**Uwagi Związku Pracodawców Polska Miedź**

**do projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych**

**(projekt z dnia 12 września 2017 roku)**

**I. Uwagi wstępne.**

Zgodnie z art. 5 ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, zamieszczonym na stronie Ministerstwa Cyfryzacji (projekt z dnia 12 września 2017 r.), przewiduje się nowelizację Kodeksu pracy w zakresie przepisów dotyczących ochrony danych osobowych pracowników (odpowiednio kandydatów do pracy). Ponadto upublicznione zostało uzasadnienie tej ustawy oraz ocena skutków regulacji, które odpowiednio w pkt 3 i 2.21 odnoszą się do zmian
w Kodeksie pracy.

Zarazem stworzona została możliwość wniesienia uwag w ramach konsultacji publicznych. Konsultacje z założenia mają stanowić sposób komunikacji pomiędzy ustawodawcą a adresatami norm prawnych. Chodzi więc o stworzenie możliwości uprzedniego zweryfikowania norm prawnych pod kątem ich społecznego i gospodarczego oddziaływania.

Projektowane przepisy wprowadzają uregulowanie ograniczające zakres oraz podstawy przetwarzania danych osobowych pracowników, co nie pozostanie bez wpływu na funkcjonowanie przedsiębiorstw. Podsumowując skutki projektowanej nowelizacji Kodeksu Pracy, należy wskazać na dwa główne obszary oddziaływania. Przepisy wpłynęłyby negatywnie na procesy biznesowe
i organizacyjne (ograniczenia dot. min. przetwarzania wizerunku pracownika oraz informacji o jego kompetencjach). Przede wszystkim jednak poza możliwościami pracodawcy mógłby pozostać obszar tzw. kontroli wewnętrznej obejmującej zapobieganie niepożądanym zjawiskom (fraudom, korupcji) wpływające na aspekty sprawozdawczości rachunkowej, a przede wszystkim realnie zagrażającym interesom przedsiębiorstwa.

Według uzasadnienia projektowanej nowelizacji, przesłanka istnienia „obowiązku prawnego” stanowi główną podstawę legalizującą przetwarzanie danych osobowych pracowników oraz kandydatów do pracy. Jako drugą przesłankę uzasadnienie wskazuje *w pełni dobrowolną zgodę pracownika* (odpowiednio kandydata do pracy) na przetwarzanie danych innych niż wymienione w art. 221 K.p. oraz danych biometrycznych. W wyniku tego rodzaju unormowania pracownik zyskałby ochronę prywatności wykraczającą w znacznym stopniu poza normy Ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO). W ocenie autora opracowania, byłaby to ochrona nadmiarowa uwzględniając szereg postanowień RODO, które i tak wprowadzają instytucje statuujące wysoką ochronę danych.

Powołane fragmenty uzasadnienia ustawy oraz z literalne brzmienie projektowanych przepisów mogą prowadzić do wniosku, że pracodawca nie będzie mógł przetwarzać danych osobowych
w oparciu o przesłankę uzasadnionego interesu, a zwłaszcza nie będzie mógł żądać od pracownika podania danych i ich przetwarzać w celu realizacji prawnie uzasadnionych interesów administratora.

**II. Oddziaływanie projektowanych przepisów w obszarze bezpieczeństwa wewnętrznego przedsiębiorstwa.**

 W ostatnich latach przyjęło się tworzenie wewnętrznych regulacji mających zapobiegać niepożądanym zjawiskom, a zwłaszcza korupcji, fraudom i konfliktom interesów, a także ogólnie promujące etyczne zachowania w miejscu pracy. Pracodawca realizuje w ten sposób dyspozycje wynikające z przepisów Kodeksu spółek handlowych (jeżeli dotyczy), art. 94 Kodeksu pracy oraz art. 10 i 24 ustawy o rachunkowości. Również Międzynarodowe Standardy Rachunkowości i Międzynarodowe Standardy Sprawozdawczości Finansowej oraz interpretacje Komisji Europejskiej obligują do podjęcia czynności zapewniających sporządzenie sprawozdania finansowego nie zawierającego istotnego zniekształcenia spowodowanego oszustwem czy innymi zdarzeniami skutkującymi błędnymi zapisami.

