

dr Marta Otto
Wydział Prawa i Administracji
Uniwersytet Warszawski

Opracowanie wycinkowe pt.:
Ochrona i przetwarzanie danych osobowych
– potrzeba i możliwość regulacji w u.z.p.

1. Uwagi wprowadzające- o potrzebie regulacji w u.z.p.

Postępująca cyfryzacja środowiska pracy, polegająca na coraz szerszym wykorzystaniu technologii cyfrowych w różnych aspektach funkcjonowania miejsca pracy (od organizacji pracy, przez sposób komunikacji, aż po monitorowanie, ocenę i zarządzanie pracownikami), prowadzi do przyspieszonej datafikacji pracy – systematycznego przekształcania aktywności pracowników, interakcji zawodowych i wyników pracy w dane podlegające zbieraniu, analizie i dalszemu wykorzystaniu przez pracodawcę. Obecny model ich pozyskiwania, coraz częściej opierający się na technologiach opartych na algorytmach umożliwia pracodawcom gromadzenie coraz większych zasobów danych (Big Data).

Kluczową rolę w tym procesie odgrywa rosnąca interoperacyjność nowych technologii. O ile wcześniej narzędzia monitoringu funkcjonowały niezależnie – rozwój technologii określanych jako *Surveillance 4.0* pozwolił na tworzenie zintegrowanych ekosystemów nadzoru, w których urządzenia i aplikacje tworzą spójną infrastrukturę przetwarzania danych. W tym modelu obserwatorem nie jest już pracodawca, lecz rozproszony system algorytmiczny (tj. zautomatyzowany system monitorujący i decyzyjny¹), generujący m.in. prognozy behawioralne, wskaźniki efektywności czy profile ryzyka,

¹ Zob.art. 2.1 h) i i) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2831 z dnia 23 października 2024 r. w sprawie poprawy warunków pracy za pośrednictwem platform



wykorzystywane później w takich obszarach, jak rekrutacja, kształtowanie warunków zatrudnienia, ocena okresowa, awans czy rozwiązywanie stosunku pracy².

Obserwowany zwrot w stronę szeroko rozumianego nadzoru technologicznego prowadzi do pogłębienia asymetrii informacyjnej, a co za tym idzie – asymetrii negocjacyjnej między pracodawcą a pracownikami. W tym kontekście ogólne zasady wynikające z rozporządzenia ogólnego o ochronie danych osobowych (dalej: RODO³) coraz częściej okazują się niewystarczające do zapewnienia adekwatnej ochrony praw podstawowych pracowników, takich jak prawo do prywatności (art. 7 Karty Praw Podstawowych UE-dalej KPP) (w tym prywatności informacyjnej Art.8 KPP), a także skorelowanych z nim: prawa do pracy (art.15 KPP), zakazu dyskryminacji (Art.21 KPP), prawa do należytych i sprawiedliwych warunków pracy (Art.31 KPP), czy do ochrony przed nieuzasadnionym zwolnieniem z pracy (Art.30 KPP)⁴.

Kluczowym wyzwaniem w praktyce jest sama konstrukcja RODO, osadzona na podejściu opartym na ryzyku i zasadzie rozliczalności obciążającej administratora danych. W konsekwencji – to pracodawca, jako administrator danych, ma obowiązek oceny „prawdopodobieństwa i wagi ryzyka” naruszenia praw lub wolności podmiotów danych (pracowników) wynikającego z planowanych operacji przetwarzania danych (Art. 24 RODO). Jednocześnie rozporządzenie nie zawiera precyzyjnych kryteriów porównywania i wartościowania ryzyk; wymaga jedynie odniesienia się do charakteru, zakresu, kontekstu i celów przetwarzania danych (motyw 76 RODO).

² Szerzej Otto M., The rise of algorithmic surveillance: legal and ethical implications for the future of work, [w:] M.Biasi AI & Labour Law (Routledge, 2026).

³ Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych)

⁴ Zob. Otto M., “Workforce Analytics v Fundamental Rights Protection in the EU in the Age of Big Data” (2019) 40 Comparative Labor Law & Policy Journal 389-404; Aloisi A., Gramano E., “Artificial intelligence is watching you at work: digital surveillance, employee monitoring, and regulatory issues in the EU context” (2020) 41 Comparative Labor Law and Policy Journal 95–122. Ponce Del Castillo A., AI: the value of precaution and the need for human control, Alida Ponce Del Castillo (ed.), Artificial intelligence, labour and society (ETUI, 2024), 13-26; Rogers B., “The Law and Political Economy of Workplace Technological Change” (2020) 55 Harvard Civil Rights–Civil Liberties Law Review 531–584.



Z punktu widzenia modelu regulacyjnego rozwiązanie to wpisuje się w logikę tzw. współzarządzania regulacyjnego (*collaborative governance*), w ramach którego ustawodawca europejski deleguje na administratorów danych odpowiedzialność za dobór kontekstowo „odpowiednich” środków technicznych i organizacyjnych (motyw 78 RODO). W realiach stosunku pracy (charakteryzującego się pogłębiającą się nierównowagą sił oraz ograniczoną zdolnością pracowników do skutecznego egzekwowania swoich praw) mechanizm ten generuje tzw. dylemat funkcjonalnej suwerenności (*functional sovereignty dilemma*) – pracodawcy zaczynają pełnić rolę quasi-regulatorów, de facto kształtując standardy ochrony danych w praktyce⁵.

W konsekwencji, instrumenty współzarządzania – zarówno formalne (takie jak kodeksy postępowania czy oceny skutków dla ochrony danych), jak i nieformalne (np. praktyki organizacyjne, wytyczne Inspektorów Ochrony Danych) – mogą przekształcić się w narzędzia fasadowe. Zamiast wzmacniać ochronę praw podstawowych pracowników w związku z przetwarzaniem ich danych osobowych, mogą legitymizować inwazyjne praktyki przetwarzania danych w oparciu o ich ‘niezbędność’ do realizacji szeroko definiowanych ‘interesów pracodawcy’ – takich jak: efektywność operacyjna przedsiębiorstwa (w tym kontrola produkcji, pełnego wykorzystania czasu pracy czy właściwego użytkowania udostępnionych pracownikowi narzędzi pracy), realizacja obowiązków BHP, ochrona mienia, tajemnicy przedsiębiorstwa, czy zapewnienie środowiska wolnego od dyskryminacji, mobbingu i molestowania⁶.

Co najważniejsze – reżim ochrony danych osobowych, ze względu na silnie zindywidualizowaną orientację, wydaje się niewystarczający do przeciwdziałania zbiorowym i zagregowanym/kumulatywnym zagrożeniom dla ochrony prywatności (w tym prywatności informacyjnej) oraz szkodom społecznym (*societal harms*), jakie mogą generować nowe technologie. Wpływ systemów technologicznych na prawa pracowników co do zasady nie powinien być postrzegany w izolacji, ponieważ

⁵ Otto M. (2022), “A step towards digital self- & co-determination in the context of algorithmic management systems”, in *Italian Labour Law e-Journal*, 15(1), 51–64.

⁶ Otto M. Privacy at Work and the Right to Private Life Outside Work [w:] Guy Davidov, Brian Langille, Gillian Lester, *The Oxford Handbook of the Law of Work*, Oxford University Press, 2024, 633–644.



zasadniczy problem nie wynika z jednego rodzaju technologii, lecz z poszczególnych ‘fal innowacji’, obejmujących różnorodne aspekty organizacji cyfrowego świata pracy. W istocie szkody społeczne ujawniają się wówczas, gdy operacje i praktyki przetwarzania danych albo utrudniają bądź uniemożliwiają korzystanie z praw, albo umożliwiają manipulowanie jednostkami i grupami w sposób zdolny do zmiany istniejących relacji władzy⁷.

W tym kontekście negocjowanie szczegółowych zasad przetwarzania danych w ramach układów zbiorowych wydaje się strategicznym narzędziem ochrony praw podstawowych pracowników we współczesnym – coraz bardziej cyfrowym – środowisku pracy⁸. Art. 88 RODO wyraźnie upoważnia przy tym państwa członkowskie oraz partnerów społecznych do ustanawiania bardziej szczegółowych norm przetwarzania danych osobowych w zatrudnieniu w drodze ustaw lub układów zbiorowych. W praktyce, układy zbiorowe mogą stać się nie tylko mechanizmem ochronnym, ale przede wszystkim narzędziem proaktywnego/partycypacyjnego modelu ustalania standardów prawnych przetwarzania danych osobowych pracowników uwzględniających szeroki zakres ryzyk generowanych przez cyfrowe środowisko pracy. Art. 88 RODO powinien być zatem postrzegany jako potencjalny punkt wyjścia do rekonfiguracji modelu regulacji ochrony danych osobowych w świecie pracy w sposób lepiej odpowiadający asymetriom władzy oraz strukturalnym zagrożeniom generowanym przez technologie nadzoru.

Niniejsza ekspertyza wycinkowa ma na celu dostarczenie związkom zawodowym praktycznych wskazówek dotyczących kluczowych obszarów negocjacji w układach zbiorowych w zakresie ochrony i przetwarzania danych osobowych pracowników w kontekście wyzwań współczesnego środowiska pracy.

⁷

⁸ V. De Stefano and S. Taes, “Algorithmic management and collective bargaining”, *Transfer*, 29(1), 2023, 21–36; V. Doellgast, S. Appalla, D. Ginzburg, J. Kim and W. L. Thian, “Global case studies of social dialogue on AI and algorithmic management”, ILO Working Paper No. 144, 2025; ETUC, *Artificial Intelligence for Workers, Not Just for Profit: Ensuring Quality Jobs in the Digital Age*, Resolution adopted 4–5 March 2025, A. Aloisi, “Regulating algorithmic management at work in the European Union: data protection, non-discrimination and collective rights”, *International Journal of Comparative Labour Law and Industrial Relations*, 40(1), 2024, 37–70.



