



Technology Industries of Finland – Legal Assessment of the Current EU Regulatory Framework for AI in the Workplace

Summary

- When compared to the Platform Directive, the robust, comprehensive, and effective protection provided by the EU legal framework for workers in matters related to the usage of AI systems and algorithmic management in workplaces can, in practice, be deemed to be at the same level as the protection provided by the Platform Directive for platform workers in corresponding matters. Therefore, no additional regulation at EU level concerning these subjects is necessary.
- Employees' health, safety, and fundamental rights are protected in a precautionary manner by the AI Act. Said protection is further strengthened and supplemented by the provisions on ex-post control and penalties, as well as by other provisions of the AI Act in addition to other relevant EU legislation.
- While ensuring the necessary transparency, accountability, and explainability, the AI Act and GDPR guarantee that a human is *de facto* always in command when decisions concerning employees' employment (e.g., dismissals or changing terms and conditions of the employment) are made in a way that includes an AI system, at the very least if employees oppose such processes.
- The GDPR effectively narrows down the collection, processing, and storage of personal data related to employees to only what is absolutely necessary and simultaneously prevents both disproportionate and undue surveillance at work and other violations of the employees' privacy, independently of whether an AI system is deployed in a workplace or not.
- The current EU legal framework provides robust and comprehensive cooperation and participation mechanisms for employees in matters related to, among others, dismissals, privacy, as well as health and safety in a way that guarantees employees a high level of influence, independently of whether these matters are related to usage or intended usage of AI systems or not.
- The current EU legal framework ensures in a sufficient manner and in a way that supports long-term, internal, and external employability that employees are proficient in using AI systems, do not lose their autonomy, and can also adapt to changes while paying special attention to employees in a vulnerable position, such as elderly employees.
- The current EU legal framework robustly prevents and prohibits discriminatory treatments of employees on the basis of biased algorithms or deployment of AI systems. In addition, the current EU legal framework guarantees that a human is *de facto* in control in connection with making decisions concerning the terms and conditions of employees which provides the same level protection against discrimination and unequal treatment, regardless of whether an AI system is deployed or not.
- The current EU legal framework effectively obliges employers to take care of the employees' health, safety, capacity to work, and wellbeing, including when AI systems are deployed in workplaces. It also effectively takes into account and prevents all possible hazards, whether physical or mental, associated with the usage of AI systems in workplaces. This includes but is not limited to employees' excessive workload and work insensitivity, loss of job autonomy, job isolation, and related stress, insecurity, depression, or anxiety.

1. Introduction

The purpose of this Annex is to describe the European Union ("**EU**") regulatory environment that applies to deploying artificial intelligence ("**AI**") in workplaces. However, the below legal assessment does not comprehend all EU (or any national legislation) applicable to the usage of AI systems in workplaces. Instead, the purpose of this Annex is to provide information on the said legal framework in connection with matters and issues that are most often associated to the risks of deploying AI systems in workplaces and especially those that are related to the employees. Furthermore, this Annex focuses on assessing the use of AI in the workplace in the above context from a purely legal perspective. Therefore, although not mentioned in this Annex, there are also several concrete benefits for employees when it comes to the use of AI in the workplace. However, the type of algorithmic management that does not fall within the scope of the Artificial Intelligence Act ("**AI Act**"), i.e., that is ultimately commanded by a human, is not directly assessed here since most of the EU legislation described in this Annex is technology-neutral, meaning that such algorithmic management is already covered by the current legal framework in a way that provides sufficient protection for the employees. This assessment has been made from the perspective of private sector employees.

The assessment is divided to the following sections: 2) General Protection of Health, Safety, and Fundamental Rights Provided by the AI Act; 3) Preventing Deterioration and Other Adverse Effects on Employees' Terms and Conditions of Employment; 4) Privacy of Employees; 5) Cooperation with the Employees; 6) Ensuring that Employees are Equipped with the Necessary Skills; 7) Equality of Employees; and 8) Health and Safety of Employees.

As a summary, it can be stated that the current EU legislation, including the AI Act and General Data Protection Regulation ("**GDPR**"), provide a robust, comprehensive, and effective protection for the employees at EU level that needs no further supplementary legislation. When compared to the Platform Directive, the above-mentioned protection provided by the EU legal framework for employees in matters related to the usage of AI systems in workplaces can, in practice, also be deemed to be in the same level than the protection provided by the Platform Directive for platform workers in corresponding matters.