Istnieje obawa, że zostanie przyjęta restrykcyjna wykładnia projektowanego art. 223 K.p.
w części odwołującej się do przesłanki wypełnienia obowiązku wynikającego z przepisu prawa. Obecna redakcja projektowanego zapisu wydaje się co prawda być mniej rygorystyczna wobec obecnie obowiązującej normy z art. 221  § 4 K.p., co jednak może nie usunąć nasuwających się wątpliwości. Obowiązek dbałości o dobro zakładu pracy ma charakter ogólny, a żaden przepis nie statuuje katalogu czynności, z którymi można powiązać przetwarzanie danych osobowych w tym aspekcie. Podobnie działania pracodawcy promujące i egzekwujące zachowania etyczne jak unikanie konfliktu interesów,
a tym bardziej realizujące politykę antykorupcyjną i zapobiegającą sprzeniewierzeniom środków, wymagają aktywności związanej z przetwarzaniem danych osobowych pracowników w zakresie wprost nieuregulowanym.

W kontekście powyższego, na szczególną uwagę zasługuje treść motywu (47) RODO: „*Prawnie uzasadnionym interesem administratora, którego sprawa dotyczy, jest również przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom*”. Brak jest argumentów natury aksjologicznej, w tym zwłaszcza społecznych, dla uzasadnienia wyłączenia pracowników z kręgu osób, których dane osobowe mogą być przetwarzane w calu zapobiegania oszustwom bądź innym niepożądanym sytuacjom o zbliżonej wadze dla przedsiębiorstwa i społeczeństwa.

Zaznaczyć należy, że pracownik nie wchodzi w relacje związane jedynie ze stosunkiem pracy. Pracodawca, obok celów związanych bezpośrednio ze stosunkiem pracy, realizuje również inne cele między innymi w zakresie wewnętrznego bezpieczeństwa organizacyjnego przedsiębiorstwa, w tym dbałości o prawidłową politykę finansową, także w aspekcie nadzoru korporacyjnego. Są to bowiem zachowania społecznie akceptowalne (czy wręcz pożądane).

W ocenie autora opracowania, zasadnym jest także odwołanie się do *Opinii 2/2017 Grupy Roboczej Art. 29 Dyrektywy nr 95/46/EC do spraw ochrony danych osobowych w sprawie przetwarzania danych w pracy* przyjętej w dniu 8 czerwca 2017 r., opublikowanej pod adresem: <http://ec.europa.eu/justice/data-protection/index_en.htm>.

Grupa Robocza Art. 29 wyraźnie opowiada się za możliwością przetwarzania danych osobowych pracownika również w oparciu o przesłankę uzasadnionego interesu. Jednoznacznie wskazuje na to pkt 6.2 powołanej Opinii: „*Uzasadniony interes pracodawcy może niekiedy być powoływany jako podstawa prawna, jednak wyłącznie wówczas, gdy przetwarzanie jest ściśle konieczne dla uzasadnionego celu oraz uwzględnia zasady proporcjonalności i pomocniczości. Test proporcjonalności powinien zostać przeprowadzony przed wdrożeniem jakiegokolwiek narzędzia monitorującego celem rozważenia, czy wszystkie dane są konieczne, czy przetwarzanie ma znaczenie większe niż ogólne zasady prywatności pracowników w miejscu pracy oraz jakie środki muszą być przedsięwzięte, aby zapewnić, że naruszenie prawa do życia prywatnego oraz tajemnicy komunikacji są ograniczone do koniecznego minimum.*”

W świetle utrwalonego orzecznictwa nie budzi również wątpliwości dopuszczalność zobowiązania pracownika przez pracodawcę do udzielenia informacji o zamiarze podjęcia lub podjęciu dodatkowej aktywności zawodowej, jeżeli dotyczy to pracy i nie jest sprzeczne z umową o pracę (tak: wyrok Sądu Najwyższego z dnia 19.01.2017 r., I PK 33/16; wyrok Sądu Najwyższego z dnia 5.03.2007 r., I PK 228/06). Zatem w zakresie uzasadnionym ochroną interesów pracodawcy, do jakich niewątpliwie należy przeciwdziałanie zagrożeniom korupcyjnym oraz konfliktom interesów, jak również mając na względzie dążenie pracodawcy do zapewnienia prawidłowości i transparentności w zakresie obowiązków rachunkowych, pracodawca powinien mieć prawo domagać się od pracownika podania informacji oraz przetwarzania jego danych osobowych - motyw (47) RODO. Takie podejście jest skorelowane z obowiązkiem pracownika dbania o dobro zakładu pracy, zgodnie z art. 100 § 2 pkt 4 K.p. Chodzi więc o bezpieczeństwo wewnętrzne przedsiębiorcy postrzegane również jako dbałość o interes pracodawcy w aspekcie finansowym i prawno-karnym.