2. Artykuł 88 RODO – klauzula fakultatywnego doprecyzowania (*facultative specification clause*)⁹⁾

RODO zostało przyjęte jako instrument pełnej harmonizacji unijnego systemu ochrony danych osobowych¹⁰⁾. Jednocześnie zawiera ono przepisy przewidujące możliwość wprowadzania przez państwa członkowskie stosownych regulacji krajowych, o ile mieszczą się one w granicach wyznaczonych przez rozporządzenie i służą doprecyzowaniu jego ogólnych norm (tzw. „klauzule upoważniające”¹¹⁾). Do tej kategorii należy art. 88 RODO, dotyczący przetwarzania danych osobowych w sferze zatrudnienia. Przepis ten przyznaje państwom członkowskim kompetencje do przyjmowania „bardziej szczegółowych przepisów” w drodze ustaw oraz porozumień zbiorowych (w tym zakładowych porozumień z przedstawicielami pracowników – *vide* motyw 155 RODO) dotyczących przetwarzania danych osobowych w sferze zatrudnienia, obejmujących w szczególności warunki, na których dane osobowe w związku z zatrudnieniem można przetwarzać za zgodą pracownika do celów procedury rekrutacyjnej, wykonywania umowy o pracę (w tym wykonywania obowiązków określonych w przepisach lub w porozumieniach zbiorowych), zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

Przepisy te, co do zasady (co wynika wprost z art. 88 ust. 2 RODO), muszą jednak zapewniać ochronę godności pracownika, jego uzasadnionych interesów i podstawowych praw – w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy

⁹⁾ Szerzej: Abraha H. (2024), *Hauptpersonalrat der Lehrerinnen*: Article 88 GDPR and the Interplay between EU and Member State Employee Data Protection Rules. *Mod Law Rev.*, 87: 484-496. 9

¹⁰⁾ Art. 1 ust. 1 RODO w związku z motywami 9, 10 i 13 RODO

¹¹⁾ Zob. wyrok TSUE z dnia 30 marca 2023 r., *Hauptpersonalrat der Lehrerinnen und Lehrer*, C-34/21, EU:C:2023:270, pkt 51-52 i przytoczone tam orzecznictwo.



przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy. Stosowna swoboda regulacyjna ma zatem charakter warunkowy, tj. możliwa jest jedynie tam, gdzie towarzyszą jej adekwatne gwarancje ochronne.

Trybunał Sprawiedliwości w sprawie *Hauptpersonalrat* (C-34/21) wyraźnie podkreślił przy tym, że państwa członkowskie, korzystając z ww. kompetencji, pozostają w pełni związane celami RODO – tj. zapewnieniem wysokiego poziomu ochrony praw i wolności osób, których dotyczy takie przetwarzanie (*vide* motyw 10 RODO). Zgodnie z tym celem – art. 88 ust. 1 RODO należy interpretować szeroko: „bardziej szczegółowe przepisy”, które państwa członkowskie mogą ustanowić w celu ochrony praw pracowników w związku z zatrudnieniem, mogą dotyczyć wszystkich osób wykonujących pracę w ramach stosunku podporządkowania, niezależnie od formalnej podstawy prawnej zatrudnienia¹². TSUE wskazał, że RODO nie definiuje pojęć „pracownik” i „zatrudnienie”, dlatego należy je rozumieć w znaczeniu potocznym jako osobę wykonującą pracę pod kierownictwem innej osoby za wynagrodzeniem, co obejmuje zarówno sektor prywatny, jak i publiczny¹³.

W literaturze słusznie podkreśla się, że regulacje państw członkowskich wprowadzone w ramach art. 88 RODO nie mają charakteru *lex specialis* – tj. derogującego stosowne przepisy rozporządzenia, lecz stanowią jedynie instrument zmierzający do uszczegółowienia norm ogólnych¹⁴. W praktyce oznacza to, że art. 88 RODO nie może być wykorzystywany do modyfikowania przesłanek legalności przetwarzania określonych w art. 6 i 9 RODO ani zasad przetwarzania danych z art. 5 RODO (*tj. zgodności z prawem, rzetelności (fairness), przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, a także integralności i rozliczalności*), lecz wyłącznie do ich doprecyzowania w kontekście zatrudnienia. Co więcej, w opinii TSUE regulacje przyjmowane na podstawie art. 88

¹² *Hauptpersonalrat der Lehrerinnen und Lehrer* pkt 44–46, 53–55

¹³ *Ibidem* pkt 41–43.

¹⁴ Kotschy W., ‘The proposal for a new General Data Protection Regulation – problems solved?’ (2014) 4 *International Data Privacy Law* 274, 277



RODO muszą realnie doprecyzowywać zasady przetwarzania danych w zatrudnieniu, tj. wprowadzać treści normatywne właściwe dla regulowanej dziedziny i odrębne od przepisów ogólnych wspomnianego rozporządzenia¹⁵.

3. RODO a porozumienia zbiorowe w świetle orzecznictwa TSUE

W wyroku z 19 grudnia 2024 r. w sprawie *MK v. K GmbH* (C-65/23) Trybunał Sprawiedliwości Unii Europejskiej¹⁶ jednoznacznie stwierdził, że porozumienia zakładowe mogą stanowić podstawę prawną przetwarzania danych osobowych pracowników na podstawie art. 88 ust. 1 RODO wyłącznie wtedy, gdy zawierają szczegółowe regulacje dotyczące sposobu i celów przetwarzania, a jednocześnie spełniają wymogi ogólnych zasad ochrony danych (art. 5 RODO) oraz przesłanki legalności (w tym kryterium niezbędności) określone w art. 6 oraz 9 RODO. Trybunał odrzucił tym samym podejście, zgodnie z którym autonomia układowa mogłaby stanowić samoistne źródło legalizacji operacji przetwarzania, niezależnie od wymogu niezbędności oraz proporcjonalności wynikających z rozporządzenia. W konsekwencji – strony porozumienia zakładowego nie mogą przyjmować rozwiązań, które pomijają lub łagodzą wymogi wynikające z rozporządzenia, ani korzystać z porozumienia jako „zastępczej podstawy prawnej” dla działań, które nie spełniają warunków legalności przewidzianych w RODO¹⁷.

Trybunał podkreślił również, że – choć strony porozumień zbiorowych mogą dysponować pewnym zakresem swobody w określaniu niezbędności przetwarzania danych w rozumieniu art. 5, 6 i 9 RODO – to jednak swoboda ta podlega pełnej kontroli sądowej w celu zapewnienia zgodności ze standardami RODO. W konsekwencji, jeśli sąd krajowy rozpoznający sprawę po przeprowadzeniu kontroli stwierdzi, że niektóre

¹⁵ Zob. *Hauptpersonalrat der Lehrerinnen und Lehrer*, pkt 81.

¹⁶ Wyrok TSUE z 19 grudnia 2024 r. w sprawie C-65/23 *MK v K GmbH* ECLI:EU:C:2024:1053. Sprawa dotyczyła porozumienia zakładowego regulującego korzystanie z oprogramowania „Workday”, pozwalającego na przekazywanie danych pracowników na serwer spółki-matki w Stanach Zjednoczonych. Pracownik zakwestionował legalność przetwarzania, wskazując, że przekazywane dane obejmowały informacje niewymienione w porozumieniu. Po częściowej przegranej przed sądem pracy wniósł apelację do Federalnego Sądu Pracy, który skierował do TSUE pytania prejudycjalne dotyczące relacji pomiędzy art. 88 RODO a autonomią układową stron stosunku pracy.

¹⁷ *MK v K GmbH* pkt. 50.



postanowienia danego porozumienia zbiorowego nie spełniają warunków i ograniczeń określonych w RODO, powinien on wówczas odstąpić od stosowania tych przepisów¹⁸.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie *MK v. K GmbH* wzmacnia rolę partnerów społecznych w kształtowaniu szczegółowych gwarancji ochrony danych osobowych w środowisku pracy, przy jednoczesnym jednoznacznym podkreśleniu konieczności utrzymania wysokiego poziomu ochrony danych pracowników. Orzeczenie to potwierdza nadrzędność podstawowych zasad przetwarzania danych osobowych, wyrażonych w art. 5, 6 i 9 RODO, nad regulacjami krajowymi oraz sektorowymi, w tym nad postanowieniami układów i porozumień zbiorowych. Zgodnie z ugruntowaną linią orzecniczą TSUE – akty te nie mogą ograniczać się do ogólnych czy blankietowych odesłań do przepisów RODO, lecz powinny przekładać wynikające z nich zasady na konkretne, precyzyjne i egzekwowalne standardy odpowiadające realiom współczesnego środowiska pracy. Tym samym, aby zapewnić realną ochronę danych pracowników, konieczne jest precyzyjne określenie materialnych i proceduralnych wymogów w treści takich porozumień, tak aby abstrakcyjne normy przekładały się na weryfikowalne obowiązki po stronie pracodawcy.

Tytułem wyjaśnienia kontekstu, w jakim zapadło powyższe orzeczenie, należy wskazać, że zgodnie z art. 79 RODO każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna, iż przysługujące jej na mocy rozporządzenia prawa zostały naruszone w wyniku przetwarzania jej danych osobowych w sposób z nim niezgodny. Uprawnienie to może być realizowane niezależnie od złożenia skargi do organu nadzorczego, o którym mowa w art. 77 RODO (tj. w Polsce do Prezesa Urzędu Ochrony Danych Osobowych). Równolegle art. 82 RODO przyznaje każdej osobie fizycznej, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów rozporządzenia, prawo do dochodzenia od administratora lub podmiotu przetwarzającego stosownego odszkodowania lub zadośćuczynienia.

¹⁸ *MK v K GmbH* pkt.55-56, 59.



Trybunał Sprawiedliwości Unii Europejskiej, w wyroku z dnia 20 czerwca 2024 r. (sygn. C-590/22), wyraźnie podkreślił przy tym, że zakres zastosowania art. 82 RODO obejmuje wyłącznie naruszenia wynikające z samego rozporządzenia. W sytuacji, w której doszło także do naruszenia przepisów prawa krajowego, ewentualne rozszerzenie odpowiedzialności lub zwiększenie wysokości odszkodowania może być rozpatrywane wyłącznie na podstawie regulacji krajowych, a nie przepisów RODO¹⁹.

Co istotne: ww. postępowania mogą być prowadzone równolegle – nie istnieje obowiązek oczekiwania na rozstrzygnięcie Prezesa UODO przed wniesieniem pozwu cywilnego. W praktyce jednak decyzja organu nadzorczego potwierdzająca naruszenie przepisów RODO stanowi istotny dowód w postępowaniu cywilnym, dlatego często rekomenduje się w pierwszej kolejności wniesienie skargi do UODO, a następnie (w razie powstania szkody) skierowanie sprawy na drogę sądową.

