Warszawa, dn. 30.09.2025 r.

Permanentna inwigilacja, czyli czy twój pracownik wie jak bardzo go monitorujesz?

Twój Kluczowy Pracownik udał się na zasłużony, dwutygodniowy urlop w Bieszczady (lub inne miejsce, gdzie nie ma telefonów, WiFi, czy nawet gołębi pocztowych). I w połowie wyjazdu wybucha coś w firmie. Możliwe straty: dziesiątki, jak nie setki tysięcy złotych. Coś, można ugasić tylko dokumentem, którego jedyna kopia jest na skrzynce e-mail Twojego Kluczowego Pracownika. Co robić?
To proste: dział IT resetuje hasło do skrzynki e-mail i w 10 minut znajdujemy potrzebną wiadomość, pożar ugaszony. Ale, czy na pewno? Czy właśnie nie naruszyliśmy zasad ochrony danych osobowych? Czy Dział HR powiadomił człowieka, że coś takiego może się zdarzyć? Czy dopełniliśmy wymogów monitoringu z art. 22(3) Kodeksu Pracy?

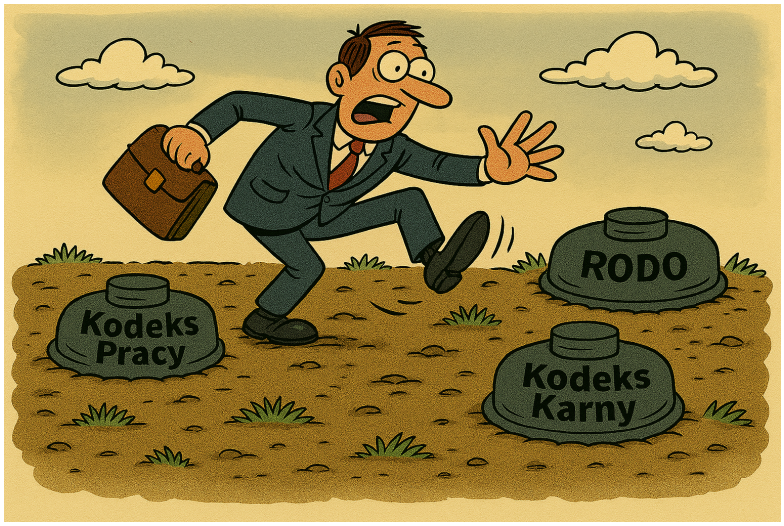
Po co zaglądać w skrzynkę e-mail pracownika?

Dostęp do materiałów na zasobach używanych przez czasowo niedostępnego pracownika to tylko jeden z przykładów sytuacji, w której pracodawca może mieć uzasadnioną, legalną potrzebę dostępu do jego służbowej skrzynki e-mail. Inne przykłady to:

- weryfikacja pełnego wykorzystania czasu pracy,
- weryfikacja właściwego użytkowania narzędzi pracy,
- działanie różnego rodzaju zabezpieczeń technicznych, filtrów antyspamowych, systemów Deata Leakage Prevention (DLP), itp.,
- uzasadnione podejrzenie poważnego naruszenia obowiązków pracowniczych,
- archiwizacja skrzynki po zakończeniu współpracy.

O czym pamiętać?

Jeżeli mielibyście Państwo zapamiętać jedną rzecz z tej publikacji to to, że wgląd pracodawcy do poczty elektronicznej pracownika można porównać do przejścia pola minowego. Da się to zrobić bezpiecznie – ale trzeba działać ostrożne, z odpowiednim przygotowaniem. Zaś w przypadku błędów skutki mogą być bolesne.



