Working Paper 1/2026

Citation suggérée : Ludovica Robustelli, The protection of personal data in the context of AI systems used for profesionnal purporeses : a neglected issue, *Blogdroiteuropéen,* Working paper 1/2026, mars 2026, accessible à https://wp.me/p6OBGR-6yy

The protection of personal data in the context of AI systems used for professional purposes: a neglected issue

Ludovica Robustelli, docteure en droit de l'UE et chercheuse postdoctorale au CNRS (Nantes Université)

Sommaire

Résumé en français : Bien que le déploiement de l'IA sur le lieu de travail ait suscité beaucoup d'attention, peu d'importance a été accordée aux violations potentielles des données à caractère personnel des travailleurs qui y sont associées. Dans un contexte d'engouement croissant à l'égard de l'IA, il importe de rappeler que les travailleurs sont exposés au traitement de leurs données à caractère personnel par l'IA (et pas que) sur le lieu de travail autant à des fins de recrutement que de gestion du travail. Il convient donc d'établir un juste équilibre entre la protection des données à caractère personnel et la législation sur l'IA afin d'éviter des violations, ainsi que le sentiment pour les employés d'être sous-surveillance, autant de facteurs qui menacent d'exacerber le déséquilibre entre les travailleurs et les employeurs. Un aperçu des risques liés au déploiement de l'IA dans le contexte professionnel montre que la législation actuelle doit encore être améliorée, malgré les efforts de l'UE pour minimiser les risques. Le présent article vise à formuler des suggestions sur la base de l'état actuel de la législation.

Key-words: personal data protection, artificial intelligence, algorithmic management, high-risk AI systems, platform workers.

Introduction

The risks associated with the use of AI in the workplace have long been well known. The technostress associated with information overload due to digitisation, the fear of being replaced by robots and the resulting job losses are all examples[1].

In terms of how these systems are designed and trained, data, including personal data, is an essential component. The General Data Protection Regulation (GDPR)[2] sets out specific rules for the processing of employees' personal data by employers. For example, online recruitment based on a single automated decision is prohibited, and the use of profiling to assess employee's performance is subject to strict rules[3]. Article 88 of the GDPR also provides that Member States may adopt more protective provisions for the protection of workers' personal data[4], provided they previously notify them to the European Commission[5]. This shows that the protection of workers' personal data is an area that needs to be explored and where there is still a leeway for improvement. Nevertheless, this issue tends to be dismissed since the AI Regulation came into force[6], despite the importance of ensuring its proper articulation with the GDPR to safeguard the protection of workers' personal data.

[1] On the risks and opportunities of the deployment of AI systems at work, see Chiara Cristofolini, 'Navigating the impact of AI systems in the workplace: strengths and loopholes of the EU AI Act from a labour perspective', (2024) 17(1) *Italian Labour Law e-Journal*, <https://doi.org/10.6092/issn.1561-8048/19796> accessed 17 October 2025; Adrian Todolí-Signes, 'Making algorithms safe for workers: occupational risks associated with work managed by artificial intelligence', (2021) 27(4), *Transfer: European Review of Labour and Research*; Moore Phoebe V., 'OSH and the future of work: benefits and risks of artificial intelligence tools in workplaces', (2019) in Duffy V. (eds) *Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management. Human Body and Motion*. HCII 2019. Lecture Notes in Computer Science, vol 11581. Springer, Cham. <https://doi.org/10.1007/978-3-030-22216-1_22>, accessed 17 October 2025; Osoba Osonde A., Welser William, *The risks of artificial intelligence to security and the future of work* (RAND, 2017).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), [2016] OJ L 119/1.

[3] *Ibid.*, art 22 par 1-2 '1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent. (…)'.

[4] *Ibid.*, art 88 par 1 ' Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship'.

[5] *Ibid.*, par 3 'Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.'.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AIA), [2024] OJ L 2024/1689.

