



Dziś drugi artykuł z cyklu „Jesień z compliance”, w którym omówione zostaną kwestie związane z przetwarzaniem danych osobowych pracowników. Opisujemy cztery problematyczne przypadki, w których pracodawca musi rozstrzygnąć, czy jego działania będą dotyczyć sfery prywatności pracowników oraz czy przy ich realizacji nie narusza ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.; dalej: u.o.d.o.).

# Dane osobowe pracowników повинien chronić pracodawca



**Edyta Jagiełło**  
radca prawny,  
prawnik w kancelarii Raczkowski Paruch



**Robert Stępień**  
aplikant radcowski,  
prawnik w kancelarii Raczkowski Paruch

**S**prawdzenie przez pracodawcę ewentualnej karalności przyszłego pracownika co do zasady jest zabronione. Zgodnie z art. 6 ust. 1 pkt 10 ustawy z 24 maja 2000 r. o Krajowym Rejestrze Karnym (t.j. Dz.U. z 2015 r. poz. 1036) pracodawca może uzyskać informacje zgromadzone w rejestrze karnym w zakresie niezbędnym dla zatrudnienia pracownika, jeżeli z przepisów ustawy wynika wymóg niekaralności lub korzystania z pełni praw publicznych przez osobę zajmującą konkretne stanowisko pracy. W aktualnym stanie prawnym niewiele jest takich regulacji. Tymczasem takie informacje o pracowniku mają istotne znaczenie w związku z podjęciem decyzji np. o dopuszczeniu do pracy z dziećmi bądź pracy na stanowisku, z którym wiąże się odpowiedzialność materialna za mienie (tak też jest w przypadku magazyniera). Dlatego często pracodawcy wymagają od potencjalnych kandydatów, aby sami przedstawiali im zaświadczenia z Krajowego Rejestru Karnego. Taka praktyka jest niezgodna z prawem. Pracodawcy nie mają prawa do przetwarzania danych o karalności, jeżeli nie pozwala na to wyrażnie przepis prawa.

Wprawdzie samo żądanie podania danych nie jest jeszcze ich przetwarzaniem, ale też wymaga podstawy prawnej (por. wyrok Naczelnego Sądu Administracyjnego z 28 czerwca 2011 r., sygn. akt I OSK 1264/10), której brak w przypadku rekrutacji na stanowisko magazyniera. Ponadto już zapoznanie się z okazanym zaświadczeniem z KRK, a tym samym uzyskanie informacji w nim zawartych, jest przetwarzaniem danych, nawet jeżeli pracodawca nie zachowa takiego zaświadczenia w aktach.

Przetwarzania danych o karalności, które pracodawca pozyskał, zapoznając się z treścią zaświadczenia z KRK, nie można także zalegalizować poprzez odebranie od kandydata zgody na takie przetwarzanie. Zgoda jako podstawa prawna

przetwarzania danych osobowych pracowników jest kwestionowana zarówno przez generalnego inspektora ochrony danych osobowych (GIODO), jak i przez Naczelną Sąd Administracyjny (NSA). GIODO uważa, że taka zgoda, aby była skuteczna, musi być wyrażona w pełni dobrowolnie. Natomiast w relacji między pracodawcą a pracownikiem trudno jest zdaniem GIODO mówić o dobrowolności, gdyż występuje w tym przypadku stosunek nadrzędności zatrudniającego nad zatrudnionym, co może sprzyjać wymuszaniu zgody. Jeszcze dalej, jeżeli chodzi o kwestionowanie zgody w stosunkach pracy, posunął się NSA. W wyroku z 1 grudnia 2009 r. (sygn. akt I OSK 249/09) stwierdził, że wyrażona na prośbę pracodawcy zgoda pracownika na pobranie i przetworzenie jego danych osobowych narusza jego prawa i swobodę wyrażenia przez niego woli. Uznanie faktu wyrażenia zgody jako okoliczności uzasadniającej pozyskanie od pracownika innych danych niż wskazane w art. 22<sup>1</sup> kodeksu pracy (ustawy z 26 czerwca 1974 r. – Kodeks pracy; t.j. Dz.U. z 2014 r. poz. 1502 ze zm.) stanowiłoby obejście tego przepisu. Jeżeli tak jak w omawianym przypadku pracodawca żąda podania określonych danych, np. o niekaralności, a dodatkowo informuje kandydata, że ich podanie jest warunkiem koniecznym wzięcia udziału w rekrutacji, to trudno twierdzić, że zgoda, której kandydat

udzieliłby w tych okolicznościach, chcąc uniknąć negatywnych konsekwencji w postaci wykluczenia go z procesu rekrutacyjnego, jest zgodą wyrażoną w sposób dobrowolny.