Na tym tle należy również wyraźnie podkreślić, że Art. 22 ustawy o układach zbiorowych pracy oraz porozumieniach zbiorowych²⁰ przewidujący szczególny tryb sądowej kontroli układów zbiorowych pracy w zakresie ich zgodności z przepisami prawa pracy nie stanowi *lex specialis* wobec przepisów RODO i nie wyłącza kompetencji Prezesa Urzędu Ochrony Danych Osobowych do oceny zgodności postanowień układu zbiorowego pracy z przepisami o ochronie danych osobowych.

4. Kluczowe obszary regulacji w układach zbiorowych

4.1. Podstawy przetwarzania danych osobowych w zatrudnieniu

Układy zbiorowe pracy mogą odgrywać kluczową rolę w uszczegóławianiu oraz ograniczaniu zakresu przetwarzania danych osobowych pracowników, w szczególności poprzez minimalizowanie wykorzystania przesłanek o szerokim marginesie interpretacyjnym. Z perspektywy zgodności z zasadą legalności oraz

¹⁹ Ocena skutków wyroku TSUE z dnia 11 kwietnia 2024 roku w sprawie C-741/21 juris GmbH wydana przez Prezesa Urzędu Ochrony Danych Osobowych dnia 18 maja 2024 roku; <https://uodo.gov.pl/pl/138/3116> :

²⁰ Ustawa z 5.11.2025 r. o układach zbiorowych pracy i porozumieniach zbiorowych (Dz.U. z 2025 r. poz. 1661),



zasadą minimalizacji danych – regulacje autonomiczne powinny dążyć do oparcia przetwarzania danych na przesłankach ściśle związanych z realizacją stosunku pracy, w szczególności na niezbędności przetwarzania do wykonania umowy o pracę (art. 6 ust. 1 lit. b RODO) oraz na wypełnianiu obowiązków prawnych ciążących na pracodawcy (art. 6 ust. 1 lit. c RODO). Równocześnie układy te powinny w sposób wyraźny limitować możliwość odwoływania się do przesłanki ‘prawnie uzasadnionego interesu pracodawcy’ (art. 6 ust. 1 lit. f RODO), która w praktyce jest szczególnie podatna na nadużycia.

W zakresie stosowania art. 6 ust. 1 lit. f RODO podkreślenia wymaga, że – zgodnie ze stanowiskiem Grupy Roboczej Art. 29 – przesłanka ta wymaga istnienia „rzeczywistego i aktualnego interesu”, odpowiadającego bieżącej działalności administratora lub korzyściom spodziewanym w dającej się przewidzieć przyszłości²¹. W konsekwencji przetwarzanie danych oparte na prawnie uzasadnionym interesie pracodawcy, który nie jest dostatecznie skonkretyzowany lub zindywidualizowany (w szczególności gdy opiera się jedynie na ogólnych obawach, spekulatywnych zagrożeniach bądź marginalnym ryzyku), nie może zostać uznane za podstawę prawną przetwarzania danych²².

Co więcej, zgodnie z motywem 47 RODO, w praktyce interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, mogą przeważać nad interesami administratora – zwłaszcza w przypadkach, w których osoba ta nie ma rozsądnych podstaw, by oczekiwać przetwarzania jej danych w określonym celu. Motyw ten (nota bene analogicznie do utrwalonej linii orzeczniczej ETPCz odnośnie art. 8 EKPCz) nakłada zatem na pracodawcę obowiązek uwzględnienia ‘rozsądnych oczekiwań’ pracownika, wynikających z charakteru łączącego strony stosunku prawnego. W realiach stosunku pracy, w którym pracownik zajmuje pozycję strukturalnie słabszą, standard oceny zgodności przetwarzania danych z przesłanką uzasadnionego interesu powinien być stosowany z uwzględnieniem szczególnej ochrony praw pracownika wynikającej

²¹ Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN, WP217, p. 24.

²² Otto M., The Right to Privacy in Employment. A Comparative Analysis (Hart Publishing, 2016), 189.



z prawa pracy oraz prawa ochrony danych. Dla przykładu: wykorzystywanie narzędzi takich jak systemy monitorujące wykorzystanie czasu pracy przez pracowników zdalnych może co do zasady służyć prawnie uzasadnionym interesom pracodawcy. Realizacja tych interesów musi jednak następować w sposób proporcjonalny oraz adekwatny do ryzyka naruszenia praw podstawowych pracownika, w szczególności prawa do prywatności i ochrony danych osobowych.

Granice dopuszczalności powoływania się na prawnie uzasadniony interes w kontekście pracy zdalnej zostały wyraźnie określone w decyzji francuskiego organu ochrony danych (*Commission Nationale de l'Informatique et des Libertés-CNIL*) z 19 grudnia 2024 r. W sprawie tej ukarano agencję nieruchomości za stosowanie narzędzia *Time Doctor*, instalowanego zarówno na urządzeniach służbowych, jak i prywatnych pracowników. Oprogramowanie to monitorowało aktywność klawiatury i myszy, wykonywało cykliczne zrzuty ekranu, rejestrowało odwiedzane strony internetowe oraz klasyfikowało je jako „produktywne” lub „nieproduktywne”. Uzyskane dane wykorzystywano między innymi do odliczania przerw oraz obniżania wynagrodzenia za okresy uznane za ‘nieaktywne’.

CNIL uznał, że tego rodzaju monitoring naruszał zasadę minimalizacji danych określoną w art. 5 ust. 1 lit. c RODO, a stopień intensywności i ciągłość nadzoru nie były ani niezbędne, ani proporcjonalne w stosunku do deklarowanych celów pracodawcy. Co istotne: organ stwierdził również, że pracodawca nie mógł opierać przetwarzania na przesłance prawnie uzasadnionego interesu, gdyż praktyka ta naruszała ‘rozsądne oczekiwania pracowników’ co do dopuszczalnych granic nadzoru. Zgodnie bowiem z art. L3121-1 francuskiego Kodeksu pracy – podobnie jak w prawie polskim – czas pracy oznacza pozostawanie do dyspozycji pracodawcy i wykonywanie jego poleceń, a nie stałą aktywność mierzoną bodźcami fizycznymi, takimi jak ruchy myszy lub wprowadzanie tekstu²³.

²³ Délibération SAN-2024-021 du 19 décembre 2024
<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000051120331>.



Podsumowując – konstrukcja podstaw prawnych przetwarzania w układach zbiorowych musi być powiązana ze szczegółowymi gwarancjami zarówno materialnymi, jak i proceduralnymi. Układy zbiorowe pracy powinny ograniczać możliwość odwoływania się do przesłanki prawnie uzasadnionego interesu pracodawcy w tych obszarach przetwarzania, które wiążą się z podwyższonym ryzykiem naruszenia praw lub wolności pracowników – w szczególności w przypadku automatycznych systemów monitorujących i podejmujących decyzje (tj. zarządzania algorytmicznego) lub przekazywania danych do państw trzecich spoza EOG.

4.2. Zgoda pracownika i możliwość jej kolektywizacji/wzmocnienia w kontekście ochrony danych w zatrudnieniu

Zgoda pracownika jako podstawa prawna przetwarzania danych osobowych w rozumieniu RODO od lat postrzegana jest jako konstrukcja wątpliwa, a w wielu przypadkach wręcz nieadekwatna. Wynika to z inherentnej nierównowagi negocjacyjnej pomiędzy pracodawcą a pracownikiem, która podważa dobrowolność oświadczenia woli po stronie pracownika. Stosownie do motywu 42 RODO – wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji. Pracownik funkcjonujący w relacji podporządkowania może zatem racjonalnie zakładać, że odmowa zgody lub jej wycofanie pociągnie za sobą negatywne konsekwencje, zarówno formalne, jak i nieformalne. W takim układzie zgoda kreuje jedynie fikcję autonomii informacyjnej, co przyznaje również prawodawca unijny – wskazując, że zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem (motyw 43 RODO).

Ustawodawca krajowy przyjmuje wobec zgody pracownika podejście wyraźnie ograniczające. Zgodnie z art. Art. 22^{1a} k.p. – zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez



pracodawcę innych danych osobowych niż wymienione w art. 22¹ § 1 i 3 k.p., zarówno w przypadku danych osobowych udostępnianych przez osobę ubiegającą się o zatrudnienie lub pracownika na wniosek pracodawcy lub przekazanych pracodawcy z inicjatywy ww. osób. Co do zasady: brak zgody lub jej wycofanie nie może jednak skutkować niekorzystnym traktowaniem ani negatywnymi konsekwencjami dla kandydata lub pracownika. Z kolei Art. 22^{1b} k.p. dopuszcza możliwość oparcia przetwarzania przez pracodawcę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, na zgodzie osoby ubiegającej się o zatrudnienie lub pracownika jedynie wyjątkowo – tj. wyłącznie w sytuacji, gdy przekazanie tych danych następuje z inicjatywy tej osoby. Rozwiązanie to potwierdza, że zgoda w relacji zatrudnienia nie jest traktowana jako równorzędna i pełnowartościowa podstawa legalizująca przetwarzanie danych, lecz jako konstrukcja wymagająca dodatkowych gwarancji, mających zminimalizować ryzyko jej ‘wymuszenia’ w warunkach podporządkowania pracowniczego.

Układy zbiorowe mogą w praktyce odgrywać istotną rolę w doprecyzowywaniu warunków, które gwarantują, że zgoda pracownika ma charakter dobrowolny i świadomy, a także w wyznaczaniu obszarów, w których stosowanie indywidualnej zgody powinno być całkowicie wyłączone (jako wykraczające poza tzw. ‘rozsądne oczekiwania pracowników’ co do przetwarzania danych osobowych w zatrudnieniu). Dotyczy to w szczególności wdrażania systemów zarządzania algorytmicznego, których funkcjonowanie, logika i cele są dla pracowników zazwyczaj nieprzejryste, a jednocześnie trudno sprzeciwić się ich stosowaniu (art. 21 RODO) (*vide* w szczególności osoby wykonujące pracę za pośrednictwem platform cyfrowych (motyw 39 Dyrektywy platformowej)).