It should also be noted that AI Omnibus, i.e. the changes made to the AI Act in summer 2026, did not change the above-mentioned in the long run. The extensive requirements for high-risk systems were originally set to take effect in August 2026. With the Omnibus package, this deadline was postponed because the necessary standards, common specifications, guidelines, and the readiness of national authorities had been delayed. The requirements will begin to apply on December 2, 2027, to the systems described in Annex III (a more general, use-case-based list that also includes HR and employee related use cases) and on August 2, 2028, to products covered by the laws listed in Annex I (certain products subject to market surveillance where AI is a safety-critical component but that are not relevant in connection with the topic of this Annex). The Commission must still ensure that supporting measures, i.e., guidelines, standards, and best practices, are in place in time for the start of enforcement. Otherwise, the Omnibus did not present any significant changes regarding the use of AI at work and especially ones that would undermine the level of protection the AI Act provides for natural

persons, including employees.¹

In any case, it should also be remembered that any new EU legislation in this area would have to be in line with the scope and limits of EU competence.

2. General Protection of Health, Safety, and Fundamental Rights Provided by the AI Act

Even though not always mentioned separately in connection with each section below, it should be noted that the protection of the employees' health, safety, and fundamental rights² are already incorporated to the very essence of the AI Act since it introduces the compulsory risk-management system that is run throughout the entire lifecycle of AI systems that pose risks related to health, safety, and fundamental rights (i.e., a high-risk AI system). Among other things, when applied (further elaborated below) the said risk-management system includes an obligation towards AI-system providers to continuously identify and mitigate the relevant risks of AI systems on health, safety, and fundamental rights in light of their intended purpose and reasonably foreseeable misuse, including the possible risks arising from the interaction between the AI system and the environment within which it operates, while taking into account the state of the art in AI. As part of the risk-management system, AI-system providers are also obligated to take care of the quality and relevance of data sets used, technical documentation and record-keeping, transparency and the provision of information to deployers, human oversight, and robustness, accuracy, and cybersecurity that effectively mitigate the risks for health, safety and fundamental rights. The providers of the AI systems must also ensure that the intended systems to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person and natural persons. The AI Act also stipulates more specific transparency obligations for providers and deployers of AI systems that can be deemed effective.

Providers of a high-risk AI systems are also obligated to perform a conformity assessment procedure that is usually based on internal control before placing such an AI system on a market or deploying it otherwise and put in place a quality management system. Most importantly, providers of a high-risk AI system must immediately take the necessary corrective actions to bring that system into conformity, to withdraw it, to disable it, or to recall it, as appropriate, if they consider or have a reason to consider that a high-risk AI system does not comply with the AI Act and inform deployers, distributors, and importers concerned about this. Upon a reasoned request by a competent authority, providers of a high-risk AI system are also obligated to co-operate and provide necessary information to a competent authority and grant access to it to the automatically generated logs of the high-risk AI.

In addition, if deployers, distributors, or importers of the AI system make significant

¹ The changes made to the AI Act in connection with the Omnibus are mentioned later in this updated version of the Annex when they are deemed to have relevance to the subject of it.

² Including but not limited to the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, the right to non-discrimination, workers' rights, the rights of persons with disabilities, gender equality, and the right to an effective remedy and to a fair trial.

modifications of their own to the provided AI system which maintain its high-risk classification or if they make changes that transform the AI system to a high-risk AI system, deployers, distributors, and importers shall be obligated to comply with the above-mentioned obligations related to the risk-management system, conformity assessment procedure, quality management system, necessary corrective actions, and co-operation with a competent authority. Importers of a high-risk AI system must also withhold from placing it to market if they deem that the high-risk AI system does not comply with the AI Act and corresponding obligation applies also to distributors of a high-risk AI system if they deem that the AI system does not comply with the provisions concerning risk-management system described in Section 2., Chapter III of the AI Act. Deployers are also obligated to follow the instructions of the high-risk AI system provider and report possible severe risks to the provider, distributor, and surveillance authority, in which case they must suspend the use of such AI system. The importer and distributor of a high-risk AI system are also subject to a similar reporting obligation, where applicable. Nevertheless, all the above-mentioned operators, for their part, are required to cooperate with the relevant competent authorities in any action those authorities take in relation to the high-risk AI system in order to implement the AI Act.

