykorzystuje GPS do śledzenia lokalizacji pojazdu w czasie rzeczywistym; systemy te zapewniają również możliwość przechowywania innych szczegóło-

[11] *Ibidem*, s. 23.

© for this edition by CNS

wych informacji związanych z jazdą (takich jak informacje o prędkości pojazdu) w celu ich dalszego przetwarzania. Tego rodzaju urządzenia są powszechnie stosowane, w szczególności przez organizacje prowadzące działalność w sektorze transportu lub zarządzające dużymi flotami pojazdów. Co do zasady, stosowanie rejestratorów danych na temat zdarzeń można będzie uznać za zgodne z prawem wyłącznie w przypadku konieczności przetwarzania danych osobowych pracownika gromadzonych przez te rejestratory w prawnie uzasadnionym celu i w przypadku zgodności przetwarzania z zasadami proporcjonalności i pomocniczości.

Bez wątpienia dla dokonania takiej oceny będzie miało znaczenie, czy zastosowanie rejestratora zdarzeń będzie służyło działaniom prewencyjnym pracodawcy w celu zapewnienia większego bezpieczeństwa pasażerów (co ma szczególne znaczenie w przypadku podmiotów świadczących usługi transportowe) czy działaniom mającym na celu wykrycie pracowników, którzy przekraczają dozwoloną prędkość podczas prowadzenia pojazdów służbowych, przez co stwarzają większe ryzyko ponoszenia przez pracodawcę kosztów związanych z mandatami drogowymi, w celu ich zdyscyplinowania. Nie da się zaprzeczyć, że niezależnie od tego, jaki cel przyświeca pracodawcy, skutek w postaci podniesienia poziomu bezpieczeństwa i tak wystąpi. Niemniej jednak cel w postaci zapewnienia bezpieczeństwa — czy to pracowników, czy innych uczestników ruchu drogowego — powinien być nadrzędny nad celem ekonomicznym pracodawcy w postaci uniknięcia ponoszenia kosztów wynikających z użytkowania pojazdów niezgodnie z przepisami prawa o ruchu drogowym. Gdyby się zatem okazało, że pracodawca deklarując, iż celem monitoringu GPS jest kontrola właściwego użytkowania narzędzia pracy w postaci samochodu, przez co rozumiane jest stosowanie się do reguł ruchu drogowego, a w rzeczywistości dane z monitoringu służą wyłącznie monitorowaniu częstotliwości kończących się mandatami naruszeń, będziemy mieć do czynienia z przetwarzaniem niezgodnym z celem.

Prowadzenie monitoringu GPS z uwzględnieniem rejestratora zdarzeń w nadrzędnym celu, jakim jest bezpieczeństwo może być również niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Ważne jest jednak, aby komunikacja kierowana do pracowników była pełna, a przekaz zrozumiały.

ZDALNE MONITOROWANIE STANU ZDROWIA PRACOWNIKÓW

Producenci technologii już od dłuższego czasu oferują rozwiązania pozwalające na monitorowanie stanu zdrowia. Obecnie coraz większym zainteresowaniem cieszą się one również wśród pracodawców upatrujących w nich sposobu na zwiększenie bezpieczeństwa pracowników. Monitoring wizyjny nie zawsze jest wystarczającym narzędziem, gdyż nie obejmuje on wszystkich miejsc na te-

© for this edition by CNS

renie zakładu, a przede wszystkim wymaga permanentnej obserwacji w czasie rzeczywistym. Nagrania z monitoringu są wykorzystywane przede wszystkim do analizy zdarzeń wypadkowych już po fakcie, w celu zbadania ich przyczyn i ograniczenia zagrożenia w przyszłości.