W literaturze przedmiotu słusznie zauważa się przy tym, że nowoczesne systemy nadzoru działają zarówno w sposób wertykalny, jak i horyzontalny: z jednej strony indywidualnie monitorują pracownika, z drugiej zaś klasyfikują, agregują i porównują dane zbiorcze w celu konstruowania wzorców, benchmarków oraz wskaźników ryzyka. W konsekwencji dane jednej osoby mogą wpływać na modele predykcyjne stosowane



wobec innych – co sprawia, że skutki przetwarzania mają charakter relacyjny, grupowy i rozproszony²⁴. W tym ujęciu pojawia się kategoria *shared vulnerabilities*, rozumiana jako wspólna podatność grupy pracowniczej (wrażliwych podmiotów danych - *vulnerable data subjects* -vide motyw 75 RODO) wynikająca z faktu, że przetwarzanie danych jednego pracownika generuje efekty oddziałujące na całą zbiorowość. Zjawiska te nie mogą być skutecznie adresowane jedynie poprzez indywidualne prawa jednostki, ponieważ naruszenia mają charakter kolektywny – ingerują bowiem w zbiorową autonomię pracowniczą, strukturę stosunków władzy w miejscu pracy oraz możliwości negocjowania warunków zatrudnienia. Poniższe dwa praktyczne przykłady dobrze ilustrują ww. problem:

- Algorytmiczny scoring zespołu:

W praktyce organizacyjnej coraz częściej stosowane są systemy zarządzania wydajnością pracy, które generują zbiorcze wskaźniki efektywności zespołów (np. średni czas odpowiedzi na zapytania, tempo realizacji zadań czy poziom zgodności z procedurami), obliczane na podstawie danych jednostkowych wszystkich członków grupy. Dane pojedynczego pracownika (nawet incydentalne) wpływają bezpośrednio na wynik całego zespołu, który następnie stanowi podstawę decyzji dotyczących premii, grafiku pracy czy dalszego monitoringu. W efekcie każdy pracownik staje się współodpowiedzialny za wynik algorytmiczny generowany z danych innych osób. Indywidualna zgoda na przetwarzanie danych nie obejmuje zatem relacyjnego i kolektywnego wymiaru skutków takiego systemu.

- Modele predykcyjne absencji:

W ramach zaawansowanej analityki HR stosowane są modele predykcyjne, które na podstawie historycznych danych dotyczących absencji całej populacji pracowników (np. częstotliwości krótkoterminowych zwolnień lekarskich, wzorców nieobecności w określonych okresach roku lub w konkretnych zespołach) tworzą statystyczne profile „pracowników podwyższonego ryzyka absencji”. Dopasowanie konkretnej osoby do takiego profilu może skutkować negatywnymi konsekwencjami decyzyjnymi – takimi jak pominięcie przy awansie, ograniczenie dostępu do szkoleń – nawet jeśli indywidualne zachowania tej osoby nie uzasadniają takich działań. Decyzja wobec

²⁴ Viljoen S., ‘A Relational Theory of Data Governance’ (2021) Yale Law Journal 131/2, 573-653.



jednostki jest w tym przypadku pochodną wzorców wyodrębnionych z danych całej grupy pracowniczej²⁵.

W tym kontekście zasadne staje się rozważenie kolektywnych modeli zgody negocjowanych i egzekwowanych na poziomie układów zbiorowych. Mechanizm ten polegałby przede wszystkim na wzmocnieniu przesłanki zgody poprzez proceduralne gwarancje wypracowane przez reprezentację pracowników, uwzględniające rzeczywiste interesy oraz zagrożenia o charakterze grupowym. Tego rodzaju zgoda stwarzałaby nie tylko realną przeciwwagę dla sytuacji, w których indywidualna zgoda powinna być uznana za prawnie niedopuszczalną z uwagi na nieusuwalną asymetrię negocjacyjną stron, ale również realną możliwość odmowy zgody na operacje przetwarzania danych osobowych (bez negatywnych konsekwencji-działań odwetowych ze strony pracodawcy). Z drugiej strony zasadne wydaje się zastąpienie, w określonych sytuacjach, zgody indywidualnej zgodą kolektywną, a konkretniej przekształcenie ‘rozsądnych oczekiwań pracowników’ w ‘oczekiwania normatywne’/wiążące standardy’ doprecyzowane w układzie zbiorowych, których nie można wyłączyć w drodze indywidualnej zgody pracownika. Z perspektywy zgodności z RODO mechanizm kolektywnej zgody musiałby jednak spełniać szereg kryteriów materialnych i proceduralnych, w tym: wyraźne określenie celów przetwarzania dla którego stosowna zgoda została udzielona, ograniczenia dalszego wykorzystania danych, gwarancje wycofania zgody bez negatywnych konsekwencji, obowiązek konsultacji z reprezentacją pracowników przy zmianie celu przetwarzania.

Podsumowując: w obliczu postępującej cyfryzacji środowiska pracy przetwarzanie danych pracowników nie dotyczy już jednostek w izolacji. Współczesne ramy prawne ochrony danych osobowych w zatrudnieniu muszą zatem uwzględniać perspektywę zbiorową, a nie wyłącznie indywidualistyczną. Kolektywizacja zgody, oparta na koncepcji ‘*shared vulnerabilities*’, stanowi krok w kierunku rzeczywistego zrównoważenia przewagi negocjacyjnej i informacyjnej pracodawcy, przekształcając

²⁵ Szerzej: Nath, Gopal & Harfouche, Antoine & Coursey, Austin & Saha, Krishna & Prabhu, Srikanth & Sengupta, Saptarshi. (2022). Integration of a machine learning model into a decision support tool to predict absenteeism at work of prospective employees.



RODO z instrumentu formalnej jedynie zgodności w narzędzie negocjowania szeroko rozumianych warunków pracy (‘rozsądnych oczekiwań co do ochrony prywatności i danych osobowych) w cyfrowym środowisku pracy.

4.3. Zagwarantowanie udziału związków zawodowych w ocenę skutków dla ochrony danych

Zgodnie z art. 35 RODO pracodawca ma obowiązek przeprowadzenia oceny skutków dla ochrony danych (*data protection impact assessment* – DPIA) w przypadku operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Co do zasady – ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może m.in. wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

- jeżeli przetwarzanie może poskutkować dyskryminacją, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową;
- jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
- jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych²⁶;
- jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa;
- jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej,

²⁶ Zob. Wyrok TSUE z dnia 1 sierpnia 2022 r. OT/Vyriausioji tarnybinės etikos komisija (Sprawa C-184/20). W opinii TSUE, jeżeli można wyciągnąć wnioski dotyczące danych szczególnej kategorii „w wyniku operacji intelektualnej polegającej na dedukcji lub łączeniu informacji”, mogą one być uznane za dane szczególnej kategorii w rozumieniu artykułu 9 RODO.



zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą (motyw 75 RODO).

Co istotne: prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych (motyw 76 RODO).

Art. 35 ust. 3 RODO podaje przykłady operacji przetwarzania, które mogą powodować wysokie ryzyko dla praw i wolności osób fizycznych. Zgodnie z nim ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku:

- a. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się 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;
- b. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
- c. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Systematyczny monitoring pracowników (zwłaszcza przy użyciu zaawansowanych technologii) czy przetwarzanie danych osobowych za pomocą zautomatyzowanych systemów monitorujących lub zautomatyzowanych systemów decyzyjnych (w Polsce nadal stosowane głównie przez cyfrowe platformy pracy) powszechnie uznawane są przy tym za operacje obarczone wysokim ryzykiem, co w praktyce czyni DPIA niemal obowiązkowym przy wdrażaniu nowych systemów nadzoru w miejscu pracy²⁷.

²⁷ Zob. KOMUNIKAT PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony. Wykaz uzupełnia i konkretyzuje wytyczne Grupy Roboczej Art. 29 (WP 248)



Europejska Rada Ochrony Danych (EROD) zaleca jednak, aby – w razie wątpliwości, czy ocena skutków dla ochrony danych jest obowiązkowa – ją przeprowadzić.²⁸ Jak wskazuje UODO, „jest to bowiem instrument, który ułatwia administratorom przestrzeganie przepisów o ochronie danych osobowych. Wdrożenie skutecznej procedury oceny skutków dla ochrony danych pozwala nie tylko minimalizować ryzyka, ale także budować zaufanie osób, których dane są przetwarzane (m.in. może pozwolić na ocenę środków ułatwiających tym osobom korzystanie ze swoich praw, czy też ocenę zapewnienia przejrzystości przetwarzania danych osobowych). Z tego względu korzystne dla administratora może być przeprowadzenie oceny skutków dla ochrony danych również wtedy, gdy nie jest ona obowiązkowa (dobrowolna ocena skutków dla ochrony danych)”²⁹.

W tym kontekście warto zauważyć, że Art. 35 ust. 9 RODO nakłada na pracodawcę obowiązek zasięgnięcia opinii przedstawicieli pracowników jedynie „w stosownych przypadkach”, co pozostawia szerokie pole do interpretacji i może prowadzić do marginalizacji udziału pracowników w procesie DPIA. W tym świetle szczególnego znaczenia nabiera art. 8 tzw. dyrektywy platformowej³⁰, który doprecyzowuje, że przetwarzanie danych osobowych przy użyciu zautomatyzowanych systemów monitorujących lub decyzyjnych z dużym prawdopodobieństwem powoduje wysokie ryzyko w rozumieniu art. 35 ust. 1 RODO, a tym samym wymaga obligatoryjnego zasięgnięcia opinii osób wykonujących pracę za pośrednictwem platform oraz ich przedstawicieli. Dyrektywa nakłada również obowiązek przedstawienia wyników oceny skutków dla ochrony danych reprezentacji pracowników.

„Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679”, które 25.05.2018 r. zostały zatwierdzone przez Europejską Radę Ochrony Danych (EROD); https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en.

²⁸ Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679, s. 9

²⁹ <https://uodo.gov.pl/pl/598/3617>

³⁰ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2831 z dnia 23 października 2024 r. w sprawie poprawy warunków pracy za pośrednictwem platform.