In addition to corrective measures and considerable fines determined in Articles 79, 80, and 99 of the AI Act applying to the misclassification of an AI system, the market surveillance authority can also temporarily prohibit or recall the AI system if the provider does not take the necessary corrective action by 15 working days at most, or as provided for in the relevant EU harmonisation legislation. The market surveillance authority can also perform inspections in connection with the surveillance of the correct classification of the AI system. In case the market surveillance authority detects certain severe risks related to health, safety, and fundamental rights in connection with the classification assessment or otherwise, the market surveillance authority can also prohibit or recall the AI system permanently if the provider of the AI system does not remedy said deficiencies. Providers, deployers, distributors, importers, and even authorised representatives of a high-risk AI system shall be subject to administrative fines of up to EUR 15 million or, if the offender is an undertaking, up to 3 % of its total worldwide annual turnover for the preceding financial year, whichever is higher, in the event of not complying with their other duties stipulated by the AI Act. (Maximum amounts of fines on infringements related to prohibited AI practices are correspondingly EUR 35 million or 7 % of the undertaking's total worldwide annual turnover for the preceding financial year and correspondingly EUR 7.5 million or 1 % of the undertaking's total worldwide annual turnover for the preceding financial year for providing incorrect, incomplete, or misleading information to notified bodies or national competent authorities in reply to a request.) However, as a result of the AI Omnibus, fines are also capped for SMCs, in an equivalent manner to SMEs. In other words, SMEs and SMCs pay the lower of the percentage of global annual turnover or the fixed amount, whereas larger organisations must pay the higher value as described above.³ In addition, Member States are also obligated to lay down the rules on effective, proportionate, and dissuasive penalties and other enforcement measures, which may also include warnings and non-monetary measures, applicable to infringements of the AI Act by the above-mentioned operators.

³ Correspondingly due to the Omnibus, in an equivalent manner to SMEs, SMCs may provide the elements of the technical documentation specified in Annex IV in a simplified manner established by the Commission. The implementation of the quality management system referred in Article 17 shall also be proportionate to the size of the provider's organisation in particular, if the provider is an SME, including a start up, or an SMC. Such providers are, in any event, obligated to respect the degree of rigour and the level of protection required to ensure the compliance of their high-risk AI systems with the AI Act.

Therefore, it is obvious that the health, safety, and fundamental rights and simultaneously other rights of employees are protected in a precautionary manner by the AI Act. Said protection is further strengthened and supplemented by the provisions on ex-post control and penalties, and by other provisions of the AI Act in addition to other applicable EU legislation.

3. Preventing Deterioration and Other Adverse Effects on Employees' Terms and Conditions of Employment

One of the most common fears related to the use of AI in the workplace is that the employees' terms and conditions of employment will deteriorate in one way or another. Among other things, AI is feared to arbitrarily decide on dismissals, hires, and on other such matters of great importance to employees. These fears are largely based on the misconception that the current EU legal framework does not oblige employers to leave the final decision on matters relating to terms and conditions of employment to a human being.

First of all, it should be noted that in Annex III of the AI Act, it is stated that AI systems intended to be used for recruitment, to make decisions affecting terms of employment relationships, the promotion or termination of employment relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of employees are considered as high-risk AI systems, with the few exceptions mentioned in Article 6(3) of the AI Act that all stipulate that the AI system does not materially influence the outcome of decision making (i.e., said exceptions do not apply if a human is not significantly involved in the decision making). Moreover, these exceptions cannot be applied where the AI system performs a profiling of employees. It should also be noted that the AI Omnibus did not remove provider's obligation to document the assessment before the system in question is placed on the market or put into service where it deems that one or more of the above-mentioned classification exceptions apply to an AI system mentioned in Annex III of the AI Act and to register itself and such non-high-risk AI system to the EU database managed by the Commission. In addition, upon request of national competent authorities, the provider shall provide the documentation of the assessment. However, to streamline compliance and reduce the associated costs, the registration of AI systems was simplified by streamlining the required content in Section B of Annex VIII of the AI Act.

Special attention should be paid to the fact that the aforementioned list of Annex III expressly dictates without limitations that all "*AI systems intended to be used to make decisions affecting terms of work-related relationships*", which is a rather broad and comprehensive concept, are deemed to be high-risk AI systems. As a result, all AI systems making any decisions affecting the terms and conditions of employment, including those of lesser importance, fall within the scope of this classification.