Jednocześnie GIODO dopuszcza zbieranie dodatkowych informacji o kandydatach, jeżeli oni sami te dane podają w CV, mimo że pracodawca o to nie prosi. Wówczas zgoda na przetwarzanie

danych jest zdaniem GIODO w pełni dobrowolna. Wydaje się wobec tego, że kluczowym kryterium oceny dobrowolności wyrażenia zgody na przetwarzanie danych, a co za tym idzie – jej skuteczności, jest to, czy kandydat podał jakieś dane z własnej woli, czy z inicjatywy i na prośbę pracodawcy. Z tego względu powoływanie się na zgodę kandydata w przypadku zbierania danych o niekaralności wydaje się tym bardziej nieuzasadnione. Jest mało prawdopodobne, żeby osoba ubiegająca się o zatrudnienie sama z własnej woli pojawiła się na spotkaniu rekrutacyjnym z wyciągiem z KRK. Może się to zdarzyć w przypadku innych danych, np. referencji, które kandydaci często sami przedkładają, ale jeśli chodzi o dane o niekaralności, to jednak w zdecydowanej większości przypadków będą one udostępniane na prośbę pracodawcy, co z góry wyklucza dobrowolność zgody na ich przetwarzanie.

## 1 ZAŚWIADCZENIE O NIEKARALNOŚCI

Spółka MAGAZYNUI Z NAMI prowadziła rekrutację na stanowisko magazyniera do magazynu, w którym przechowywane są materiały budowlane. Zgłosił się m.in. Roman Kowalski. Agata Marcinkowska, pracownica działu HR, zadzwoniła do niego, aby zaprosić go na spotkanie:

- Dzień dobry. Panie Romanie, dzwonię w związku z pana zgłoszeniem do rekrutacji na stanowisko magazyniera w MAGAZYNUI Z NAMI. Czy znajdzie pan czas na spotkanie w przyszłą środę o godz. 11.00 w naszej siedzibie?
- Oczywiście, będę na pewno.
- Świetnie. Proszę przynieść ze sobą zaświadczenie o niekaralności z Krajowego Rejestru Karnego.
- Jak to? Po co wam takie informacje?
- Niekaralność jest warunkiem wzięcia udziału w rekrutacji na stanowisko magazyniera. Będzie pan odpowiadał za materiały o dużej wartości, więc chcemy się zabezpieczyć.
- A jeżeli nie przyniosę ze sobą takiego zaświadczenia?
- Obawiam się, że wtedy nie będzie pan mógł wziąć udziału w rekrutacji...
- No dobrze, skoro tak... Pewnie jeszcze będziecie chcieli, żebym podpisał jakieś dodatkowe zgody, dając wam to zaświadczenie z KRK? Kolega mi mówił, że musiał się zgodzić, bo to jego dane osobowe.
- Nie, panie Romanie, nic pan nie musi podpisywać. Nie jest nam potrzebna pana zgoda, bo nie zbieramy pana danych. Oddamy panu to zaświadczenie, nie będziemy go nawet kserować. Chcemy tylko, żeby je pan okazał.
- Rozumiem. W takim razie do zobaczenia za tydzień.

**Pytanie:** Czy przyszedł pracodawca może prosić kandydata o zaświadczenie z KRK? Czy faktycznie nie przetwarza danych, jeśli wymaga tylko okazania takiego dokumentu? A jeżeli jest to przetwarzanie danych, to czy powinien odebrać zgodę kandydata i czy będzie ona skuteczna?