Konsultacja z przedstawicielami pracowników nie powinna jednak mieć charakteru incydentalnego. Kluczowe zatem wydaje się wynegocjowanie w układach zbiorowych mechanizmu obowiązkowego i systematycznego włączania związków zawodowych w cały cykl DPIA odnośnie do operacji przetwarzania przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Taki mechanizm docelowo powinien obejmować:

1. Konsultacje przed rozpoczęciem DPIA: Związki zawodowe powinny mieć możliwość wpływu na zidentyfikowanie obszarów ryzyka przed przeprowadzeniem stosownej analizy (np. mogą wskazywać konkretne formy monitoringu lub profilowania, które ich zdaniem wymagają uwagi, współtworząc tym samym matrycę ryzyka).
2. Opiniowanie DPIA: związki zawodowe powinny weryfikować, czy DPIA przeprowadzona przez pracodawcę:
 - Zawiera opis planowanego przetwarzania danych oraz uzasadnienie jego realizacji;
 - Wskazuje podstawę prawną przetwarzania danych;
 - Dokonuje oceny niezbędności przetwarzania danych w odniesieniu do jego celów, przy założeniu gromadzenia wyłącznie danych minimalnych;
 - Identyfikuje oraz ocenia ryzyka dla danych osobowych osób, których operacje dotyczą;
 - Wskazuje środki służące ograniczeniu ryzyka i zapewnieniu zgodności z przepisami, obejmujące odpowiednie zabezpieczenia techniczne i organizacyjne.
3. Wspólną identyfikację środków zaradczych: związki zawodowe powinny współuczestniczyć w definiowaniu technicznych i organizacyjnych zabezpieczeń (np. anonimizacja, minimalizacja danych, ograniczenie dostępu, okres retencji) – co pozwala na lepsze dostosowanie działań do realnych potrzeb/'rozsądnych oczekiwań pracowników'.
4. Stały przegląd i aktualizację DPIA: W miarę zmian w systemach przetwarzania (np. wprowadzenie nowych narzędzi monitoringu czy ich integracja do systemów automatycznego nadzoru) związki zawodowe powinny być włączane do ponownej



analizy ryzyka i środków zaradczych. Dzięki temu ocena skutków nie będzie jednorazowym raportem, lecz żywym dokumentem dostosowującym się do potencjalnie dynamicznie zmieniających się realiów pracy.

4.4. Konkretyzacja praw podmiotów danych/pracowników

Skuteczna ochrona danych osobowych pracowników wymaga nie tylko istnienia ogólnych norm prawnych, lecz także przekształcenia ich w mechanizmy możliwe do praktycznego zastosowania w zakładzie pracy. Zgodnie z art. 12 ust. 2 RODO, pracodawca ma obowiązek ułatwiania pracownikom wykonywania ich praw wynikających z przetwarzania danych osobowych przysługujących im na mocy art. 15–22 RODO. Układy zbiorowe mogą odegrać w tym procesie kluczową rolę, operacjonalizując ogólne prawa wynikające z RODO i nadając im formę jasnych, egzekwowalnych standardów działania.

Krajowe przepisy oraz układy zbiorowe, w myśl art. 88 ust. 2 RODO, mogą określać szczegółowe środki realizacji tego obowiązku, ze szczególnym uwzględnieniem przejrzystości przetwarzania w kontekście zatrudnienia. W praktyce chodzić może m.in. o:

- przygotowanie jasnych instrukcji krok po kroku dotyczących składania wniosków o dostęp do danych, sprostowanie, usunięcie lub ograniczenie przetwarzania;
- wskazanie dedykowanych osób kontaktowych, które udzielają wsparcia i odpowiadają na pytania pracowników w sprawach związanych z przetwarzaniem danych;
- regularne informowanie pracowników o ich prawach oraz sposobie ich realizacji, np. w ramach szkoleń lub komunikacji wewnętrznej.

4.4.1. Prawo do informacji

Przejrzystość jest jedną z podstawowych zasad RODO. Art. 88 ust. 2 wyraźnie wskazuje, że krajowe regulacje oraz układy zbiorowe powinny kłaść na nią szczególny



nacisk. W praktyce prawo do informacji często bywa realizowane w sposób fasadowy: informacje są dostarczane fragmentarycznie, w sposób niezrozumiały lub w formie zbyt technicznej, co uniemożliwia realną kontrolę nad przetwarzaniem danych. Układy zbiorowe mogą przeciwdziałać temu poprzez doprecyzowanie co najmniej niżej wymienionych obszarów:

1. Ramy czasowe

Informowanie powinno odbywać się w następujących etapach:

- na etapie rekrutacji,
- przy zawieraniu umowy o pracę,
- w trakcie zatrudnienia, zwłaszcza przy wdrażaniu nowych technologii i zmianach procesów przetwarzania.

Układy zbiorowe mogą określić konkretne terminy (np. min. 30 dni przed wdrożeniem konkretnego systemu).

2. Zakres i sposób przekazywania informacji

RODO nakłada na administratora obowiązek przekazania m.in. informacji o „logice” stojącej za zautomatyzowanym podejmowaniem decyzji. Układy zbiorowe mogą doprecyzować, jakie informacje są w kontekście zatrudnienia rzeczywiście istotne, aby zapobiec praktyce udzielania ogólnikowych lub technicznie hermetycznych wyjaśnień, które faktycznie uniemożliwiają zrozumienie zasad działania algorytmów. Układy zbiorowe mogą przeciwdziałać takim praktykom, wymagając udostępniania informacji w formie zrozumiałych raportów czy opisowych streszczeń zamiast surowych plików danych.

4.4.2 Prawo dostępu

Prawo dostępu, przewidziane w art. 15 RODO, umożliwia osobie, której dane dotyczą, weryfikację legalności i rzetelności przetwarzania jej danych osobowych. Zgodnie z motywem 63 RODO – każda osoba, której dane dotyczą, powinna mieć prawo do pełnej wiedzy i informacji; w szczególności w zakresie:

- celów przetwarzania danych osobowych,
- planowanego okresu, przez jaki dane będą przetwarzane,



- odbiorców danych,
- założeń ewentualnego zautomatyzowanego przetwarzania danych,
- konsekwencji przetwarzania w przypadku profilowania.

W kontekście zatrudnienia – skuteczność prawa dostępu bywa jednak ograniczana przez pracodawców, którzy powołują się m.in. na ochronę tajemnicy przedsiębiorstwa, bezpieczeństwo systemów IT czy „nadmierny charakter” żądań (art.12 ust. 5 RODO). Układy zbiorowe mogą dodatkowo wzmocnić skuteczność prawa dostępu poprzez m.in. wskazanie kategorii informacji, które nie mogą być traktowane jako tajemnica przedsiębiorstwa w kontekście danych pracowniczych – takich jak np. historia logowań, dane o produktywności czy decyzje algorytmiczne.

4.5. Zarządzanie algorytmiczne – wyzwania i luki regulacyjne

Zarządzanie algorytmiczne stanowi jedno z kluczowych współcześnie wyzwań regulacyjnych w kontekście zatrudnienia, w szczególności w świetle dostrzegalnego braku interoperacyjności regulacyjnej (*regulatory interoperability*), tj. niewystarczającej koordynacji pomiędzy stosownymi standardami prawnymi Unii Europejskiej, regulacjami krajowymi oraz normami sektorowymi³¹.

W praktyce żaden z obowiązujących obecnie aktów prawnych nie zapewnia całościowej ani systemowej odpowiedzi na ryzyka wynikające z wykorzystania systemów algorytmicznych w środowisku pracy. Na poziomie ponadnarodowym ogólne rozporządzenie o ochronie danych (RODO) ustanawia technologicznie neutralny zestaw standardów prawnych, których celem jest zapewnienie wysokiego poziomu ochrony praw podstawowych osób, których dane dotyczą przy jednoczesnym zagwarantowaniu swobody przepływu danych w UE (art.1 RODO).

³¹ Zob. Otto M., The rise of algorithmic surveillance: legal and ethical implications for the future of work, [w:] M.Biasi AI & Labour Law (Routledge, 2026).



Dyrektywa platformowa, poprzez wprowadzenie bardziej szczegółowych regulacji dotyczących zautomatyzowanych systemów monitorowania i podejmowania decyzji (w tym zakazów przetwarzania określonych kategorii danych; np. dotyczących stanu emocjonalnego czy psychicznego) oraz wzmocnienie prawa do informacji i konsultacji pracowników platformowych i ich przedstawicieli, w większym stopniu odpowiada na strukturalne asymetrie władzy i informacji charakterystyczne dla gospodarki platformowej. Niemniej jednak, w świetle potencjalnie ograniczonej implementacji przez państwa członkowskie, rodzi ona realne ryzyko dalszej fragmentaryzacji regulacyjnej w UE. W praktyce zawężona (jedynie sektorowa) transpozycja mogłaby prowadzić do utrwalenia znaczących różnic w poziomie ochrony praw podstawowych między pracownikami platformowymi, a pracownikami zatrudnionymi w tradycyjnych sektorach czy branżach – mimo że wszystkie grupy są coraz częściej poddawane porównywalnym formom algorytmicznego nadzoru i kontroli³².

Co istotne: z uwagi na utrzymujący się brak krajowych inicjatyw regulacyjnych w zakresie zarządzania algorytmicznego³³ - nadal otwarte pozostaje pytanie, w jakim stopniu ustawodawstwa państw członkowskich będą zdolne przeciwdziałać niejako immanentnym dla ww. technologii zjawiskom *surveillance creep* (tj. łączeniu rozproszonych narzędzi nadzoru w zintegrowane systemy algorytmiczne) oraz *data creep* (tj. rozszerzaniu zakresu przetwarzania danych pierwotnie zebranych w określonym celu na nowe, często nieprzewidziane pierwotnie cele).

Co do zasady: na gruncie RODO, aby ustalić, czy cel dalszego przetwarzania danych osobowych jest zgodny z celem, w którym dane te zostały pierwotnie zebrane, pracodawca – po spełnieniu wszystkich wymogów warunkujących zgodność pierwotnego przetwarzania z prawem – powinien uwzględnić między innymi:

³² FEPS Europe Policy Study (2024), Algorithmic management in traditional workplaces, Case studies on the impact of algorithmic technologies in seven sectors in the Nordics, : <https://feps-europe.eu/publication/algorithmic-management-in-traditional-workplaces/>

³³ Zob. Hendrickx, F., Mangan D., Gramano E., *Privacy@work: a European and Comparative Perspective* (Kluwer Law International, The Netherlands); Eurofound, ‘Regulatory responses to algorithmic management in the EU, (2024).



- wszelkie powiązania pomiędzy tymi celami a celami zamierzonego dalszego przetwarzania;
- kontekst, w którym dane osobowe zostały zebrane, w szczególności rozsądne przesłanki pozwalające osobom, których dane dotyczą, oczekiwać dalszego wykorzystania danych oparte na rodzaju ich powiązania z administratorem;
- charakter danych osobowych;
- konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; oraz
- istnienie odpowiednich zabezpieczeń – zarówno podczas pierwotnej, jak i zamierzonej operacji dalszego przetwarzania.