At the very least when combined with the rest of the list of Annex III, it is safe to say that when making decisions concerning employees' terms and conditions of employment, such AI systems are always classified as high-risk AI systems. This means that the precautionary and ex-post protection described above in Section 2. of this Annex (incl. the risk-management system and obligation to comply with strict transparency, accountability, and human oversight requirements) always applies to

such AI systems. In addition, attention should be paid to the fact that certain significant obligations providing security to the employees are also imposed on the deployers of high-risk AI systems (i.e., the employers). Among others, based on Article 26 of the AI Act, deployers of a high-risk AI systems are always obligated to assign human oversight of such AI systems to natural persons who have the necessary competence, training, and authority, as well as the necessary support to perform such task. By requiring human oversight, the AI Act, therefore, *de facto* prevents the adoption of fully automated decision-making tools in the workplace.

In the highly unlikely event that said provision of the AI Act does not guarantee a robust application of the human-in-command principle, especially when deciding on even slightly significant terms of employment of an employee, the GDPR ensures the implementation of said principle. First of all, Article 22 of the GDPR gives individuals 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*". For the sake of clarity, the provision in question lays down a prohibition in principle, the infringement of which does not need to be invoked individually by a person subject to automated decision making (case C-634/21 of the Court of Justice of the European Union). Furthermore, said article is also applied if a human is not in fact involved in the decision making. In other words, because, taking into account the extremely wide concept of personal data as described in Article 4(1) of the GDPR, all AI systems (high-risk or not) always require more or less personal data in order to make automated decisions concerning the employees, Article 22 of the GDPR applies always to a situation where an AI system is producing legal or similar significant effect concerning the employee, including especially decisions altering the terms and conditions of the employee's employment, unless one of the exceptions mentioned below apply. For the sake of clarity, Article 22 of the GDPR also applies if the data used for automated decision-making does not consist purely of personal data (i.e., said automated decision-making can also include data not classified as personal data). It should also be noticed that the rules on high-risk AI systems or other provisions of the AI Act do not grant permission to violate this prohibition of the GDPR.

In the limited exceptions where said right provided by Article 22 of the GDPR does not apply – a) the (automated) decision is necessary for entering into, or performance of, a contract between the data subject and a data controller or b) is based on the data subject's (i.e., the employee's) explicit consent – the data controller (i.e., the employer) shall implement at least the employee's right to obtain human intervention on the part of the controller, to express their point of view, and to contest the decision. In other words, in these exceptional situations where Article 22 of the GDPR does not apply, the data controller (i.e., the employer) is forced to put a human in command if the data subject (i.e., the employee) so requires. Therefore, the employee always has a way to oppose automated decision making when the said exceptions of Article 22 apply. However, regarding explicit consent, the European Data Protection Board deems that, in principle, employees will not be in a position to freely provide consent to processing carried out by their employer, as employees may feel that they are unable to refuse their employer's request. In practice, this means that it is very difficult for employers to receive valid consent from an employee in the eyes of the GDPR which makes application of the said exception quite rare in the context of employment. In addition, a third exception to said right provided by Article 22 of the GDPR exists, i.e., the (automated) decision is authorised by EU 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. This exception does not include said right for human intervention. However, since the EU has not taken advantage of

said possibility, at least in connection with employment relationships, the exception is, therefore, not applicable to employees working in accordance with EU labour and employment regulation. In addition, if Member States have applied said exception (Finland at least has not), they still must lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests which sufficiently protects the employees. It should also be noted that the employees' right to access, rectify, and erase their data, as guaranteed by the GDPR, further strengthens the above-mentioned rights and provide additional protection also in this context.

In addition, according to the AI Act, employers must always inform employees and their representatives about applying a high-risk AI system to them before the system is being deployed. In addition, Articles 13(2)(f), 14(2)(g), and 15(1)(h) of the GDPR dictate that data subjects (i.e., employees) must be informed about the existence of automated decision-making, including profiling, and, at least in these cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. This means that employees cannot be unaware of the usage of such a system and the related logic and consequences (co-operation and related matters are further described below in Section 5. of this Annex). The AI Act also categorically denies both providers and deployers of any AI systems the possibility of deploying subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, meaning that employees can neither be tricked to make nor accept decisions that are contrary to their benefits by using such techniques.