**W** każdym przypadku, kiedy pracodawca zleca na zewnątrz określoną usługę, dla wykonania której niezbędne jest przekazanie danych osobowych pracowników, konieczne jest uregulowanie kwestii powierzenia ich przetwarzania. Zgodnie z art. 31 ust. 1 u.o.d.o. administrator danych (a więc w tym przypadku pracodawca) może powierzyć ich przetwarzanie innemu podmiotowi na podstawie umowy zawartej na piśmie. Może ona przybrać formę odrębnego dokumentu lub klauzuli zawartej w umowie głównej regulującej świadczenie usług, w związku z którym dane są przekazywane. Instytucja powierzenia przetwarzania danych osobowych jest bardzo często stosowana w praktyce, co jest pochodną rosnącego znaczenia outsourcingu usług na rzecz wyspecjalizowanych podmiotów. W przypadku zawarcia takiej umowy nie dochodzi do zmiany administratora danych. Pozostaje nim podmiot powierający, a więc pracodawca, jako że to on nadal decyduje o celu i środkach przetwarzania tych danych (por. art. 7 pkt 4 u.o.d.o.).

Umowa o powierzeniu przetwarzania danych powinna precyzować cel i zakres przetwarzania tych danych przez podmiot, któremu jest ono przekazane. Niedopuszczalne są jakiegokolwiek działania takiego podmiotu na danych powierzonych mu do przetwarzania, które wykraczałyby poza cel i zakres ich przetwarzania wskazany w umowie. Jeśli zatem administrator danych gromadzi i przetwarza dane osobowe pracowników w związku z zatrudnieniem, a następnie powierza ich prze-

tworzenie innemu podmiotowi w celu prowadzenia obsługi kadrowo-płacowej, to taki podmiot może je wykorzystywać tylko w tym konkretnym celu. Nie może natomiast używać tych danych np. w celach marketingowych, gdyż byłoby to niezgodne z umową o powierzeniu ich przetwarzania, a co za tym idzie – z przepisami ustawy o ochronie danych osobowych.

Podmiot, któremu zostało powierzone przetwarzanie danych osobowych pracowników, ma obowiązek podjąć środki zabezpieczające te dane. Nie zwalnia to administratora danych, a więc pracodawcy, z obowiązku nadzoru nad procesem ich przetwarzania. Odpowiedzialność z tytułu naruszenia ustawy o ochronie danych osobowych spoczywa bowiem zarówno na pracodawcy jako administratorze danych, jak i na podmiocie, któremu powierzono zostało ich przetwarzanie.

Administrator danych (w naszym przypadku pracodawca) nie ma obowiązku powiadamiania osób, których dane dotyczą, ani uzyskiwania ich odrębnej zgody na przetwarzanie tych danych przez podmiot zewnętrzny, któremu jest powierzane wykonywanie określonych usług (por. decyzja GIODO, sygn. GI-DEC-DS-215/05).

## 2 OUTSOURCING USŁUG

Spółka ZAKUPOMANIA na podstawie umowy o świadczenie usług przekazała obsługę płacową firmie zewnętrznej RozliczmyTwojePłace.pl. Pani Katarzyna z działu HR spółki ZAKUPOMANIA powzięła jednak wątpliwość, czy może przesłać dane pracowników do tej firmy. Dotychczas to ona zajmowała się rozliczaniem płac i posiadała upoważnienia do przetwarzania danych pracowników. W tej sprawie spotkała się więc z szefem.

- Panie prezesie, czy ja na pewno mogę przesłać dane naszych pracowników do tej firmy zewnętrznej? – zapytała.
- Pani Kasiu, jak najbardziej – odpowiedział prezes. Mamy przecież z nimi zawartą umowę na obsługę płac.
- Tak, ale ta umowa nie mówi nic o przekazaniu danych, a przeczytałam w internecie, że wymagane jest jakieś powierzenie przetwarzania danych – dopytywała dalej pani Katarzyna.
- Pani Kasiu, sprawdźmy to i porozmawiamy jutro, ale przecież jeśli nie prześlemy danych, to oni nie będą mogli nam świadczyć usług płacowych. Jest więc chyba oczywiste, że musimy dane przekazać i to jest pewnie takie doro-

**Pytanie:** Czy w związku z zawarciem umowy o świadczenie usług płacowo-kadrowych pracodawca może przekazać zewnętrznej firmie dane swoich pracowników? Czy sama taka umowa będzie do tego wystarczającą podstawą? Czy pracownik musi wyrazić na to zgodę?