Należy też zwrócić uwagę na normę ISO 37001, której celem jest wspomaganie firm w implementacji strategii i procedur pomocnych w ograniczeniu ryzyka wystąpienia korupcji w organizacji (<https://www.pwc.pl/pl/pdf/poradnik-antykorupcyjny-dla-biznesu.pdf>).

Na instrumenty związane ze zwalczaniem korupcji powołują się także Marian Cichosz i Alina Hussein, autorzy opracowania dostępnego na stronie: <https://cba.gov.pl/ftp/publikacje/Materialy_pokonferencyjne_II.pdf> (zwłaszcza str. 50 i 54).

Tym samym norma wyrażona w projektowanym art. 224 § 1 K.p. odnosząca się wyłącznie do ochrony mienia poprzez CCTV wydaje się zbyt wąska w relacji o potrzeb gospodarczych i społecznych.

Odwołując się do zaleceń zawartych w pkt 6.2 *Opinii 2/2017 Grupy Roboczej Art. 29 Dyrektywy nr 95/46/EC do spraw ochrony danych osobowych w sprawie przetwarzania danych w pracy*, „*narzędzie monitorujące*” powinno być rozumiane szeroko, w sposób odpowiadający potrzebom gospodarczym i społecznym. Ostatecznie to ogół pracowników będzie ponosić negatywne skutki naruszania dobra zakładu pracy przez jednostki naruszające obowiązujące normy.

W tym kontekście wskazać można także na akceptowaną obecnie możliwość ingerowania przez pracodawcę w prywatność pracowników m. in. poprzez monitorowanie aktywności w sieci, kontrolę służbowej poczty elektronicznej, monitoring wizyjny. Opiniujący pomija szerszą analizę tego aspektu z uwagi utrwalone w tym zakresie poglądy judykatury oraz GIODO (warunkiem jest uprzedzenie pracownika o potencjalnej ingerencji). Unormowanie wprowadzone zgodnie z projektem cytowanego przepisu może spowodować szereg wątpliwości w odniesieniu do monitorowania środowiska pracy w szerszym ujęciu, zwłaszcza że art. 88 RODO w ust. 2 wprost odnosi się do *systemów monitorujących* (a więc nie tylko do CCTV).

Z kolei zapis w projektowanym art. 224 § 1 K.p. *monitoring nie może stanowić środka kontroli wykonywania pracy przez pracownika* spowoduje ograniczenia lub wątpliwości w wypadkach przeliczania pieniędzy, wydawania przepustek czy nadzorowania procesów produkcyjnych.

Zakres przygotowywanej noweli powoduje więc wątpliwości co do legalności pozyskania danych, których przetwarzanie niejednokrotnie determinuje prawidłowe funkcjonowanie przedsiębiorstw, zwłaszcza średnich i dużych. Przy tym dyspozycja art. 222 § 1 K.p. nie usuwa wszystkich potencjalnych problemów.

Dotyczy to także przetwarzanie wizerunku pracownika, co byłoby możliwe wyłącznie na podstawie jego zgody, ewentualnie przepisu prawa (wypełnienia obowiązków w okolicznościach precyzowanych przez art. 223 K.p.). Tymczasem słusznie wskazuje się, że istnieją sytuacje, w których realizacja uzasadnionego interesu pracodawcy wymaga przetwarzania danych osobowych w zakresie wykraczającym poza aktualnie obowiązującą dyspozycję art. 221 K.p. Jako przykład wskazuje się właśnie przetwarzanie wizerunku np. w związku z przyjętą organizacją pracy, uzasadnioną zakresem działalności przedsiębiorstwa (np. stanowisko Głównego Inspektora Ochrony Danych Osobowych:
„*Z uwagi jednak na to, że wśród wymienionych informacji o pracowniku w powołanych przepisach Kodeksu pracy nie ma zdjęcia pracownika, to pracodawca, aby  móc legalnie je pozyskać w celu np. umieszczania na identyfikatorach czy stronach internetowych firm, musi – co do zasady – pozyskać na to zgodę pracownika. /…/ Istnieją jednak sytuacje wyjątkowe, gdy wizerunek pracownika jest ściśle związany z wykonywanym przez niego zawodem czy charakterem pracy. Jako przykład podać można choćby pracowników ochrony, co do których – ze względów bezpieczeństwa – powinna być możliwość ich identyfikacji. Wówczas można odstąpić od pozyskiwania takiej zgody w tym właśnie celu.*” - źródło: <http://www.giodo.gov.pl/pl/348/4859>.