A konkretnie: Kodeks Pracy mówi, że wgląd pracodawcy w służbową pocztę elektroniczną należy traktować tak samo, jak stosowanie monitoringu wizyjnego. W RODO też można znaleźć trochę uwag na ten temat. Oznacza to, że monitorowanie poczty pracownika dopuszczalne tylko wtedy, jeżeli:

- nie dojdzie do naruszenia tajemnicy korespondencji oraz innych dóbr osobisty pracownika[1],
- zasady kontroli zostały udokumentowane w układzie zbiorowym pracy, w regulaminie pracy albo w obwieszczeniu[2],
- zasady kontroli zostały udostępnione pracownikom minimum 14 dni przed jej uruchomieniem / przed dopuszczeniem nowej osoby do pracy (to tylko jeden z elementów budowania RODO świadomości w organizacji),
- dopilnowano stosowania i udokumentowania zasady privacy by design i privacy by default,
- pracownicy zostali poinformowani o takim sposobie przetwarzania danych zgodnie z art. 13 RODO (czyli stosowny zapis musi być w „klauzuli informacyjnej" RODO).

„Spiesz się powoli". Absolutnie nie twierdzimy, żeby rezygnować z takich rozwiązań, a dostęp do skrzynki e-mail pracownika może mieć ogromne znaczenie biznesowe dla Spółki. Można to zrobić legalnie – o czym szerzej pisał na naszym blogu Maciej Łukaszewicz. Ale pójście na skróty może przynieść więcej szkody niż pożytku.

Niejawne stosowanie takiego (lub jakiegokolwiek innego) monitoringu teoretycznie jawi się również jako prawnie dopuszczalne. Ale to materiał na osobną publikację – na gruncie wyroku Europejskiego Trybunału Praw Człowieka w sprawie López Ribalda i inni przeciwko Hiszpanii z 2013 roku.

[1] Wbrew pozorom to nie jest aż tak trudne do wykonania w praktyce. W zdecydowanej większości przypadków po samym polu „nadawca" i temacie wiadomości e-mail można relatywnie łatwo odróżnić korespondencję służbową od prywatnej. Jeżeli zatem maila z kontraktem z firmą X to spokojnie możemy ominąć ewentualne maile typu „wyniki badań krwi" czy „kochanie pamiętaj kupić mleko wracając z pracy".

[2] Jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.

Podsumowując

Autor niniejszego tekstu ma pełną świadomość, że nawet w braku odpowiedniej dokumentacji ochrony danych osobowych większość pracowników w takiej sytuacji nie robiłaby pracodawcy problemu o taką sytuację. No chyba, że potem ten pracownik odchodziłby z firmy z jakimiś pretensjami, w nieprzyjemnej atmosferze. Zdarzyła się Wam kiedyś taka sytuacja? W sensie, żeby ktoś rzucił papierami, odszedł w atmosferze konfliktu? Bo np. my w iSecure tylko w pierwszej połowie września 2025 r. ogarnialiśmy dla klienta dopiero jedną sytuację „niezadowolony z czegoś pracownik napisał skargę na RODO". Patrząc, ile godzin wszystkim może pochłonąć jedna taka skarga (pomijam już całkowicie potencjalne straty jak skarga „chwyci" w UODO albo Inspekcji Pracy) to zwyczajnie taniej może wyjść poukładać wszystko jak trzeba zawczasu.

P.S.

Jeżeli czytając przykład ze wstępu zastanowiliście się Państwo nad pytaniem „ojej, a co ja bym zrobił/a gdyby Mój Kluczowy Pracownik miał te materiały tylko na prywatnym mailu" – to oto macie kolejny argument za tym, by pracownikom nie pozwalać na wykorzystywanie prywatnych wiadomości e-mail w celach służbowych.
Grafika wygenerowana przez Microsoft Copilot (GPT-4), na podstawie opisu autora publikacji.

Już **18 listopada br.** planujemy zorganizować **bezpłatny webinar** pt. „**Czy HR potrzebuje IOD-a bardziej niż myśli? Praktyczne przykłady wsparcia**". Jeśli chcesz zagwarantować sobie udział w tym wydarzeniu, zarejestruj się już dzisiaj: https://www.isecure.pl/webinar/czy-hr-potrzebuje-iod-a-bardziej-niz-mysli-praktyczne-przyklady-wsparcia/

Daniel Taberski - radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.