On 1 August 2024, one of the world's first instrument attempting to regulate AI systems within the EU internal market (and beyond) came into force. Since then, all attention is focused on the obligations binding operators involved in the lifecycle of these systems. Depending on the risks to safety, health and the protection of fundamental rights, AI tools are subject to a classification based on four levels of risk, ranging from prohibited practices to systems presenting no risk[7]. AI systems deployed in the workplace are a privileged target for observation since many of their uses are classified as high-risk[8]. This is especially the case since the European Commission has introduced two proposals (Digital and AI Omnibus)[9] that are aimed at simplifying regulations relating to AI systems and, among others, personal data protection rules. The objective of these proposals is to reduce regulatory and administrative burdens in order to foster innovation and competitiveness in the EU[10]. However, there is a high risk that these simplification measures could affect the level of protection for workers whose personal data are processed by AIS at work, rendering some of their rights void.

The use of AI systems for professional reasons generally pursues various objectives. The first is recruitment. AI systems are often used to scan CVs to select candidates for interview, or to draw up a job description based on the profile sought. In the context of the employment relationship, employers can profile workers to assess their performance, sanction or promote them and, possibly, use a generative AI system to congratulate on them. All the previously mentioned use cases are considered to present a high risk[11], and all mainly involve the processing of personal data, the risks of which are, however, currently underestimated.

This paper addresses the implications of deploying AI systems in the workplace for workers' personal data and aims to answer the following questions: what risks does deploying AI systems in the workplace pose to workers' personal data? Is current legislation satisfactory enough to mitigate these risks? Is there still room for improvement? To answer these questions, the AIA and the GDPR will be analysed considering the Digital and AI Omnibus Proposals. The Platform Work Directive[12] will be dealt with only regarding the aspects intersecting with the AIA and presenting relevance to the GDPR (Chapter III, personal data processing by means of automated monitoring systems or automated decision-making systems). This Directive sets up a rebuttable presumption of employment relationship between the worker and the platform when the platform gives directives to the worker[13]. This considerably improves their working

[7] On the limits of this classification, see Martin Ebers 'Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act', (2025) 16 *European Journal of Risk Regulation* 692.

[8] It should be noted that high-risk AIS obligations are not yet applicable. They will be applicable from August 2026 for AIS used in employment (art. 6.2) and from August 2027 for AIS referred to in art. 6.1 AIA.

[9] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) COM/2025/837 final; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM/2025/836 final.

[10] Bracy Jedidiah, 'European Commission proposes significant reforms to GDPR, AI Act', (2025) *Iapp* < https://iapp.org/news/a/european-commission-proposes-significant-reforms-to-gdpr-ai-act>, accessed 13 January 2026.

[11] See Annex III: High-Risk AI Systems Referred to in Article 6(2), AIA.

[12] Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work PE/89/2024/REV/1 [2024] OJ L 2024/2831.

[13] *Ibid.*, art 5.

rights and conditions.

The following developments will focus on the risks relating to workers' personal data protection when an AI system is used in the recruitment process and for work management (II), considering the current applicable legislation and the mitigation measures in force (III), together with their loopholes (IV) and attempt to suggest potential improvements (V).

I. The risks

There are two aspects to the processing of workers' personal data by AIS: firstly, personal data are collected and processed as input for the tool, and secondly, personal data are processed to produce the AIS outputs. Both processes involve the processing of personal data, the consequences of which are intertwined in the event of the deployment of an AIS at work. Indeed, the AIS is intended not only to track the worker or implement surveillance measures, but also to inform or directly take management decisions about him with "fresh data". Therefore, they are not treated separately within this paper.

Specific threats arise depending on whether AI systems are used for recruitment or management processes.

A- Recruitment process

There has been much discussion about the loopholes in AI systems used for recruitment purposes, but not enough on the implications for personal data protection. The way AI works goes against its basic principles. The loss of control that workers experience over their personal data infringes their right to the informational self-determination, which is the right to control their personal data[14]. The European Parliament has emphasised the importance of educating employees on the use of AI tools as a potential solution to this issue[15].

Recital 39 of the GDPR states that workers must be aware of the risks and rules associated with algorithmic management. This is especially relevant considering the multiple sources of information employers have at their disposal, such as social media, publicly available data on job applicants, and recruitment agencies. Some tools allow the collection of personal data by default, without a clear purpose, in case this information could be useful for potential future usage[16]. This also conflicts with the purpose limitation principle, which requires that personal data are processed only for specific grounds and with the data subject's agreement[17].