Proponowane pracodawcom urządzenia do noszenia na ciele pracowników (w postaci zegarka, breloczka czy opaski na nadgarstek) samodzielnie monitorują ich stan i aktywność, a w razie zagrożenia przesyłają sygnał na przykład do centrali ratownictwa medycznego pracodawcy. Urządzenia te, dzięki wbudowanemu lokalizatorowi, pozwalają też szybko dotrzeć do pracownika w celu udzielenia mu pomocy medycznej. Z korzystaniem z tej formy ochrony życia i zdrowia pracowników łączy się jednak poważne ryzyko pozyskania przez pracodawcę nadmiarowej liczby danych osobowych dotyczących zdrowia pracowników, a zatem danych szczególnej kategorii. Co więcej, literalne brzmienie art. 22^3 k.p. wskazywałoby na niemożność stosowania innych form monitoringu w celach innych niż wymienione w tym przepisie, wśród których nie znajdziemy bezpieczeństwa pracowników. Jak już jednak zostało wskazane w uwagach wstępnych, uregulowanie monitoringu w kodeksie pracy nie jest równoznaczne z zakazem prowadzenia go w celach innych niż wymienione w k.p., o ile spełniona będzie którakolwiek z przesłanek legalizujących przetwarzanie danych osobowych. W przypadku danych dotyczących zdrowia, katalog przesłanek uchylających zakaz przetwarzania tych danych zawarty jest w art. 9 RODO. Zgodnie z art. 9 ust. 2 lit. b RODO zakaz przetwarzania danych szczególnej kategorii nie znajduje zastosowania wówczas, gdy przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą. Dyskusyjne jest, czy dozwolone przepisami powinno być przetwarzanie danych, czy też wystarczy, aby dozwolone przepisami było wypełnianie obowiązków i wykonywanie uprawnień, do realizacji których niezbędne jest przetwarzanie danych. Opowiadam się za drugą ze wskazanych powyżej wykładni, ponieważ przyjęcie pierwszej oznaczałoby zakwestionowanie przetwarzania danych w ramach całego szeregu regulacji przewidzianych w przepisach prawa pracy, które nie referują wprost do danych osobowych, a tym samym nie przewidują w swej treści odpowiednich zabezpieczeń praw podstawowych i interesów osoby, której dane dotyczą. Dla przykładu można wskazać na przetwarzanie przez pracodawcę danych dotyczących chorób zawodowych pracownika, przetwarzanie danych o zdrowiu członków rodziny pracownika na potrzeby przyznania świadczeń socjalnych, przetwarzanie danych osobowych o przynależności związkowej w celu dokonania potrącenia składki członkowskiej, czy też udzielenia zwolnienia od pra-

© for this edition by CNS

cy zawodowej na czas pełnienia funkcji w zarządzie organizacji związkowej czy też wykonania czynności doraźnej.

Ochrona życia i zdrowia pracowników stanowi jeden z podstawowych obowiązków pracodawcy. Zgodnie z art. 207 k.p. § 2 pracodawca jest zobowiązany chronić zdrowie i życie pracowników przez zapewnienie bezpiecznych i higienicznych warunków pracy przy odpowiednim wykorzystaniu osiągnięć nauki i techniki. W szczególności pracodawca jest obowiązany reagować na potrzeby w zakresie zapewnienia bezpieczeństwa i higieny pracy oraz dostosowywać środki podejmowane w celu doskonalenia istniejącego poziomu ochrony zdrowia i życia pracowników, biorąc pod uwagę zmieniające się warunki wykonywania pracy.

Zdarzają się takie sytuacje, w których — z uwagi na szczególne ryzyko związane z funkcjonowaniem zakładu pracy czy też odosobnieniem miejsca pracy — w razie wypadku nie zawsze na miejscu jest osoba, która będzie w stanie udzielić pomocy pracownikowi. W mojej ocenie stosowanie urządzeń monitorujących stan zdrowia pracowników czy też pozwalających na zlokalizowanie ich w okresie bezruchu uprawdopodobniających zasłabnięcie będzie wówczas uzasadnione, z tym jednak zastrzeżeniem, że dostęp pracodawcy do danych o stanie zdrowa powinien być ściśle ograniczony do tego celu. Jak wiadomo, w zależności od zaawansowania technologicznego, tego rodzaju urządzenia niejednokrotnie posiadają wiele funkcjonalności. Zliczają liczbę kroków wykonywanych przez pracowników, rejestrują tętno, monitorują ich nawyki senne. Gromadzone przez te urządzenia dodatkowe dane dotyczące zdrowia powinny być jednak dostępne wyłącznie dla pracowników. Co więcej, dane dotyczące zdrowia pracowników mogą być również przetwarzane przez podmiot, który wyprodukował dane urządzenie lub który oferuje określoną aplikację do zainstalowania na smartfonie, zatem przy dokonywaniu wyboru urządzenia lub usługi pracodawca powinien ocenić politykę ochrony prywatności danego producenta lub usługodawcy, aby upewnić się, że nie doprowadzi ona do niezgodnego z prawem przetwarzania danych dotyczących zdrowia pracowników.