Pracodawcy coraz częściej sięgają po różnego rodzaju środki techniczne w celu monitorowania wykonywania pracy przez zatrudnionych. Monitoring może mieć różne formy: monitoring wizyjny przy użyciu kamer, kontrola skrzynki e-mailowej, śledzenie aktywności w internecie itd. W Polsce kwestia stosowania monitoringu nie jest wprost uregulowana w przepisach prawa. Brak jest również orzecznictwa Sądu Najwyższego, które odnosiłoby się do tej kwestii. Dlatego konieczne jest odwoływanie się do dorobku doktryny oraz orzecznictwa Europejskiego Trybunału Praw Człowieka (ETPCz), a także do przepisów dotyczących ochrony danych osobowych. Dane gromadzone podczas monitoringu są bowiem danymi osobowymi w rozumieniu art. 6 ust. 1 ustawy o ochronie danych osobowych. Zgodnie z przepisami tej ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dane te mogą przy tym przybierać formę zdjęć, filmów, głosów czy komunikatów wyrażonych w jakikolwiek sposób.

W myśl art. 23 ust. 1 pkt 2 powołanej wyżej ustawy przetwarzanie danych osobowych jest dopuszczalne w szczególności wówczas, gdy jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Jednym z podstawowych obowiązków pracodawcy jest zapewnienie pracownikom bezpiecznych i higienicznych warunków pracy. Powinność ta jest jednocześnie źródłem jego uprawnień do kontrolowania zatrudnionych oraz miejsca, w którym wykonują pracę (zwłaszcza takich miejsc, gdzie pracownicy mogliby np. paść ofiarą przestępstwa lub ulec wypadkowi). Zatrudnieni mają z kolei obowiązek wykonywania pracy zgodnie z umową o pracę oraz są zobowiązani do dbałości o dobro zakładu pracy, co jednocześnie przekłada się na uprawnienie pracodawcy do nadzorowania ich pracy, a tym samym jest podstawą do zbierania danych dla potrzeb realizacji uprawnień nadzorczych w tym zakresie.

Z powyższych uprawnień i obowiązków można wyinterpretować prawo pracodawcy do monitorowania pracowników w zakresie, w jakim jest to niezbędne dla prawidłowego wykonywania tych uprawnień i obowiązków.

Podstawy prawnej monitorowania zatrudnionych można upatrywać również w rozporządzeniu ministra pracy i polityki socjalnej z 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz.U. nr 148, poz. 973), zgodnie z którym przy planowaniu wykonywania zadań z użyciem ekranu monitora pracodawca nie może bez wiedzy pracownika dokonywać kontroli jakościowej i ilościowej jego pracy. Wnioskując a contrario kontrola taka jest dopuszczalna, jeżeli pracownik zostanie o niej wcześniej poinformowany.

Przetwarzanie danych zbieranych w związku ze stosowaniem monitoringu może być również uzasadnione występowaniem po stronie pracodawcy prawnie usprawiedliwionego celu przetwarzania tych danych (art. 23 ust. 1 pkt 5 u.o.d.o.). Takim celem może być np. wyeliminowanie korzystania z internetu w celach prywatnych, ochrona tajemnicy przedsiębiorstwa oraz zabezpieczenie się przed wyrządzeniem szkody przez pracownika, np. w wyniku kradzieży. Jednak wprowadzając monitoring, pracodawca musi zwrócić uwagę na zasadę adekwatności przetwarzania danych w stosunku do celu ich przetwarzania. Również forma i zakres monitorowania