[14] This is true especially when workers do lack Ai literacy or when the AI algorithms are regularly updated.

[15] European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics 2018/2088(INI) pt 62.

[16] Butterworth Michael, 'The ICO and artificial intelligence: The role of fairness in the GDPR framework', (2018) 34 *Computer Law & Security Review* 259.

[17] GDRP, art 5 par 1 '1. Personal data shall be: (…)
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');'.

AI systems used for job interviews can infer personal data from characteristics such as voice and emotional state to create a personality profile[18]. The AI systems need strong data; this means increasing data sources as well as their relevance and quantity[19]. For example, an AI system used for CV scanning could also collect information from public social media profiles to improve the chances of selecting the best candidate.

Some systems produce job vacancy notices, select relevant CVs, interview applicants, and keep in touch with them[20]. However, these processes conflict with the minimisation principle, which states that only personal data that is essential to the processing purposes should be treated[21]. Unfortunately, job candidates are not able to refuse this kind of personal data processing; the risk of retaliation is too high. For this reason, consent is not an appropriate legal basis for processing personal data at the recruitment stage.

Respecting the accuracy principle is also challenging with AI systems because they can produce erroneous results and lead to discrimination and privacy infringements. Therefore, the European Parliament proposed an amendment to prohibit the use of workers' biometric data to infer their feelings in June 2023[22]. On this point, Article 5(1)(d) of the GDPR requires that personal data are processed accurately and, if inaccurate, are rectified or deleted without delay.

B- Work management

The main feature of algorithmic work management is that management decisions are informed directly by data. Amazon has used wearables for surveillance purposes to carry out this kind of management[23]. For example, AI bracelets have been used to monitor workers' activities and alert them when their movement was not appropriate[24]. The CNIL (French Data Protection Authority) fined Amazon France Logistique €32 million for adopting a scanning system intended to monitor workers' performance and

[18] De Stefano Valerio, Wouters Mathias, 'AI and digital tools in workplace management and evaluation. An assessment of the EU's legal framework' (2022) Osgoode Legal Studies Research Paper no 4144899, 12 <https://ssrn.com/abstract=4144899> consulted 17 October 2025. See also art 5, par 1 AIA, which prohibits this practice.

[19] *Ibid.* 27.

[20] See Halefom Abraha, 'Regulating algorithmic employment decisions through data protection law', (2023)14(2) *European Labour Law Journal* 173.

[21] Phoebe V. Moore, 'Data subjects, digital surveillance, AI and the future of work', (Scientific Foresight Unit, European Parliament 2020) 34 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf> accessed 17 October 2025. This is also the case of personal data processing for work management purposes.

[22] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), P9_TA(2023)0236, (Ordinary legislative procedure: first reading), Proposal for a regulation art 5 – par 1– pt d c (new) amendment 226 <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html> accessed 17 October 2025.

[23] Delfanti Alessandro, Radovac Lilian and Taylor Walker, *The Amazon Panopticon: A Guide for Workers, Organizers & Policymakers* (UNI Global 2021).

[24] De Stefano Valerio, Wouters Mathias (n 18) 25.

retain this data for over a month, deeming it disproportionate despite the high standards of the Amazon business model[25].

Platform workers experience the most surveillance, and women are more exposed than men[26]. The OECD defines algorithmic management in the workplace as 'the use of technological tools, which may include artificial intelligence (AI), to fully or partially automate tasks that were traditionally carried out by human managers'[27]. This means that workers can be monitored by other sources than AI[28]. Indeed, some drivers have had their professional accounts deactivated because of bad ratings from customers, by a platform algorithm rather than by an AI system.

Some AI systems could also dismiss workers if they fail to meet deadlines[29]. All these decisions are based on personal data, such as the location used to calculate delivery speed, customer feedback that could relate to the worker's personal attitude, and information provided by the worker in his account. This is a significant intrusion into their personal data protection right[30]. Furthermore, the reliability of these AI systems is questionable, as they can predict but not interpret the casual relationships between things[31]. Some mistakes can occur because of this limitation.