INNE FORMY MONITORINGU A PROFILOWANIE I ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI

Zgodnie z definicją zamieszczoną w art. 4 pkt 4 RODO „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

© for this edition by CNS

Aby przetwarzanie danych osobowych mogło zostać uznane za profilowanie, niezbędnym jest łączne wystąpienie następujących trzech elementów:

— profilowanie musi stanowić zautomatyzowaną formę przetwarzania;

— profilowaniu muszą podlegać dane osobowe; oraz

— celem profilowania musi być ocena czynników osobowych osób fizycznych.

Zgodnie z wytycznymi Grupy Roboczej art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE (WP 251)[12] profilowanie oznacza gromadzenie informacji o danej osobie (lub grupie osób fizycznych) i ocenę ich cech lub wzorców zachowania w celu zakwalifikowania ich do określonej kategorii lub grupy, w szczególności do celów analizy lub prognozy takich aspektów, jak wykazywane przez dane osoby zdolności do wykonania danego zadania, zainteresowania lub ustalania prawdopodobnych zachowań. Istotą profilowania jest tworzenie profilu osoby na podstawie różnorodnych informacji, które jej dotyczą. Sporządzenie profilu osobowego pozwala na dokonywanie ocen, analiz i prognoz odnoszących się do tej osoby[13].

W przypadku innych form monitoringu mamy co do zasady do czynienia z zautomatyzowaną formą przetwarzania danych osobowych. Jak jednak wynika z powyższego, aby w jego ramach dochodziło do profilowania, pracodawca musiałby oceniać czynniki osobowe osób fizycznych. Z profilowaniem możemy mieć na przykład do czynienia wówczas, gdy analiza GPS pojazdu prowadzonego przez pracownika pozwala na określenie jego stylu jazdy, szybkości relacji na bodźce zewnętrzne czy też, w przypadku pozyskiwania danych o jakości snu pracownika, poziomie zmęczenia w poszczególnych dniach i godzinach, co umożliwiają urządzenia do monitowania stanu zdrowia pracowników.

Zgodnie z art. 22 ust. 1 RODO osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Samo zastosowanie zautomatyzowanego przetwarzania danych osobowych nie podlega żadnym dodatkowym ograniczeniom. Konieczność stosowania art. 22 RODO pojawia się dopiero wówczas, gdy w wyniku zautomatyzowanego przetwarzania danych — bez jakiegokolwiek udziału czynnika ludzkiego — miałyby zostać podjęte decyzje wywołujące wobec podmiotu danych określone skutki prawne lub w podobny sposób istotnie na nią wpływające. Zgodnie z wytycznymi Grupy Roboczej art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE (WP 251), jeżeli ostateczna de-

[12] *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, WP 251*, Urząd Ochrony Danych Osobowych, 5.12.2020, https://www.uodo.gov.pl/data/filemanager_pl/908.pdf (dostęp: 24.10.2022).

[13] P. Fajgielski, *Komentarz do art. 4 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 117.

© for this edition by CNS

cyzja zostaje podjęta przez człowieka po przeprowadzeniu oceny i uwzględnieniu innych czynników, taka decyzja nie opiera się wyłącznie na zautomatyzowanym przetwarzaniu:

> Aby można było uznać, że ma miejsce udział człowieka, administrator musi zapewnić, że jakikolwiek nadzór nad decyzją jest znaczący, a nie stanowi tylko symbolicznego gestu. Powinno być to prowadzone przez kogoś, kto ma władzę i kompetencje do zmiany decyzji. W ramach analizy należy wziąć pod uwagę wszystkie istotne dane[14].

Powyższe uwagi na temat profilowania i zautomatyzowanego podejmowania decyzji nie są czysto teoretyczne. Artykuł 13 ust. 2 lit. f oraz art. 14 ust. 2 lit. g RODO nakładają bowiem na administratora (a więc pracodawcę) szczególne obowiązki informacyjne w tym zakresie. Nakazują one podanie osobie, której dane dotyczą, istotnych informacji o zasadach podejmowania takich decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Zautomatyzowane podejmowanie decyzji, w tym profilowanie, jest także objęte prawem dostępu przysługującego osobie, której dane dotyczą (art. 15 ust. 1 lit. h). Szczególny nacisk na profilowanie został położony w art. 21 RODO, który reguluje prawo do sprzeciwu.

Co więcej art. 35 ust. 3 lit. a RODO wprowadza obowiązkową ocenę skutków dla ochrony danych w przypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, gdy opiera się ona na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną. Konieczność dokonania oceny skutków dla ochrony danych osobowych zachodzi w przypadku jakichkolwiek decyzji, przy podejmowaniu których wykorzystywano profilowanie.