W konsekwencji – uwzględniając w szczególności specyfikę kontekstu zatrudnienia (obejmującą m.in. strukturalną nierównowagę sił między osobą, której dane dotyczą, a administratorem, oraz „rozsądne oczekiwania prywatności” ukształtowane w orzecznictwie ETPCz na gruncie art. 8 EKPC (art. 6 ust. 4 lit. b RODO)), jak również potencjalne konsekwencje dalszego przetwarzania dla pracowników i ochrony ich praw podstawowych (art. 6 ust. 4 lit. d RODO) – nie można automatycznie uznać, że integracja systemów nadzoru lub rozszerzanie ich funkcji poza pierwotnie przewidziany cel jest zgodna z prawem wyłącznie z uwagi na legalność pierwotnych operacji przetwarzania (np. monitoringu, w tym monitoringu algorytmicznego-*vide* ‘inne formy monitoringu’ art. 22^{3§} 4k.p.)

W praktyce, aby skutecznie przeciwdziałać powyższemu zjawiskom, konieczne jest zatem nadanie zasadzie ograniczenia celu (art. 5 ust. 1 lit. b RODO) realnego/materialnoprawnego znaczenia. Na obecnym etapie, w większości państw członkowskich, w tym w Polsce (*vide* art. 22^{2§} 1 i 4, art. 22^{3§} 1-4), zasada ta zdaje się być niejako konsumowana przez szerszą zasadę zgodności z prawem. W efekcie istnienie ryzyko, że w przypadku wdrożenia automatycznych systemów monitorujących i decyzyjnych istnienie szeroko zdefiniowanego, prawnie uzasadnionego interesu po stronie pracodawcy (*vide* 22^{3§} 4 – ‘inne formy monitoringu’) – zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz



właściwego użytkowania udostępnionych pracownikowi narzędzi pracy będzie traktowane jako wystarczające uzasadnienie dla rozszerzenia zakresu dotychczasowego nadzoru ponad pierwotnie przewidziany cel.

W konsekwencji, wydaje się zatem zasadne dalsze doprecyzowanie w układach zbiorowych pracy zasady ograniczenia celu, w tym przede wszystkim przesłanek warunkujących kompatybilność dalszego przetwarzania z pierwotnym celem, a także wprowadzenie mechanizmu zgody kolektywnej na rozszerzenie celu przetwarzania danych osobowych poza pierwotnie przewidziany. Rozwiązania te umożliwiłyby funkcjonowanie ww. standardów RODO nie jako formalnych mechanizmów zgodności, lecz jako realnych instrumentów materialnoprawnych służących równoważeniu dynamicznej ekspansji algorytmów w miejscu pracy.

5. Przetwarzanie danych osobowych przez związki zawodowe

Działalność związkowa nierozzerwalnie wiąże się z przetwarzaniem danych osobowych, w tym danych szczególnej kategorii – takich jak informacje o przynależności związkowej (art. 9 RODO). Dla zapewnienia zgodności z RODO kluczowe znaczenie ma prawidłowe zidentyfikowanie administratora danych oraz podstawy prawnej dla każdego z tych procesów.

5.1. Związki zawodowe jako administratorzy danych

Poszczególne jednostki organizacyjne związku zawodowego – takie jak organizacje zakładowe, międzyzakładowe – mogą być administratorami danych. Zgodnie z art. 13 pkt 7 ustawy o związkach zawodowych (dalej: u.z.z), statut związku określa co prawda, które z jego jednostek organizacyjnych posiadają osobowość prawną. Niemniej jednak, na gruncie rozporządzenia ogólnego brak osobowości prawnej danej struktury związkowej, nie wyklucza jej statusu jako administratora danych. Zgodnie z utrwalonym stanowiskiem – decydująca jest faktyczna decyzyjność w zakresie celów i sposobów przetwarzania danych (art. 4 pkt 7 RODO)³⁴. Innymi słowy: jednostki

³⁴ Cf. The Opinion of the Working Party on the Protection of Individuals with Regard to the Processing of



organizacyjne związków zawodowych, które nie posiadają osobowości prawnej, mogą być uznane za administratorów, jeśli faktycznie decydują o celach i sposobach przetwarzania danych.

W praktyce, w zależności od konkretnej procedury, administratorem będzie ta jednostka organizacyjna związku, której przepisy ustawowe czy układy zbiorowe przyznają kompetencje do działania w danej sprawie. W przeważającej większości przypadków, w odniesieniu do indywidualnych spraw pracowniczych, podmiotem tym będzie zakładowa organizacja związkowa.

Należy przy tym pamiętać, że zastosowanie konstrukcji ‘współadministrowania’ danymi między różnymi szczeblami organizacji związkowych, zgodnie z art. 26 RODO, wymaga określenia w sposób przejrzysty odpowiednich zakresów swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz obowiązków informacyjnych administratorów danych³⁵. Co równie ważne – zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą. W praktyce brak ww. formalnych, jasnych uzgodnień czyni konstrukcję współadministrowania iluzoryczną i niezgodną z przepisami RODO.

5.2 Podstawy prawne przetwarzania danych osobowych przez związki zawodowe

- **Współpraca między pracodawcą a związkiem zawodowym w indywidualnych sprawach pracowniczych³⁶**

Personal Data on the Concepts of “Controller” and “Processor”, adopted on 16 February 2010, 00264/10/PL, WP 169.

³⁵ Cf. Motyw 79 RODO: Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna, administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami.

³⁶ Szerzej: Pisarczyk Ł., Miętek, A. (2021). Personal data processing within the framework of cooperation between the employer and the trade union in individual employment matters. *Krytyka Prawa. Niezależne Studia Nad Prawem*, 13(2), 178–194.



Przepisy prawa pracy przewidują współdziałanie pracodawcy z zakładową organizacją związkową w indywidualnych sprawach ze stosunku pracy. Pracodawca ma obowiązek współdziałać w takich sprawach z zakładową organizacją związkową reprezentującą pracownika z tytułu jego członkostwa w związku zawodowym albo wyrażenia zgody na obronę praw pracownika niezrzeszonego w związku (art.7 u.z.z.)

Zgodnie z art. 30 ust. 3 u.z.z. pracodawca – zanim podejmie działanie w indywidualnej sprawie, w której prawo pracy nakłada na niego obowiązek współdziałania z zakładową organizacją związkową – musi zwrócić się do tej organizacji z zapytaniem, czy dany pracownik korzysta z jej ochrony. Informacja o członkostwie jest przy tym zbędna z perspektywy celu, jakim jest ustalenie, czy pracodawca ma obowiązek skonsultować swoje działania ze związkiem. Po potwierdzeniu, że pracownik jest reprezentowany przez związek, pracodawca przekazuje dane niezbędne do zajęcia stanowiska w konkretnej sprawie. Zakres tych danych zależy od charakteru stosownej procedury konsultacyjnej.

Co istotne, dane osobowe są definiowane szeroko na gruncie RODO i oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej – tj. takiej, którą można zidentyfikować, bezpośrednio lub pośrednio, w szczególności na podstawie [przykładowo wskazanych] identyfikatorów (imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego lub jednego bądź kilku czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej) (Art.4 pkt.1 RODO).

Zgodnie z opinią Grupy Roboczej Art.29 (tj. poprzednikiem EROD – Europejskiej Rady Ochrony Danych) pojęcie danych osobowych obejmuje zarówno informacje „obiektywne”, które można zweryfikować lub sprostować, jak i informacje „subiektywne” (opinie lub oceny), które stanowią kluczową kategorię danych osobowych przetwarzanych w kontekście zatrudnienia³⁷.

³⁷ Working Party Opinion 4/2007 on the concept of personal data, 01248/07/EN/WP136, 6.



Aby uznać dane za „dotyczące” określonej osoby fizycznej, należy jednak wykazać występowanie elementu „treści” („informacja dotyczy danej osoby”), elementu „celu” („dane są wykorzystywane lub mogą być wykorzystywane w celu oceny, traktowania w określony sposób lub wpływania na status bądź zachowanie osoby”) lub elementu „skutku” („wykorzystanie danych może mieć wpływ na prawa i interesy określonej osoby”)³⁸.

W związku z tym, co do zasady, elementy wykorzystywane przy podejmowaniu decyzji dotyczących np. awansu pracownika, podwyżki wynagrodzenia lub przydzielenia nowych zadań (takie jak coroczne oceny okresowe, dokumenty dotyczące postępowań dyscyplinarnych, wnioski szkoleniowe, rankingi, itp) stanowią dane osobowe dotyczące tego pracownika³⁹.

Rodzaj Przetwarzanych Danych

Przykładowe Procedury Konsultacyjne

Dane dotyczące nienależytego wykonywania pracy lub zachowania

Konsultacja zamiaru wypowiedzenia umowy o pracę (art. 38 KP), zamiaru rozwiązania umowy bez wypowiedzenia z winy pracownika (art. 52 §1 pkt 1 KP), rozpatrzenie sprzeciwu od nałożenia kary porządkowej (art. 112 §1 KP).

Dane dotyczące popełnienia przestępstwa

Konsultacja zamiaru rozwiązania umowy bez wypowiedzenia z winy pracownika, gdy przestępstwo uniemożliwia dalsze zatrudnienie (art. 52 §1 pkt 2 KP).

Dane wrażliwe dotyczące zdrowia

Konsultacja zamiaru rozwiązania umowy bez wypowiedzenia z powodu długotrwałej choroby pracownika (art. 53 §1 KP).

Dane dotyczące warunków zatrudnienia

Konsultacja wypowiedzenia zmieniającego warunki pracy lub płacy (art. 42 §1 w zw. z art. 38 KP).

³⁸ ibidem 10–11.