The automation bias is explicitly mentioned in article 14 of the AIA, dealing with human oversight[32]. It refers to human beings' tendency to over-rely on suggestions by AI systems, so that human control over the tool is just confirmation of its output[33].

[25] CNIL, 'Employee monitoring: CNIL fined AMAZON FRANCE LOGISTIQUE €32 million', (2024) < https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million>, accessed 14 January 2026.

[26] UN, ILO, *Mind the AI Divide: Shaping a Global Perspective on the Future of Work*, (2024) <https://www.ilo.org/publications/major-publications/mind-ai-divide-shaping-global-perspective-future-work> 7 accessed 17 October 2025.

[27] OECD, *Algorithmic Management in the Workplace. New Evidence from an OECD Employers Survey* (2025) 31Artificial Intelligence Papers 9 <https://www.oecd.org/en/publications/algorithmic-management-in-the-workplace_287c13c4-en.html>.

[28] (which is supposed to be autonomous, have access to external data source, to draw on these data for improvements and carry out defined objectives); the deployment of AI systems makes the surveillance even more intrusive. See Kaplan Andreas and Michael Haenlein, 'Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence', (2019)62 *Business Horizons* 17 <https://www.researchgate.net/publication/328761767_Siri_Siri_in_my_hand_Who's_the_fairest_in_the_land_On_the_interpretations_illustrations_and_implications_of_artificial_intelligence> accessed 17 October 2025.

[29] Adrienn Lukács, Szilvia Váradi, 'GDPR-compliant AI-based automated decision-making in the world of work', (2023) (50) 105848 *Computer Law & Security Review* 4-5 <https://doi.org/10.1016/j.clsr.2023.105848> accessed 17 October 2025.

[30] Phoebe V. Moore (n 21) 32.

[31] Bergstein Brian, 'AI Still Gets Confused About How The World Works', (2020) (123)2 MIT *Technology Review* 62 <https://wp.technologyreview.com/wp-content/uploads/2020/02/MIT-Technology-Review-2020-03.pdf?_ga=2.190850602.1666107823.1600110008-729040863.1586204955> accessed 17 October 2025.

[32] AIA art 4 par 1 'High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.'

[33] Johann Laux, Hannah Ruschemeier, 'Automation Bias in the AI Act: On the Legal Implications of Attempting to De-Bias Human Oversight of AI', (2025) Forthcoming in the *European Journal of Risk Regulation* 1 <https://arxiv.org/abs/2502.10036> accessed 17 October 2025; Kate Goddard, Abdul Roudsari and Jeremy C Wyatt, 'Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators', (2012) (19)1 *JAMIA (Journal of the American Medical Informatics Association)* 121.

II. Risks minimization by EU Law

AI systems used in the workplace are classified as high-risk in the AIA. Annex 3 paragraph 4 clarifies this point.

Recital 57 of the AIA takes seriously data protection issues and states as follows: 'AI systems used to monitor the performance and behaviour (…) may also undermine the essence of their fundamental rights to data protection and privacy'. Furthermore, AIA applies without prejudice of the GDPR; in case of conflict, GDPR prevails, except when data are processed within secured spaces (the sandboxes) or to prevent biases (art 10)[34]. Recital 67 also lays down an obligation of transparency from the collection of personal data, which is used for training AI systems.

The deployment of AI systems at work raises sensitive issues regarding biometric personal data, which refer to information relating to a person's body, such as fingerprints or facial images. This data can be used for authentication or identification purposes, or to detect emotions. The processing of such data is prohibited as they're considered sensitive under art 9 GDPR, except when the worker has consented to it, its processing is necessary within the employment sector or the social security, or for the purpose of occupational medicine[35]. However, consent is not an appropriate legal ground. Indeed, according to recital 39 of the GDPR the worker could suffer prejudice because of the consent refusal and since the employment relationship is not symmetric, consent is not freely given[36].

[34] AIA, art 2 par 7 'Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulation (EU) 2016/679 or (EU) 2018/1725, or Directive 2002/58/EC or (EU) 2016/680, without prejudice to Article 10(5) and Article 59 of this Regulation.'