pracy w danym dziale i ma uzasadnione podejrzenie, że jej przyczyną jest zbyt częste korzystanie przez pracowników z internetu i poczty dla celów prywatnych, to powinien objąć monitoringiem wyłącznie ten dział, a nie całą firmę. Aby monitoring był legalny, konieczne jest poinformowanie zatrudnionych o możliwości jego stosowania z jednoczesnym określeniem jego formy, zakresu oraz celu, któremu ma służyć (por. np. wyrok ETPCz z 3 kwietnia 2007 r., sygn. akt 62617/00 w sprawie Copland v. Wielka Brytania). Odpowiednie zapisy powinny się znaleźć w regulaminie pracy lub też pracownicy powinni zostać zaznajomieni z zasadami monitorowania ich pracy w inny sposób przyjęty u danego pracodawcy. Od każdego pracownika warto ponadto uzyskać indywidualne pisemne oświadczenie o zapoznaniu się z zasadami stosowania monitoringu. Nie ma natomiast konieczności uzyskiwania zgody pracownika na jego przeprowadzanie, gdyż jak wskazano powyżej, pracodawca ma inne niż zgoda pracownika podstawy prawne do przetwarzania danych gromadzonych w związku z monitoringiem.

Wydaje się, że celowe byłoby dopuszczenie stosowania w pewnych szczególnych okolicznościach ukrytego monitoringu, a więc takiego, o którym pracownicy nie zostali poinformowani. Przykładowo uzasadnione może być poinformowanie o monitorowaniu skrzynki służbowej pracownika, którego podejrzewa się o przekazywanie tajemnic handlowych konkurencji. W przeciwnym wypadku, tj. gdyby pracownik został o tym powiadomiony, realizacja celu – wykrycie przecieku – mogłaby być niemożliwa. Zalecana jest jednak wyjątkowa ostrożność przy stosowaniu takiej formy monitoringu.

W każdym przypadku stosowanie monitoringu nie powinno nadmiernie ingerować w prywatność pracownika. Pracodawca nie jest uprawniony bez uprzedniej pisemnej zgody adresata i nadawcy do zapoznania się z treścią wiadomości prywatnej. W przypadku natrafienia na taką wiadomość w trakcie przeglądania poczty pracownika pracodawca nie powinien jej otwierać. Całkowicie niedopuszczalne jest także przetwarzanie sensytywnych danych pracownika (ujawniających np. pochodzenie rasowe, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową bądź partyjną, stan zdrowia, nałogi lub informacje o życiu seksualnym). Nawet uprzednia pisemna zgoda pracownika nie uzasadnia przetwarzania takich danych. W konsekwencji, w przypadku natknięcia się na takie informacje, powinny one zostać niezwłocznie usunięte z systemu.

Jeżeli monitoring jest legalny, tj. spełnione są wszystkie wyżej wymienione warunki, to wówczas materiały uzyskane w drodze kontroli mogą być bez ograniczeń używane jako dowody w sądzie. Oznacza to, że pracodawca będzie mógł uzasadnić np. wypowiedzenie umowy o pracę uzyskanymi w ten sposób informacjami i dowodzić jego zasadności w procesie przy użyciu wydruków z systemu.

### 3 MONITORING POCZTY

Firma zajmująca się sprzedażą leków dostała anonimową informację, że jeden z pracowników, Krzysztof Wawrzyniak, który wówczas znajdował się w okresie wypowiedzenia, wykradł bazę danych klientów. Prezes zarządu zwrócił się w tej sprawie do Anny Marciniak, dyrektor HR:

– Pani Aniu, proszę o sprawdzenie skrzynki e-mailowej Krzysztofa i potwierdzenie, czy rzeczywiście wysyłał dane poza spółkę – polecił.  
– Czy mamy prawo tak zrobić? – zapytała Marciniak.  
– Tak – odparł prezes. – Rozmawiałem na ten temat z naszym prawnikiem, który stwierdził, że jest to legalne. W naszym regulaminie pracy jest zapis, że pracodawca ma prawo monitorowania służbowej poczty elektronicznej pracowników m.in. w celu zwalczania zjawiska ujawniania danych stanowiących tajemnicę przedsiębiorstwa. Kontrola wykazała, że pan Krzysztof przesłał ze służbowej skrzynki na swój prywatny adres e-mailowy plik Excel zawierający listę i dane kontaktowe wszystkich klientów spółki. Pracodawca rozwiązał z nim umowę o pracę bez wypowiedzenia. W odpowiedzi na to zbulwersowany pracownik podniósł, iż monitoring jego poczty był nielegalny i że pracodawca nie będzie miał jak udowodnić kradzieży listy klientów, bo nie może użyć w sądzie dowodów zgromadzonych w trakcie monitoringu.