³⁹ EDPB Guidelines 01/2022 on data subject rights - Right of access, 33



▪ **Przetwarzanie danych dotyczących członków związku zawodowego**

– Niezbędność do wypełnienia obowiązków i wykonywania praw (art. 9 ust. 2 lit. b RODO)

Art. 9 ust. 2 lit. b RODO dopuszcza przetwarzanie szczególnych kategorii danych (w tym dotyczących członkostwa w związkach zawodowych), jeśli jest to niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. W praktyce oznacza to, że w określonych ustawowo bądź w porozumieniu zbiorowym sytuacjach dochodzi do zgodnego z prawem ujawnienia pracodawcy informacji o członkostwie w związku. Do takich sytuacji na gruncie prawa krajowego należą:

- Udzielenie pracownikowi urlopu bezpłatnego w związku z pełnieniem funkcji związkowej poza zakładem pracy (art. 25 u.z.z.).
- Zwolnienie z obowiązku świadczenia pracy na okres kadencji w zarządzie zakładowej organizacji związkowej (art. 31 u.z.z.).
- Wskazanie pracodawcy imiennej listy działaczy objętych szczególną ochroną stosunku pracy (art. 32 u.z.z.).
- Przekazanie pracodawcy wniosku o pobieranie składek członkowskich z wynagrodzenia pracownika (art. 33¹ u.z.z.). W tym przypadku pracodawca staje się administratorem danych o przynależności związkowej, ale przetwarzanie to jest ściśle ograniczone do celu pobrania składki. Pracodawca nie może wykorzystać tej wiedzy w żadnym innym celu.

– Przetwarzanie w ramach działalności związkowej (art. 9 ust. 2 lit. d RODO):

Zgodnie z art. 9 ust. 2 pkt d RODO – zakaz przetwarzania szczególnych kategorii danych osobowych (w tym danych osobowych ujawniających przynależność do związków zawodowych) nie znajduje zastosowania w sytuacjach, gdy przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń, w szczególności przez niezarobkowy podmiot o celach związkowych – pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub



byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których one dotyczą.

Przepis ten pozwala zatem związkom zawodowym na przetwarzanie danych członków, byłych członków oraz osób utrzymujących z organizacją stałe kontakty. Co istotne, przepis ten nie pozwala na ujawnianie danych osobowych na zewnątrz organizacji bez zgody osoby, której dane dotyczą. Stanowi on zatem jedynie podstawę dla wewnętrznych procesów, takich jak prowadzenie ewidencji członków.

W praktyce, jak słusznie wskazuje Dörre-Kolasa, jednym z najczęstszych błędów jest opieranie przetwarzania danych członków na zgodzie. Biorąc pod uwagę konstytutywny element zgody, jakim jest możliwość jej wycofania w każdym czasie (art. 7 ust.3 RODO) – skuteczne cofnięcie zgody przez członka związku doprowadziłoby do absurdu, w której związek (mimo formalnego utrzymania członkostwa danej osoby) nie mógłby przetwarzać jej danych, a tym samym nie mógłby wypełnić swoich ustawowych obowiązków sprawozdawczych i weryfikacyjnych (np. wynikających z art. 25¹ u.z.z.).⁴⁰

5.3. Dostęp związków zawodowych do danych osobowych pracowników

Istotnym zagadnieniem w zbiorowym prawie pracy jest określenie zakresu, w jakim realizacja ustawowych uprawnień związków zawodowych może stanowić podstawę dostępu do danych osobowych pracowników przetwarzanych przez pracodawcę. Zagadnienie to nabiera dodatkowej doniosłości wobec opisywanej we wprowadzeniu do niniejszej ekspertyzy wycinkowej, rosnącej roli zaawansowanych technologii (w tym zautomatyzowanych systemów monitorowania i podejmowania decyzji) w środowisku pracy.

⁴⁰ Szerzej, Dörre-Kolasa, D. (2019), Administrator danych osobowych w zbiorowym prawie zatrudnienia. Studia z Zakresu Prawa Pracy i Polityki Społecznej (Studies on Labour Law and Social Policy), 2019, 367-388.



Szczególne znaczenie ma w tym względzie art. 28 ustawy o związkach zawodowych, który stanowi, iż pracodawca jest obowiązany, na wniosek związku zawodowego, udzielić informacji niezbędnych do prowadzenia działalności związkowej. Ustawodawca wskazuje przy tym przykładowe kategorie danych (w tym m.in. dotyczące warunków pracy i i zasad wynagradzania; działań, które mogą powodować istotne zmiany w organizacji pracy).

Przesłanka „niezbędności” informacji powinna być interpretowana w kontekście rzeczywistego wpływu technologii na warunki pracy i płacy czy organizację pracy. W świetle zmieniających się realiów świadczenia pracy – art. 28 u.z.z. powinien obejmować zatem również dane dotyczące systemów algorytmicznych (zautomatyzowanych systemów monitorujących i podejmujących decyzje), mających niezaprzeczalny wpływ na warunki czy organizację pracy⁴¹. Realizacja uprawnień informacyjnych z art. 28 u.z.z. może stanowić zatem podstawę prawną dostępu do informacji, które są niezbędne dla oceny wpływu technologii na warunki pracy i płacy czy organizację pracy, w tym:

- o celu i zasad działania zautomatyzowanych systemów monitoringu;
- o kategorii danych i działań monitorowanych, nadzorowanych lub ocenianych przez takie systemy;
- o odbiorców lub kategorie odbiorców danych osobowych przetwarzanych przez takie systemy oraz wszelkie przesyłanie lub przekazywanie takich danych osobowych, w tym w ramach grupy przedsiębiorstw;
- o kategorii decyzji podejmowanych lub wspieranych przez zautomatyzowane systemy decyzyjne;
- o kategorii danych i głównych parametrów uwzględnianych przez takie systemy oraz względne znaczenie tych głównych parametrów w zautomatyzowanym podejmowaniu decyzji – w tym sposób, w jaki dane osobowe lub zachowanie osoby wykonującej pracę za pośrednictwem platform wpływają na decyzje;

⁴¹ Baran K. (2024) The right of trade unions to information in the era of the fourth and fifth industrial revolutions, Białystok Legal Studies Białostockie Studia Prawnicze 2024 vol. 29 no. 2, 29-38



- o powody podjęcia decyzji o jej statusie umownym lub jakiegokolwiek decyzji o równoważnych lub szkodliwych skutkach.

Przekazanie danych w takim przypadku opierać można na przesłance legalności z art. 6 ust. 1 lit. c RODO (spełnienie obowiązku prawnego ciążącego na administratorze) lub art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes), o ile spełniony jest wymóg niezbędności i proporcjonalności przetwarzania (nadrzędny charakter wobec tych interesów).

Niezależnie od przyjętej podstawy prawnej przetwarzania – należy pamiętać, że zakres danych przekazywanych związkom zawodowym każdorazowo musi pozostawać w bezpośrednim związku z realizacją ich ustawowych funkcji reprezentacyjnych; a więc w szczególności podlega zasadzie minimalizacji danych (art. 5 ust. 1 lit. c RODO) i zasadzie ograniczenia celu (art. 5 ust. 1 lit. b RODO).

Co istotne – w wyroku z września 2024 r. Naczelny Sąd Administracyjny przesądził, że:

- ochrona danych osobowych pracowników, w szczególności w kontekście monitoringu czy profilowania, stanowi element obrony szeroko rozumianych praw pracowniczych (art. 1 ust. 1 ustawy z 23 maja 1991 r. o związkach zawodowych);
- związek zawodowy posiada legitymację procesową do inicjowania postępowań przed Prezesem UODO⁴²;
- działania związku zawodowego mogą obejmować reagowanie na niezgodne z prawem praktyki przetwarzania danych, w tym brak oceny skutków dla ochrony danych, nielegalny monitoring, zautomatyzowane podejmowanie decyzji czy nienależyte obowiązki informacyjne⁴³.

⁴² Cf. Wyrok NSA z 21 listopada 2018 r. II OSK 2851/16 : ‘interes społeczny może przemawiać za wszczęciem postępowania przez organizację społeczną wówczas, gdy sama strona mając trudności z zainicjowaniem postępowania nie wszczyna go, albo organ administracyjny nie ma wiedzy co do danego przedmiotu postępowania, a sprawa powinna być prowadzona celem jej załatwienia’

⁴³ Wyrok Naczelnego Sądu Administracyjnego z dnia 19 września 2024 r. III OSK 4707/21.



Podsumowanie

Postępująca cyfryzacja środowiska pracy niewątpliwie generuje nowe wyzwania dla zapewnienia wysokiego poziomu ochrony praw podstawowych pracowników. W warunkach rosnącej presji rynkowej na wdrażanie coraz bardziej zaawansowanych technologicznie form monitorowania i nadzoru – układy zbiorowe pracy stają się kluczowym instrumentem ochronnym, który może zostać efektywnie wykorzystany do skorygowania strukturalnej asymetrii negocjacyjnej pomiędzy stronami stosunku pracy oraz zminimalizowania szeregu ryzyk wynikających z cyfryzacji procesów zarządzania pracą. Z perspektywy pracodawców wzmocnienie roli układów zbiorowych w obszarze ochrony danych osobowych stanowić może istotny element sprawiedliwego i demokratycznego zarządzania zmianą technologiczną, który jednocześnie może pozytywnie wpływać na zwiększenie rozliczalności pracodawcy na gruncie RODO, a w konsekwencji ograniczyć ryzyko prawne, finansowe i reputacyjne związane z potencjalnymi naruszeniami przepisów o ochronie danych osobowych.

Artykuł 88 RODO potwierdza przy tym niejako szczególną legitymację związków zawodowych do aktywnego kształtowania zasad ochrony prywatności informacyjnej oraz powiązanych z nią praw podstawowych we współczesnym środowisku pracy. Układy zbiorowe pracy odgrywają w tym procesie rolę centralną – umożliwiają ustanowienie precyzyjnych, kontekstowo adekwatnych standardów przetwarzania danych osobowych pracowników. Dzięki temu mogą nie tylko skutecznie ograniczać nadużycia związane z wykorzystaniem nowych technologii w miejscu pracy, ale również wspierać rozwój odpowiedzialnych, transparentnych i zgodnych z zasadami demokratycznego zarządzania modeli cyfrowej organizacji pracy. Tym samym układy zbiorowe pracy stają się jednym z kluczowych narzędzi pozwalających na pogodzenie innowacji technologicznych ze skuteczną ochroną praw podstawowych pracowników.



Lista Kontrolna

Preambuła i Zakres Obowiązania

Jasno definiuje, których pracowników, lokalizacje firmy oraz konkretne systemy lub moduły IT obejmuje porozumienie.

Określenie Celów Przetwarzania

To kluczowy element porozumienia. Powinien wyczerpująco wymieniać wszystkie uzasadnione cele, dla których dane będą przetwarzane. Co istotne, musi również jednoznacznie wskazywać, do jakich celów dane nie mogą być wykorzystywane. Przykład: „Dane z systemu kontroli dostępu mogą być wykorzystywane w celach bezpieczeństwa oraz weryfikacji ewidencji czasu pracy, ale nie do ogólnej analizy wyników pracy.”