[35] GDPR, art 9 '1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
(…) (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(…) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (…)'.

[36] Article 29 Working Party Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018, 17/ENWP259 rev.01, 7: 'An imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.18 Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.'

Alternative legal grounds to process workers' personal data include the 'necessity to enter into a contract' (art. 6, § 2 b) and the employer's 'legitimate interest', e.g. for payroll purposes or to instruct the workforce[37], which need to be balanced against the protection of the workers' fundamental rights. Furthermore, if the worker is a data subject, he is granted all the rights resulting from this status: the right to be informed, the right to access and rectify his data, and the right to object to or restrict the processing of his personal data... These safeguards ensure that the use of personal data by AI systems in the workplace is strictly limited[38] and the data subject still has some control over his personal data. One of the most relevant provisions in the context of AI systems deployment within professional relationships is article 22 GDPR, stating that the data subject (worker) has the right not to be subject to an entirely automated decision or profiling which could have legal or other serious consequences. Some exceptions exist, but the controller (the employer) should put in place some measures to allow the data subjects to obtain the human control and express his/her point of view or contest the decision. Recital 71 of the GDPR expressly refers to this type of processing in the context of the employment relationship. It recognises the right not to be subject to a fully automated decision in an online recruitment process without human intervention. Furthermore, it stipulates that profiling aimed at assessing work performance is prohibited. On this point, even if the recitals are not binding, they help to interpret the provisions of the Regulation. Moreover, article 22 GDPR applies to AI systems but also to the algorithmic management processing carried out by the platforms[39]. Indeed, the *Schufa* case of the EU Court of justice (EUCJ) clarified the interpretation of this provision, even though the credit scoring system in question did not fall within the definition of an AI system[40], but we mention it because the decision is applicable also to AIS. Since the *Dun & Bradstreet Austria* ruling, the EUCJ stated that:

(…) article 15(1)(h) of the GDPR must be interpreted as meaning that, in the case of automated decision-making (…) the data subject may require the controller, as 'meaningful information about the logic involved', to explain, by means of relevant information and in a concise, transparent, intelligible and easily accessible form, the procedure and principles actually applied in order to use, by automated means, the personal data concerning that person with a view to obtaining a specific result, such as a credit profile[41].

The Platform Work Directive also grants platform workers affected by an automated decision a

[37] Hendrickx, Frank, 'Privacy 4.0 at Work: Regulating Employment, Technology and Automation', (2019) (41)1 *Comparative Labor Law & Policy Journal* 147.
[38] De Stefano Valerio, Wouters Mathias (n 18) 36.
[39] Adrienn Lukács, Szilvia Váradi (n 29) 2.
[40] C-634/21 *SCHUFA Holding (Scoring)* EUCJ [2023] OJ C 37, 24.1.2022. The Court states at pt 73 of its decision: the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes 'automated individual decision-making' within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.
[41] C-203/22 *Dun & Bradstreet Austria* EUCJ [2025] OJ C 222, 07.6.2022*,* pt 66: In the light of recital 71 of the GDPR, such measures must include, in particular, the obligation for the controller to use appropriate mathematical or statistical procedures, implement technical and organisational measures appropriate to ensure that the risk of errors is minimised and inaccuracies are corrected, and secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and prevent, inter alia, discriminatory effects on that person. Those measures include, moreover, at least the right for the data subject to obtain human intervention on the part of the controller, to express his or her point of view and to challenge the decision taken in his or her regard.

right to explanation[42] and to human oversight, which implies an evaluation of the impact of automated decisions on workers[43]. More specifically, any decision to terminate an employment relationship should be made by a human being (art 10, par 5). The *Dun & Bradstreet Austria* ruling grants normal workers almost equivalent protection to platform workers whenever automated decision-making is involved.

A platform worker is someone who performs 'digital labour platform' services, consisting in providing a service electronically and remotely at the receiver's request in return for payment. This also involves the use of automated monitoring or decision-making systems[44]. Processing of biometric data while performing platform work is prohibited under the Platform work directive (art 7, f) and this since the recruitment (art 7, par 2). Under the directive, a data protection impact assessment is compulsory (art. 8).