Zaznaczyć należy, że względy bezpieczeństwa odnosić należy nie tylko do służb ochrony
w rozumieniu właściwych przepisów, ale także ogólnie bezpieczeństwa wewnętrznego oraz organizacji pracy w dużych i średnich przedsiębiorstwach (identyfikatory pracowników).

**III. Oddziaływanie projektowanych przepisów w obszarze HR oraz obsługi ZFŚS**

Ponadto autor opracowania wskazuje na dalsze konsekwencje projektowanych przepisów art. 221 § 1, 2 i 4 w związku z art. 222 § 1 K.p. oraz 223 § 1 K.p.

Również przetwarzanie informacji o kompetencjach pracownika, zarówno tzw. twardych, jak
i miękkich, wydaje się niezbędne w nowoczesnej gospodarce. Za dopuszczalnością przetwarzania danych uzyskanych z testów psychologicznych opowiedziały się urzędy właściwe dla ochrony danych osobowych w Polsce, Czechach, Chorwacji i Bułgarii w opracowaniu „Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników”; dostępnym pod adresem: <https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjIsIv8YXUAhXkB5oKHbsgBGcQFgg0MAI&url=http%3A%2F%2Fwww.giodo.gov.pl%2Fplik%2Fid_p%2F6123%2Fj%2Fpl%2F&usg=AFQjCNHQyArlx4ylssYVvLPBtRHBHG5fzQ&sig2=6tY0SKkMFj8Nkqi0gCRgoQ>.

Ponadto szereg wątpliwości interpretacyjnych i praktycznych zostało ujętych w sygnalizacji GIODO do Ministra Pracy i Polityki Społecznej: <https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwjIsIv8YXUAhXkB5oKHbsgBGcQFgg8MAQ&url=http%3A%2F%2Fwww.giodo.gov.pl%2Fplik%2Fid_p%2F1749%2Fj%2Fpl%2F&usg=AFQjCNEzmz7OPmnu5d0D6xrg7qE5QKe0A&sig2=i8LEtPWdKf8DJDLB-yW6Dg>.

W odniesieniu do projektowanej treści art. 222 § 5 pkt 2 K.p. *Przetwarzanie danych osobowych obejmujących dane o stanie zdrowia − nie jest możliwe nawet za zgodą, o której mowa w § 1*, można wskazać, że uniemożliwi on premiowanie pracowników niepalących w miejscu pracy. Ta podstawa premiowania uznawana jest aktualnie za prawnie dopuszczalną. Realizuje interes zarówno pracownika, jak i pracodawcy.

Ponadto brzmienie projektowanego art. 221 § 4 (*przetwarzanie danych osobowych, o których mowa w § 1 - 3, jest możliwe tylko w zakresie niezbędnym do realizacji stosunku pracy*) oraz art. 222 § 1 (*przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 221 § 1 i 2 jest dopuszczalne tylko wtedy, gdy dotyczą one stosunku pracy i osoba ubiegająca się o zatrudnienie lub pracownik wyrazi na to zgodę*) będzie powodować utrudnienia w realizacji świadczeń wynikających
z ZFŚS. Autor wystąpienia wskazuje na powszechną praktykę pracodawców zlecania usług turystycznych na rzecz pracowników. Z uwagi na zawężenia celu przetwarzania w § 4 art. 221 K.p. do realizacji stosunku pracy oraz jednoczesne ograniczenie możliwości wyrażenia zgody pracownika do danych innych od określonych w § 1 i 2 tego przepisu, literalnie rzecz biorąc, nie będzie możliwe dokonanie udostępnień danych pracowników organizatorom turystyki oraz firmom ubezpieczeniowym. To znaczy, że pracodawca legalnie pozyska dane w związku z obsługą ZFŚS, jednak nie będzie mógł ich udostępnić nawet za zgodą pracownika.