Furthermore, according to Article 86 of the AI Act, any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 (i.e., AI systems related to critical infrastructure) thereof, and which produces legal effects (e.g., changes in the terms and conditions of employment) or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken. The said obligation applies only to the extent that the right referred to above is not otherwise provided for under Union law. The said article does not apply if it is specifically carved out in EU or national legislation but, however, there is no such EU legislation in the context of employment (or such national legislation in Finland either). Special attention should be paid to the fact that the said obligation activates in case the decision is made "*...on the basis of the output from a high-risk AI system listed in Annex III*" meaning that the mere usage of output of such AI system in the decision-making process is enough to trigger the application of Article 86.

In summary, it can be said that the current EU legal framework, while also ensuring the necessary transparency, accountability, and explainability, *de facto* robustly enforces the human-in-command principle, backed up by effective precautionary and ex-post safeguards that ensure that no AI system is able to make decisions of its own concerning changing terms and conditions of employment or other such major decisions related to employees, including recruiting, at very least if the employee opposes such process. In other words, these regulations effectively prevent employers from avoiding the application of the human-in-command principle and guarantee that, among others, no shift in the balance of power between the employer and the employees, change in job hierarchies, redefinition of tasks and roles, actions making

some job descriptions redundant and downgrading others, or blurring organisational boundaries (e.g., by facilitating subcontracting and outsourcing) is taking place because usage of an AI system. Simultaneously, the above-mentioned legislation also makes sure that employees are able to check decisions where an AI system is involved. In other words, the current EU legal framework concerning the above-mentioned matters needs no additional regulation.

4. Privacy of Employees

In addition to the deterioration of the terms and conditions of employment of the employees, the other most common fear related to the usage of AI systems is that their deployment in workplaces makes it possible to violate privacy of the employees in various ways (e.g., by allowing the employer to eavesdrop on private conversations between an employee and their family members at the employee's home or to collect data in a way that the employer knows the employee better than the employees themselves). However, the current EU legal framework prevents the actualisation of such fears in most effective ways.

As a general observation, AI systems that take advantage of personal data inevitably collect, process, and store personal data, or at least perform some of the above, which means, in practice, that the GDPR always applies too when AI systems are deployed in a workplace in a way that concerns employees. It should also be noted that the concept of personal data is extremely broad since it includes *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

First of all, processing of personal data is considered lawful only if and to the extent that at least one of the grounds mentioned in Article 6 of the GDPR applies. Furthermore, Article 5 of the GDPR specifically dictates that personal data must be *"...adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."* and that personal data shall be *"processed lawfully, fairly and in a transparent manner in relation to the data subject."* In addition to purpose specification requirement mentioned above, the GDPR also demands that personal data are not subsequently processed in a way incompatible with purposes in question. These obligations of the employer narrow significantly the collection, storage, and processing of personal data of employees. It should also be noted that the 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 is prohibited, unless one of the certain exceptions mentioned in Article 9(2) of the GDPR apply. However, in new Article 4a of the AI Act that came with the Omnibus, providers and deployers of high-risk and other AI systems are exceptionally granted a permit to process special categories of personal data to the extent that processing is strictly necessary to ensure bias detection and correction and all of the conditions and strict safeguards set out in said article are fulfilled. For the sake of clarity, the article in question does not create any obligation to conduct such bias detection and correction.

The transparency requirements of the GDPR apply to AI systems deployed in

workplaces as well. Employees thus have a right to know how personal data about them is collected, used or otherwise processed in connection with the usage of an AI system. The principle of transparency also requires that the data subject can easily find the information. These requirements also improve the lawfulness of data processing, as the controller (i.e., the employer) will also have to review its practices related to processing data when implementing said information obligation. In addition, independently of whether the personal data is collected by an AI system or not, the GDPR also imposes an obligation to the employer to make sure that personal data which are inaccurate or incorrect, having regard to the purposes of the processing, are erased or rectified without undue delay. Article 5 of the GDPR also requires that the retention period of personal data collected by the employers is as short as possible and that the employers remove or anonymise personal data that is no longer necessary. In addition, said provision of the GDPR requires that the personal data of employees is not modified without the knowledge of the controller and that the personal data must be protected against unlawful processing and accidental loss, destruction, or damage. As part of the protection from unlawful processing, access to personal data of the employees must be granted to those persons that actually need the personal data. Finally, the principle of fairness imposed in Article 5 of the GDPR stipulates that personal data collected from the employees is not misused and that it is not collected in secrecy from the employees.