In a similar vein, article 35 of the GDPR requires an impact assessment to be performed when personal data processing carries a high risk[45].

WP29 adopted guidelines on the interpretation of this provision. In this text, it also considered "high-risk" all the processing concerning "vulnerable subjects", especially within imbalanced relationship and expressly stated employees belong to this category[46].

[42] Platform work directive, art 11 par 1 'Member States shall ensure that persons performing platform work have the right to obtain an oral or written explanation from the digital labour platform for any decision taken or supported by an automated decision-making system without undue delay. The explanation shall be provided in a transparent and intelligible manner, using clear and plain language. Member States shall ensure that digital labour platforms provide persons performing platform work with access to a contact person designated by the digital labour platform to discuss and to clarify the facts, circumstances and reasons having led to the decision. Digital labour platforms shall ensure that such contact persons have the competence, training and authority necessary to exercise that function.'

[43] *Ibid.*, art 10.

[44] *Ibid.* art 2, par 1 'For the purposes of this Directive, the following definitions apply:
(a) 'digital labour platform' means a natural or legal person providing a service which meets all of the following requirements:
(i) it is provided, at least in part, at a distance by electronic means, such as by means of a website or a mobile application;
(ii) it is provided at the request of a recipient of the service;
(iii) it involves, as a necessary and essential component, the organisation of work performed by individuals in return for payment, irrespective of whether that work is performed online or in a certain location;
(iv) it involves the use of automated monitoring systems or automated decision-making systems; (…)'.

[45] GDPR, art 35 par 1 'Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks'.

[46] WP29, Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) (2017) 10, par 7: Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees , more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

Many data protection authorities (DPAs) also considered employment monitoring as high-risk[47]. The GDPR grants Member States the freedom to legislate or enter into collective agreements regarding the processing of personal data within the employment relationship (including for recruitment purposes), with the aim of improving the level of personal data protection provided by the Regulation (art 88).

III. The gaps of current legislation

Processing biometric personal data is considered a prohibited practice, but only in the workplace (recital 44, art 5 f) AIA). Moreover, detecting fatigue and pain is permitted for the prevention of workplace accidents, and the detection of facial expressions (such as a smile)[48]. This creates a loophole whereby such practices are lawful in recruitment, for example during AI-led interviews, since they shift from prohibited practices to high-risk use-cases. On this point, the Commission's Guidelines on the AI prohibited practices have interpreted the notion of 'workplace' broadly to include the hiring process[49]. Nevertheless, AI chatbots that detect fatigue or facial expressions in order to prevent potential accidents could, in the future, process sensitive data for the purpose of AI development, as well as process biometric data, provided that the user is the only person with access to this data (Digital Omnibus, art 3 par 3 - new art. 9, par. 2, k and l). This is problematic, as these new conditions could override the protection currently provided by Article 9 of the GDPR.

On this point, article 22 of the GDPR is not helpful. For article 22 to be applicable, a distinction must be made between augmented and automated decision-making systems. In the former, AI only supports the employer's decision, whereas in the latter, there is no human intervention[50]. Article 22 prohibits submitting people to an individual automated decision only when the decision is entirely automated. To circumvent this prohibition, employers can claim that human intervention is involved, even when it's not the case. Another condition for the prohibition to apply is that the automated decision must have serious consequences, such as legal effects or similar (e.g. denial to entry a territory or discrimination)[51]. Furthermore, the European Data Protection Board (EDPB) considers that the employer can invoke contractual necessity to justify the fully automated screening of candidates, when a huge amount of personal data is involved[52]. Individual automated decisions are also permitted for the performance of a

[47] Müge Fazlioglu, 'What's subject to a DPIA under the GDPR? EDPB on draft lists of 22 supervisory authorities', (*IAPP* 30 October 2018) <https://iapp.org/news/a/whats-subject-to-a-dpia-under-the-gdpr-edpb-on-draft-lists-of-22-supervisory-authorities/> accessed 20 October 2025.