Dla jasności należy wskazać, że w przypadku innych form monitoringu zawsze będziemy mieć do czynienia z zautomatyzowanym przetwarzaniem danych a niekiedy może mieć też miejsce profilowanie. Wówczas, gdy na podstawie informacji pozyskiwanych za pomocą monitoringu pracodawcy będą tworzyć profile pracowników biorąc pod uwagę określone cechy osobiste (na przykład akceptacja ryzyka, szybkość reagowania na różnego rodzaju bodźce zewnętrzne, zdolność koncentracji w poszczególnych sekwencjach czasowych w dobie pracowniczej, umiejętność adaptacji do nowych sytuacji itp.) będziemy mieli do czynienia z profilowaniem, czy wreszcie z podejmowaniem decyzji w wyniku zautomatyzowanego przetwarzania danych bez udziału czynnika ludzkiego (na przykład o ograniczeniu pracownikowi prawa do korzystania z samochodu służbowego dla celów prywatnych z uwagi na określony profil kierowcy stwarzający większe ryzyko wypadku, czy też wyłączenie możliwości pracy nocnej pracowników, którzy nie posiadają zdolności adaptacji do zmiany pory snu i pracy, co wpływa na ich szybkość reakcji).

[14] *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji…*, s. 20–21.

© for this edition by CNS

PODSUMOWANIE

Prowadzenie monitoringu pracowników za pomocą narzędzi opartych na nowoczesnych technologiach i usługach łączności elektronicznej może z jednej strony przynieść pozytywny skutek dla efektywności czynności kontrolnych pracodawcy, a z drugiej — niesie za sobą poważne ryzyka w zakresie prywatności i innych dóbr osobistych pracowników. Poczucie permanentnej inwigilacji zdecydowanie zmniejsza poczucie komfortu pracy i zaufanie pracowników do pracodawcy. Z całego szeregu dostępnych na rynku narzędzi należy zatem wybierać te, które są niezbędne do osiągnięcia celu. Zgodnie z art. 25 RODO pracodawca ma obowiązek uwzględniać ochronę danych już w fazie projektowania (*privacy by design*) oraz w drodze realizacji zasady domyślnej ochrony danych (*privacy by default*), a decyzję o ich wprowadzeniu powinna poprzedzać analiza oceny skutków dla ochrony danych. Zasada *privacy by design* wymaga w szczególności, aby już w fazie projektowania administrator brał pod uwagę zagrożenia dla prywatności i je eliminował. Zagadnienia dotyczące prywatności powinny być uwzględniane w całym cyklu technologicznym, z naciskiem na fazę projektowania określonej technologii, a następnie na etapie jej wdrażania, korzystania z niej oraz usuwania danych. Stosowanie się do powyższego wymaga przemyślanych decyzji o wprowadzeniu określonych rozwiązań technologicznych pozwalających na monitorowanie pracowników, dokładnej analizy funkcjonalności oferowanych przez rynek narzędzi, a także przejrzystej i wyczerpującej komunikacji z pracownikami.

PROCESSING OF EMPLOYEES' PERSONAL DATA IN THE FRAMEWORK OF SO-CALLED OTHER FORMS OF MONITORING

Summary

The widespread availability of new technologies allows employers to use types of employee activity monitoring that were previously non-existent in the work environment. Moreover, the popularization of remote work, in conjunction with the appearance of a new regulation in the Labor Code, naturally increases the employers' interest in the processing of data on employee online activity as well as location data. Technologies used in the context of other forms of monitoring, on the one hand, can be very effective in detecting violations of employee duties, protecting confidential information, in increasing the efficiency of work, but on the other hand, they pose serious risks to the protection of privacy and personal data. This is because digital data analysis applications can operate unnoticed by device users, thus posing greater threats to their privacy than, for example, CCTV cameras. Therefore, a re-examination of the data protection impact assessment and a careful analysis of the measures taken, taking into account the principles under both the Labor Code and the RODO, is warranted. Employers' use of data obtained in a non-compliant manner could face serious legal consequences.

Keywords: monitoring, remote working, GPS, employee control, other forms of monitoring

© for this edition by CNS

BIBLIOGRAFIA

Fajgielski P., *Komentarz do art. 4 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Opinia 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy, WP 249, Archiwum GIODO, 21.02.2018, https://archiwum.giodo.gov.pl/pl/file/13179.

Więckowska M., *Przetwarzanie danych na podstawie prawnie uzasadnionego interesu*, „ABI Expert" 2018, nr 3.

Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, WP 251, Urząd Ochrony Danych Osobowych, 5.12.2020, https://uodo.gov.pl/pl/10/10.

© for this edition by CNS