

MONITORING POCZTY ELEKTRONICZNEJ I INNE FORMY MONITORINGU

r.pr. Grzegorz Gołębiewski

16 kwietnia 2019

SPOSOBY MONITOROWANIA

- monitoring wizyjny – kamery przemysłowe
- dostęp do pomieszczeń / przemieszczanie się w zakładzie pracy – karty dostępu (RFID), dane biometryczne
- geolokalizacja – pracownicy (SIM) / pojazdy (GPS)
- poczta elektroniczna
- połączenia telefoniczne – billingi – „tajemniczy klient”
- aktywność w sieci / korzystanie z narzędzi informatycznych /korzystanie ze sprzętu

ART. 88 RODO

- 1. 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.
- 2. 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.

MONITORING – PODSTAWY PRAWNE

- nowe regulacje rangi ustawowej **VS.** dotychczasowa praktyka pracodawców – korzyści i wyzwania
- zmiany w Kodeksie pracy
 - ✓ ustawa z 10 maja 2018 o ochronie danych osobowych
 - ✓ ustawa z 21 lutego 2019 o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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
- dotychczasowe przepisy – np. kontrola trzeźwości pracownika

WARUNKI FORMALNE PROWADZENIA MONITORINGU

- regulamin pracy / ZUZP albo obwieszczenie – obowiązek określenia:
 - ✓ celów
 - ✓ zakresu
 - ✓ sposobów monitorowania
- obowiązek uprzedzenia pracowników (2 tyg.)
- obowiązek informacyjny względem nowych pracowników (przed podjęciem pracy)
- odpowiednie oznaczenie terenu objętego monitoringiem wizyjnym (1 dzień) – podobnie poczta elektroniczna, monitorowany samochód etc.
- obowiązki z art. 12 i 13 RODO

SPOSÓB PROWADZENIA MONITORINGU

- **Monitoring poczty elektronicznej**
 - ✓ nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika

OCHRONA PRYWATNOŚCI

Art. 47 konstytucji RP (także: art. 7 Karty Praw Podstawowych UE, art. 8 Europejskiej Karty Praw Człowieka)

Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Art. 49 Konstytucji RP

Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

Art. 23 KC

Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, **wizerunek, tajemnica korespondencji**, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

SPOSÓB PROWADZENIA MONITORINGU - PRZETWARZANIE DANYCH OSOBOWYCH

- **art. 5 RODO**
 - ✓ przetwarzanie zgodnie z prawem, rzetelnie i przejrzystość
 - ✓ ograniczenie celu
 - ✓ adekwatność przetwarzania / minimalizowanie danych
 - ✓ prawidłowość danych
 - ✓ ograniczenie przechowywania
 - ✓ bezpieczeństwo danych / integralność i poufność
 - ✓ rozliczalność – umiejętność wykazania przestrzegania zasad przetwarzania
- **art. 35 RODO**
 - ✓ ocena skutków dla ochrony danych? – systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie
 - ✓ PUODO – wykaz rodzajów operacji wymagających oceny skutków przetwarzania – nie podlegają obligatoryjnie systemy monitoringu wizyjnego, w których obraz jest nagrywany wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa

RODZAJE MONITORINGU

- monitoring bieżący / prewencyjny **VS.** monitoring incydentalny / proaktywny (działanie sprawdzające)
- Czy można prowadzić działania kontrolne w razie niewprowadzenia w zakładzie określonej formy monitoringu?
- Charakter (cel) podjęcia monitoringu a jego uzasadniony zakres

CELE MONITORINGU

- monitoring wizyjny :
 - ✓ zapewnienie bezpieczeństwa pracowników **LUB**
 - ✓ ochrona mienia (niekoniecznie mienia pracodawcy – również klienci, pracownicy etc.) **LUB**
 - ✓ kontrola produkcji **LUB**
 - ✓ zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę
- monitoring poczty elektronicznej (i inne formy, jeśli ich zastosowanie jest konieczne do realizacji poniższych celów):
 - ✓ zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy **ORAZ (!)**
 - ✓ zapewnienie właściwego użytkowania udostępnionych pracownikowi narzędzi pracy
 - ✓ **brak przesłanki zachowania informacji w tajemnicy!**

NAJNOWSZE ZMIANY

- przetwarzanie szczególnych kategorii DO:
 - ✓ przetwarzanie szczególnych kategorii DO (w tym danych biometrycznych) za zgodą – wyłącznie w przypadku, gdy przekazanie tych danych następuje z inicjatywy kandydata lub pracownika (brak zgody lub jej wycofanie nie może powodować niekorzystnego traktowania bądź jakichkolwiek negatywnych konsekwencji)
 - ✓ przetwarzanie danych biometrycznych – dopuszczalne również gdy podanie tych 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
 - ✓ konieczne szczególne pisemne upoważnienie do przetwarzania ww. DO plus obowiązek zachowania w tajemnicy

ODPOWIEDZIALNOŚĆ

- cywilna

- karna

Art. 267 KK

- ✓ kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie,
- ✓ kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
- ✓ kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

- administracyjna