[48] AIA, art 5, par 1 'The following AI practices shall be prohibited: (…) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons; (…)'.

[49] Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) C(2025) 884 final Annex 85, par 254 ' (…) The notion of 'workplace' in Article 5(1)(f) AI Act should also be understood to apply to candidates during the selection and hiring process, consistently with other provisions of the AI Act addressing the placing on the market, putting into service or use of AI systems in the area of employment, workers management and access to self-employment, since there is an imbalance of powers and the intrusive nature of emotion recognition may already apply at the recruitment stage.'

[50] Michael Leyer, Sabrina Schneider 'Decision augmentation and automation with artificial intelligence: Threat or opportunity for managers?' (2021) 64 Business Horizons 715.

[51] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (2018) 21.

[52] *Ibid.* 23.

contract (e.g. processing personal data for payment purposes). Such an exception could undermine the protection granted by article 22 GDPR in the recruitment process and work management.

The same can be said for the application of paragraph 3 of this article, which does not apply if the automated individual decision is permitted by national law[53]. On this point, trade secrets and industrial confidential information can prevent the communication of relevant information concerning the functioning and logic of AI systems (recital 63 of the GDPR acknowledges the IP exception)[54], and as a result hinder the exercise of the right to object to an individual automated decision.

The already fragile protection would not be improved by adopting the current proposal on the Digital Omnibus, which suggests eliminating the right not to be subject to an automated individual decision. The new article 22 rephrases the provision, stating that such a decision is permitted under the same exceptions as the current version (i.e. when consent is given, when it is necessary to enter into a contract, or when authorised by a Member State or EU law)[55]. However, with regard to the exception of entering into a contractual relationship, the 'necessity' principle is overturned, meaning that automated decision-making is allowed even when such a decision could have been made by a human[56]. If this allows workers to invoke art. 22 whenever human oversight is involved, the new provision paves the way for automated individual decisions (by upholding the EDPB guidelines on art. 22, which are non-binding) and calls into question the EUCJ's case law on the matter[57]. Decisions such as that of the Italian DPA sanctioning a subsidiary of Glovo on November 2024 for deactivating workers accounts as a result of their ratings on the basis of an abuse of art 22 GDPR could not be possible anymore[58].

Article 88 allows Member States to adopt laws that offer stronger protection than the GDPR. However, the AIA is a regulation, so according to the primacy principle national law should abide by it. But, the AIA also permits Member States to adopt legislation or administrative measures favourable to workers[59]. This means that national law has a leeway to impose more protective measures. Nevertheless, the risk is high that this article will be underused, as the corresponding article in the GDPR. This is also due to the inherent structure of the AIA which provides fewer individual rights than the GDPR[60].

[53] GDPR, par 2 b); the provision states that adequate safeguards must be taken to protect the data subject.
[54] Halefom Abraha (n 20) 178.
[55] Digital Omnibus, art 3 par 7.
[56] Digital Omnibus, recital 38.
[57] Nyob, *Digital Omnibus. First Analysis of Select GDPR and ePrivacy Proposals by the Commission. Version 1.0*, (2025) 37, <https://noyb.eu/en/digital-omnibus-first-analysis-select-gdpr-and-eprivacy-proposals-commission>, consulted 14 January 2026.
[58] GDPD, *Provvedimento del 13 novembre 2024* [10074601]- available in Italian-, < https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>.
[59] AIA, art 2 par 11 'This Regulation does not preclude the Union or Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or from encouraging or allowing the application of collective agreements which are more favourable to workers.'
[60] Alfieri Constanza, Caroccia Francesca, Paola Inversardi, 'AI Act and Individual Rights: A Juridical and Technical Perspective', (IAIL - Imaging the AI Landscape after the AI Act, 13*th* of June 2022, Amsterdam, Netherlands) <https://ceur-ws.org/Vol-3221/IAIL_paper4.pdf> accessed 20 October 2025. Among the exceptions, see art 86 AIA granting a right to explanation for individual automated decisions made by AIS.