Problem ten narasta wobec dyspozycji art. 222 § 5 pkt 2. W wypadku wyjazdów kolonijnych organizator wypoczynku może przetwarzać dane o stanie zdrowia dziecka w zakresie określonym w rozporządzeniu wydanym na podstawie art. 92t ustawie o systemie oświaty. Pracodawca pozbawiony zostałby możliwości przetwarzania tych danych w oparciu o przesłankę zgody w związku z czynnościami organizującymi wyjazd (w ramach zleconej usługi turystycznej).

**IV. Analiza dotycząca przetwarzania danych biometrycznych.**

Uzasadnienie projektu zmian trafnie wskazuje na potrzebę uregulowania przetwarzania danych biometrycznych, przywołując kontekst przetwarzania - interes pracodawcy, jak i pracownika. O ile realizacja uzasadnionego interesu przez pracodawcę może podlegać zobiektywizowanym ocenom (przez pryzmat przedmiotu lub skali działalności, to już poczucie interesu pracownika może być mocno subiektywne.

Konkludując, autor opracowania zmierza do tego, że częste będą sytuacje, w których część (być może większa) pracowników, dostrzegając interes swój oraz przedsiębiorstwa, wyrazi zgodę na przetwarzanie danych biometrycznych, a niektóre osoby jej nie wyrażą. W wypadku więc systemów dostępowych opartych o dane biometryczne, pracodawca będzie zmuszony z nich zrezygnować
z uwagi na brak zgody choćby kilku (nawet jednej) osób, bądź wdrożyć alternatywne rozwiązanie.

Dodatkowo należy zauważyć, że przepis art. 222 § 2 K.p. (*przetwarzanie przez pracodawcę danych biometrycznych obejmuje tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy
i pracownik wyrazi na to zgodę*) może być przyczyną przyszłych sporów, gdy kilku pracowników uzna swoją zgodę za wymuszoną presją wynikającą z faktu, że większość załogi wyraziła zgodę. Jawi się to jako bardzo prawdopodobne w wypadku zwłaszcza rozwiązania stosunku pracy (według *§ 3: Brak zgody, o której mowa w § 1 i 2, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenia stosunku pracy lub jego rozwiązania bez wypowiedzenia przez pracodawcę).*

Wydaje się więc zasadnym rozszerzenie możliwości przetwarzania danych biometrycznych
o przesłankę prawnie usprawiedliwionego interesu. Uwaga ta koresponduje z zapisem uzasadnienia ustawy: *W wielu przypadkach, gromadzenie danych biometrycznych uzasadnione jest stosunkiem pracy a jednocześnie ich gromadzenie w żadnym zakresie nie stanowi ograniczenie praw i wolności osób, których dane dotyczą.*

**V. Podsumowanie**

Reasumując, pracodawca powinien mieć możliwość przetwarzania danych w stopniu szerszym co do zakresu i podstawy, w tym w wyniku żądania ich podania, niezbędnych do prowadzenia procesów biznesowych i organizacyjnych, uwzględniając ryzyko oraz kontekst przetwarzania, przy poszanowaniu zasad ochrony danych osobowych.

Dotyczy to sytuacji, w których cel przetwarzania związany jest z funkcjonowaniem zakładu pracy jako pewnej całości, stanowiącej przedsiębiorstwo w znaczeniu podmiotowym i funkcjonalnym. Pracodawca realizuje bowiem szereg czynności, które sumarycznie mają prowadzić do zapewnienia prawidłowego funkcjonowania zakładu pracy. Czynności te są niezbędne do realizacji prawnie uzasadnionych interesów przedsiębiorstwa i jedynie pośrednio dotyczą stosunku pracy.

Tym samym, na podstawie art. 88 ust. 1 RODO, zasadnym byłoby, zamiast wprowadzenia istotnego ograniczania zakresu przetwarzania osobowych pracownika, uszczegółowienie zasad przetwarzania tych danych w myśl ust. 2 tego przepisu, poprzez wprowadzenie odpowiednich
i szczegółowych środków zapewniających 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.