**Pytanie: Czy pracownik miał rację? Jakie są warunki legalnego monitorowania poczty zatrudnionych?**

nia pracowników powinny być proporcjonalne do tego celu. Z tych względów w literaturze przyjmuje się, że co do zasady niedopuszczalny jest monitoring prowadzony w sposób ciągły, permanentny. Ta forma kontroli powinna być stosowana jedynie doraźnie, tj. przez pewien okres, w związku z zaistnieniem szczególnych okoliczności. Nie tylko czas trwania, ale również zakres monitoringu nie powinien być szerszy, niż usprawiedliwiają to cele jego wprowadzenia. Przykładowo, jeżeli pracodawca zaobserwował bardzo niską efektyw-

nię powodów, potwierdzając tym samym ważność umów o zakazie konkurencji.

Składając do akt postępowania orzeczenie wydane w innej sprawie lub jakiegokolwiek inny dokument, pracodawca nie ma jednocześnie prawa dokonywać w nim żadnych skreśleń bądź innych ingerencji w jego treść. Jak wskazuje WSA w Warszawie, przedmiotem badania sądu w zakresie mocy dowodowej dokumentu, oprócz jego treści, jest również jego forma i wygląd zewnętrzny. Wszelkie zatem przekreślenia, usunięcia z dokumentu jego treści spowodowałyby, że mógłby on stracić swój walor dowodowy (por. powoływany powyżej wyrok z 12 maja 2008 r., sygn. akt II SA/Wa 326/o8). Na tej podstawie WSA w Warszawie wykluczył możliwość dokonywania jakiegokolwiek przekreśleń oraz usunięć w dokumentach składanych przez strony postępowania w charakterze dowodów.

Niezależnie od powyższego istotne jest również i to, że wyrok lub inny dokument jest składany w sądzie, a zatem w organie, który z mocy swoich ustawowych kompetencji jest uprawniony do przetwarzania wszelkiego rodzaju danych osobowych w zakresie, w jakim jest to niezbędne dla wydania rozstrzygnięcia w sprawie. Złożenie dokumentów jest tym bardziej dopuszczalne i zgodne z prawem, jeżeli – tak jak w omawianej sprawie – jest to ten sam sąd, który wydał wyrok składany przez pracodawcę do akt postępowania.

### 4 UJAWNIECIE WYROKU SĄDU

KONKURENCYJNA sp. z o.o. pozwała o zapłatę kar umownych kilku byłych pracowników, którzy naruszyli zakaz konkurencji wynikający z wiążących ich ze spółką umów o zakazie konkurencji po ustaniu stosunku pracy. W odpowiedzi wystąpili oni przeciwko spółce z powodztwami o ustalenie, że umowy te są nieważne. W międzyczasie w jednej ze spraw dotyczących kar umownych sąd wydał wyrok, zasądając od pracownika Mariusza Żaka na rzecz pracodawcy karę umowną w kwocie 20 tys. zł.

– Powinniśmy załączyć ten wyrok do akt w sprawach o ustalenie nieważności umów o zakazie konkurencji – zaproponował Marek Kamiński, prawnik spółki. – Sąd wyraźnie potwierdził w nim, że umowa o zakazie konkurencji wiążąca Mariusza ze spółką była ważna. – Na pewno byłoby to dla nas korzystne – stwierdziła Aneta Kowalska pełniąca w spółce rolę dyrektora HR. – Obawiam się tylko, czy nie narazimy się w ten sposób na zarzut naruszenia danych osobowych Mariusza? – zapytała.

– Taki zarzut, choć teoretycznie realny, byłby całkowicie nieuzasadniony – odpowiedział Kamiński. – Mieliśmy kilka miesięcy temu podobną sprawę. Jeden z naszych pracowników, którego dotyczyło orzeczenie złożone przez nas do akt innego postępowania, zwrócił się do GODO o jego usunięcie z tych akt. GODO odmówił, wyjaśniając, że nie doszło do naruszenia danych osobowych, a on jako organ nie ma prawa do ingerowania w materiał dowodowy zgromadzony w postępowaniu przed sądem – zakończył.