Kategorie Danych

Precyzyjna lista wszystkich kategorii danych osobowych przetwarzanych w systemie. Służy jako kluczowe narzędzie wdrażania zasady minimalizacji danych. Związki zawodowe mogą kwestionować konieczność zbierania określonych danych.

Prawa Dostępu

Szczegółowa matryca określająca, które stanowiska w strukturze organizacji (np. HR Business Partner, Administrator Systemu) mają dostęp do których kategorii danych oraz z jakimi uprawnieniami (odczyt, zapis, usunięcie). Operacjonalizuje zasadę „need-to-know”.

Retencja i Usuwanie Danych

Określa precyzyjne okresy przechowywania dla różnych kategorii danych, powiązane z obowiązkami prawnymi lub uzasadnionymi interesami prawnymi pracodawcy. Tworzy prawnie wiążący harmonogram usuwania danych z systemu.

Międzynarodowy Transfer Danych

Określa warunki przekazywania danych poza UE/EOG, często wymagając wdrożenia standardowych klauzul umownych (SCC).

Prawa Pracowników

Opisuje proces, w ramach którego pracownicy mogą korzystać z prawa dostępu do danych, ich sprostowania lub usunięcia, często definiując konkretne punkty kontaktowe i terminy odpowiedzi.



Informowanie i Szkolenia:

Może zawierać obowiązki pracodawcy dotyczące informowania pracowników o systemie oraz zapewnienia odpowiednich szkoleń.

Uprawnienia Związków Zawodowych:

Obejmuje postanowienia umożliwiające związkom zawodowym audyt zgodności systemu z porozumieniem, (docelowo) przy wsparciu niezależnego eksperta.



Przykładowe klauzule układów zbiorowych dot. przetwarzania danych osobowych w zatrudnieniu⁴⁴

❖ Ograniczenie przetwarzania danych w systemach informatycznych

Zakres przetwarzania danych

Zgodnie z obowiązującymi przepisami prawa, w ramach funkcjonujących w zakładzie pracy systemów informatycznych przetwarzane są wyłącznie te dane osobowe pracowników, które są niezbędne do prawidłowego działania danego systemu lub do wykonywania pracy z jego użyciem. Przetwarzanie danych wykraczające poza te cele jest niedopuszczalne.

Zakaz dalszego wykorzystania danych

Dane osobowe gromadzone w ramach systemów informatycznych nie mogą być wykorzystywane przez pracodawcę ani jego jednostki organizacyjne do innych celów niż cel, dla którego zostały zebrane, w szczególności do celów operacyjnych niezwiązanych z funkcjonowaniem systemu.

Kontrola zachowania i wyników pracy

Dane osobowe pracowników mogą być wykorzystywane do kontroli zachowania i/lub kontroli wyników pracy wyłącznie wówczas, gdy:

- a) zostały zgromadzone w tym konkretnym celu, oraz
- b) pracownicy, których dane dotyczą, byli o tym poinformowani w momencie korzystania z danego systemu informatycznego.

⁴⁴ Przygotowane na podstawie: <https://publicservices.international/resources/page/digital-bargaining-hub/5-data-rights-and-data-protection---hj?lang=en&id=13182>, <https://hiva.kuleuven.be/sites/gdpir/docs/guidelines-en.pdf>, <https://publicservices.international/resources/page/digital-bargaining-hub/6-workers-rights-over-digital-tools-and-ai-their-use-and-deployment---hj?lang=en&id=13183>; https://www.eurocockpit.eu/sites/default/files/2022-08/Report_Full_KULeuven_29July2021%20fin%20draft.pdf.



❖ **Monitoring w postaci kamer zamontowanych w pojazdach służbowych objętych ubezpieczeniem**

Cel stosowania kamer

[Firma] instaluje w pojazdach flotowych objętych ubezpieczeniem kamery skierowane do przodu (*Forward Facing Cameras*) wyłącznie **w celu**:

- ustalenia przebiegu zdarzeń drogowych oraz sytuacji potencjalnie wypadkowych (*near miss*);
- wspierania poprawy bezpieczeństwa jazdy po zaistnieniu zdarzenia;
- obrony przed roszczeniami stron trzecich kierowanymi przeciwko [Firmie].

Dane uzyskane z kamer nie mogą być wykorzystywane do celów związanych z kontrolą zachowania pracownika.

❖ **Inne formy monitoringu (monitoring algorytmiczny)**

Zakaz stosowania technologii wysokiego ryzyka

Zabrania się stosowania technologii monitoringu, które są niezweryfikowane, obarczone wysokim ryzykiem błędów, braku przejrzystości lub naruszają godność i prawo do prywatności pracownika.

Zgoda związków zawodowych na monitoring algorytmiczny

W przypadku instalacji automatycznych systemów monitorujących, mających na celu zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, konieczne jest uprzednie uzgodnienie tego ze związkiem zawodowym, a także wdrożenie środków umożliwiających pracownikom oraz związkowi zawodowemu rozpoznanie działania tych urządzeń w trakcie ich używania.



W szczególności uzgodnieniu podlegają:

- cel instalacji oraz okres użytkowania,
- sposób instalacji oraz zakres rejestrowanych danych,
- rodzaje i parametry techniczne urządzeń monitorujących,
- komórka organizacyjna oraz osoba odpowiedzialna za nadzór nad systemem.

Pracodawca nie może uwzględniać danych zarejestrowanych przez ww. urządzenia monitorujące do oceny wyników pracy ani wykorzystywać ich jako podstawy do zastosowania kar porządkowych.

Jeżeli zainstalowane urządzenia naruszają postanowienia układu zbiorowego pracy, bądź też jeśli upłynął cel oraz okres ich stosowania, pracodawca niezwłocznie usuwa urządzenia monitorujące oraz informuje o tym związek zawodowy.

Monitoring nie może obejmować czasu pozostawiania pracownika poza pracą, w szczególności przerw w pracy, urlopów oraz czasu prywatnego (poza godzinami pracy). Funkcje geolokalizacji w urządzeniach służbowych muszą być dezaktywowane poza czasem pracy.

Dane uzyskane z monitoringu algorytmicznego nie mogą stanowić wyłącznej ani przeważającej podstawy podejmowania decyzji dotyczących:

1. nawiązania i rozwiązania stosunku pracy,
2. oceny okresowej, awansu lub obniżenia wynagrodzenia,
3. stosowania sankcji dyscyplinarnych.

Każda decyzja dotycząca pracownika, przy której wykorzystano dane z ww. monitoringu, wymaga niezależnej oceny dokonanej przez człowieka z uwzględnieniem dodatkowych źródeł informacji (w tym stanowiska pracownika w danej sprawie).



❖ **Wdrażanie i stosowanie systemów sztucznej inteligencji w środowisku pracy**

Zasada nadrzędnej kontroli człowieka

Systemy sztucznej inteligencji (SI) mogą być wdrażane i stosowane wyłącznie w sposób zapewniający nadrzędną kontrolę człowieka nad ich działaniem oraz wynikami, w tym możliwość ingerencji w proces decyzyjny oraz wstrzymania lub zmiany rozstrzygnięcia systemu.

Pracodawca zapewnia, że żadne decyzje wywołujące skutki prawne lub istotnie wpływające na sytuację pracownika nie są podejmowane wyłącznie w sposób zautomatyzowany bez udziału człowieka.

Bezpieczeństwo i ocena ryzyka

Przed wdrożeniem systemu SI pracodawca przeprowadza ocenę ryzyka, obejmującą analizę możliwych zagrożeń, w szczególności dla integralności fizycznej i psychicznej pracowników oraz ryzyka błędów poznawczych i błędnych wyników algorytmicznych. Systemy SI muszą być użytkowane w sposób zapewniający zapobieganie szkodom oraz ciągłą identyfikację i minimalizację ryzyk.

Zasada równego traktowania i niedyskryminacji

Systemy SI podlegają wdrażaniu i stosowaniu z poszanowaniem zasady równego traktowania i zakazu dyskryminacji.

Pracodawca zapewnia, że algorytmy i dane wejściowe nie prowadzą do uprzedzeń, nierównego traktowania lub nieuprawnionego profilowania pracowników lub grup pracowników.

Pracodawca wdraża procedury testowania stronniczości algorytmicznej, obejmujące także okresowe audyty.



Przejrzystość i nadzór

Systemy SI muszą zapewniać możliwość wyjaśnienia sposobu działania, logiki podejmowanych rozstrzygnięć oraz danych, które stanowią podstawę działania systemu.

Zakres wymaganej wyjaśnialności dostosowuje się do kontekstu, wagi i skutków decyzji podejmowanych z wykorzystaniem systemu.

Pracodawca wdraża mechanizmy kontroli jakości wyników SI oraz procedury wstrzymywania działania systemu w przypadku wyników błędnych lub niewiarygodnych.

Stosowanie systemów SI w procesach kadrowych

W przypadku wykorzystania systemów SI w procesach:

- rekrutacji, selekcji lub oceny kandydatów,
- oceny pracy, wydajności lub zachowań pracowników,
- analizy wyników pracy,
- awansów, przeniesień lub zmian warunków pracy,
- rozwiązywania stosunku pracy.

Pracodawca zapewnia pracownikom dostęp do informacji o zasadach działania systemu oraz kryteriach, na podstawie których podejmowane są decyzje.

Pracownik, którego dotyczy decyzja z udziałem SI, ma prawo:

- żądać interwencji człowieka,
- zakwestionować decyzję (w tym przedstawić swoje stanowisko w sprawie)
- żądać weryfikacji i wyjaśnienia wyników działania systemu.

Udział związków zawodowych

Wdrożenie, istotna modyfikacja lub rozszerzenie zastosowania systemu SI wymaga konsultacji ze związkami zawodowymi na etapie planowania, projektowania, oceny skutków dla ochrony danych (DPIA) oraz okresowej ewaluacji działania systemu.



Związki zawodowe mają prawo do:

- dostępu do dokumentacji oceny skutków dla ochrony danych (DPIA),
- udziału w procesie tworzenia stosownych polityk i procedur,
- wnioskowania o audyt algorytmiczny.

Pracodawca przedstawia związkom zawodowym okresowe raporty z funkcjonowania systemów SI nie rzadziej niż raz na [np. 12 miesięcy].