IV. Suggestions for improvement

Article 5 of the GDPR provides useful principles for mitigating risks. These principles help to ensure compliant data processing and reduce the risk of sanctions. A key principle is data minimisation, which requires that only the information that is strictly necessary should be processed. One way to ensure the respect of this principle is the pseudonymisation[61] or the anonymisation of personal data[62]. For example, data used for work management or recruitment could undergo pseudonymisation or anonymisation, whenever this is possible, to better protect jobseekers and employees. A new provision of the Digital Omnibus, which attempts to take into account a new ruling of the EUCJ, suggests revising the definition of pseudonymised data so that it is either personal or anonymous, depending on the operator handling the data[63]. However, such a subjective assessment should not be included in legislation, as this could encourage employers to claim that employees' data is no longer covered by the GDPR as long as the data processed by the AIS is pseudonymised.

Both employers and employees should be aware of the basic principles of personal data protection: employers to grant their respect, and employees to be aware of their rights. This is particularly important in the context of current legal uncertainties, which also affect high-risk AIS obligations under the AIA, whose application could further be postponed by the Omnibus on AI (art 1 par 31 AI Omnibus). In addition, as under the AI Omnibus AI literacy is no more an obligation but a simple recommendation[64], it is important for workers to know that the GDPR offers relevant protection against the processing of their personal data by AI systems. This is further supported by the fact that, even if the Digital and AI Omnibuses are not adopted, the obligations relating to high-risk AI systems will not apply until August 2026 at the earliest, while the GDPR is already applicable and the current version is the only enforceable one, since the Digital Omnibus still has to be negotiated by the co-legislators (as does the AI Omnibus), and the outcome could diverge from the original proposal.

It's also crucial to raise awareness on the importance of using article 88 of the GDPR in the context of AI deployment at work, in conjunction with article 80, which refers to the right of trade unions to file a GDPR complain[65]. The same can be said for article 2(11) of the AIA. Both provisions would ensure that

[61] EDPB, Guidelines 01/2025 on Pseudonymisation, (2025) 13, par 45 'Pseudonymisationmaybeemployedbycontrollersandprocessorsasoneofseveraltechnicaland organisational measures in order to implement data-protection principles according to Art. 25(1) GDPR, in particular data minimisation and confidentiality. It may also contribute to safeguarding the lawfulness, fairness, purpose limitation and accuracy principles.'

[62] Anonymization enables the respect of the principle of minimisation of personal data, since once anonymised, data are no more personal.

[63] See Digital Omnibus, art 3 and C-413/23 P *EDPS v SRB (Concept of personal data)* EUCJ [2025] OJ C 296, 21.08.2023, pt 86: '(…)pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725, in so far as pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable'.

[64] AI Omnibus, recital 5 and art 1 par 4.

[65] GDPR, art 80 '1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

the AIA applies without prejudice to the GDPR and to national laws setting higher standards for workers' protection.

Workers' representatives should also be involved in personal data protection impact assessments. DPAs should not be left alone to enforce the regulations. More awareness must be raised among workers and employers, who must be educated about the risks that AI poses to personal data protection. This can be achieved by promoting dialogue with stakeholders and workers' representatives on the subject. The establishment of educational frameworks to develop an AI workforce would also be beneficial.

DPAs should be appointed as market surveillance authority to grant consistency between the two acts (art 74 of the AIA par 8 suggests this only for repressive aims, justice and democracy but not for the employment)[66]. The possibility of cumulating the role of market surveillance authority with that of personal data protection authority would guarantee more consistency between the GDPR and the AIA in the work field.

Conclusion

This overview of the relationship between personal data protection rules and the AIA has revealed some shortcomings regarding the use of AI systems in the workplace. Despite both the GDPR and the AIA being grounded on a risk-based approach, the processing of workers' personal data by AI systems is not adequately protected. The power imbalance between workers and employers, coupled with the numerous stakeholders involved in the lifecycle of AI systems whose obligations may not align with those of the controller under the GDPR, exacerbates this issue. It seems that only platform workers benefit from better protection. However, this pessimistic conclusion is mitigated by the potential to improve the current legislation and the possibility of raising awareness of the importance of this issue.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.'

[66] According to the AIA, market surveillance authorities should have been appointed by the 5th of August 2025.