**Pytanie: Czy pracodawca może złożyć wyrok wydany w jednej sprawie do akt postępowania w innej sprawie? Czy nie prowadzi to do naruszenia danych osobowych pracownika, którego on dotyczy? Czy pracodawca powinien zanonimizować te dane? Czy GODO ma prawo ingerencji i nakazania usunięcia takiego wyroku lub innego dokumentu z akt postępowania?**

Zgodnie z par. 34 ust. 1 pkt 11 rozporządzenia ministra sprawiedliwości z 25 czerwca 2015 r. – Regulamin urzędowania sądów powszechnych (Dz.U. poz. 925) obowiązki administratora danych osobowych pełni prezes sądu. Zatem dane trafiają do podmiotu, który był już wcześniej uprawniony do ich przetwarzania, wydając wyrok składany następnie przez pracodawcę.

Dla oceny istnienia uprawnienia pracodawcy do złożenia wyroku wydanego w danej sprawie do akt innego postępowania nie ma znaczenia okoliczność, że pracownik, którego dotyczy składane orzeczenie, nie jest stroną tego drugiego procesu. Trzeba bowiem zaznaczyć, że omawiane uprawnienie do przetwarzania danych z art. 27 ust. 2 pkt 5 u.o.d.o. dotyczy danych osobowych wszystkich osób – także tych, które nie są stronami konkretnego postępowania. Potwierdził to GODO w decyzji z 28 października 2004 r. (GI-DEC-DS.-232/04).

GODO nie ma uprawnienia, aby nakazać sądowi usunięcie z akt sprawy danych osobowych wynikających z wyroku lub innego dokumentu załączonego do akt postępowania sądowego. Z chwilą włączenia złożonego przez pracodawcę wyroku (lub innego dokumentu) w poczet materiału dowodowego staje się częścią akt postępowania. Nakaz jego usunięcia z tej dokumentacji byłby nieuprawnionym ingerowaniem GODO w tok procesu przed sądem lub innym organem.

Pracodawca może przetwarzać takie dane w ramach innych postępowań sądowych, powołując się w szczególności na art. 27 ust. 2 pkt 5 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem przetwarzanie danych wrażliwych dotyczących w szczególności orzeczeń wydawanych w postępowaniach sądowych i administracyjnych jest dopuszczalne m.in. wówczas, gdy dotyczy informacji, które są niezbędne do dochodzenia praw przed sądem. Natomiast w myśl art. 232 kodeksu postępowania cywilnego (ustawy z 17 listopada 1964 r. – Kodeks postępowania cywilnego; t.j. Dz.U. z 2014 r. poz. 101 ze zm.), który reguluje także postępowanie przed sądami pracy, strony są zobowiązane wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne. Pracodawca jako strona postępowania jest zobowiązany do złożenia jako dowodu w sprawie sądowej m.in. dokumentów, które potwierdzają jego twierdzenia i przeczą zapewnieniom strony przeciwnej. Strona ma przy tym prawo składać takie dokumenty i wnioski dowodowe, jakie w jej ocenie mają istotne znaczenie dla rozpatrywanej sprawy (por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 12 maja 2008 r., sygn. akt II SA/Wa 326/o8 oraz decyzję generalnego inspektora ochrony danych osobowych wydaną w tej samej sprawie). Brak złożenia jakiegogoś dowodu może przesądzić o wyniku sprawy i spowodować, że dana strona (w tym przypadku pracodawca) przegra przed sądem. Dlatego w doktrynie podkreśla się, że ochrona danych osobowych, w tym powoływanie się na zakaz przetwarzania danych wrażliwych z art. 27 ust. 1 u.o.d.o. nie może być przeszkodą do prawidłowego rozstrzygnięcia sprawy przez sąd (por. decyzja GODO z 28 października 2004 r., GI-DEC-DS.-232/04). Nie można się sprzeciwiać przetwarzaniu takich danych, których udostępnienie jest niezbędne do dochodzenia praw przed sądem.

W omawianej sprawie złożenie wyroku wydanego w sprawie o zasądzenie kary umownej z tytułu naruszenia zakazu konkurencji do wszystkich spraw o ustalenie nieobowiązywania umów antykonkurencyjnych było niezbędne. W wyroku tym sąd jednoznacznie zaprzeczył bowiem roszcze-