The principles mentioned in Article 5 of the GDPR are also robustly enforced by the national supervision authorities meaning that they have true relevance. For example, in December 2023, the French Data Protection Authority ("**CNIL**") fined AMAZON FRANCE LOGISTIQUE EUR 32 million for setting up an excessively intrusive system for monitoring employee activity and performance. The CNIL found that AMAZON FRANCE LOGISTIQUE failed to comply with, among others, the data minimisation principle (Article 5 of the GDPR). The company used indicators on employee activity and performance, collected with the help of scanners, to manage stocks and orders in its warehouses in real time. However, the CNIL considered that providing assistance to an employee or reassigning them in real time does not require access to every detail of the employee's quality and productivity indicators collected using the scanners over the last month. Correspondingly, the CNIL found that the work schedule in the warehouses, along with the assessment and training of the employee do not require access to every detail of the data and statistical indicators provided by the scanner used by the employee and reported over the last month. The CNIL also considered that the "Stow Machine Gun" indicator, which signals an error when an employee scans an item "too quickly" (i.e., in less than 1.25 seconds after scanning a previous item); the "idle time" indicator, which signals periods of scanner downtime of ten minutes or more; and the "latency under ten minutes" indicator, which signals periods of scanner interruption between one and ten minutes, were illegal since they violated Article 6 of the GDPR (i.e., the company failed to ensure lawful processing). It is obvious that an algorithmic management system was deployed in the said warehouse. This case is a clear proof that national supervision authorities enforce the principles and other requirements of the GDPR also in connection with advanced technology in a way that prevents excessive monitoring of employees and violations of their privacy.

Controllers, including employers, must also be able to demonstrate that they comply with the above requirements. Controllers are also required to implement appropriate technical and organisational measures, including the necessary safeguards, to ensure and be able to demonstrate that the processing of employees' personal data is carried out in accordance with the above-mentioned obligations and the rest of the GDPR, as described in Articles 24, 25, and 32. Furthermore, where processing is to be carried out

on behalf of a controller, the controller shall only use processors which provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing complies with the requirements of the GDPR and ensures the protection of the rights of the data subjects, including employees.

In addition, where the nature of the processing, in particular in relation to the use of new technologies such as AI systems, is likely to result in a high risk to the rights and freedoms of natural persons, such as employees, the controller must, prior to processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Article 35 of the GDPR dictates that such a data protection impact assessment shall in particular be performed by the controllers in cases where a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the employees or similarly significantly affect the natural person. This means that a data impact assessment must always be carried out by the employer beforehand if they intend to deploy an AI system that performs the above-mentioned evaluation or decision making towards the employees. Correspondingly, a data impact assessment must always be performed before processing on a large scale of special categories of data referred to in Article 9(1) of the GDPR. This includes but is not limited to data concerning a natural person's health, sex life, sexual orientation, religious or philosophical beliefs, political opinions, or trade union membership. In other words, deployment of any such AI systems in a workplace that poses any realistic danger to the rights and freedoms of employees, requires conducting a data impact assessment before the processing of personal data, and consequently the deployment of an AI system performing such processing is done.

Said impact assessment must always include, at very least, i) a systematic description of the envisaged processing operations and the purposes of the processing, ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes, iii) an assessment of the risks to the rights and freedoms of data subjects, and iv) planned measures to address the risks to ensure the protection of personal data and demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other interested parties. If necessary, and at least if the risk related to the processing of personal data changes, the controller is also obligated to reassess whether the processing of personal data is performed in accordance with the data impact assessment. In addition, controllers that deploy a high-risk AI system must, if necessary, use the information given by the providers of high-risk AI systems stipulated in Article 13 of the AI Act in connection with performing the data impact assessment. Most importantly, the controller is obligated to consult the supervisory authority prior to processing where the said data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. Where the supervisory authority is of the opinion that the intended processing would infringe the GDPR, the supervisory authority may, among others, impose a temporary or definitive limitation (including a ban on processing) which would in practice prevent the usage of an AI system that does not comply with the GDPR.

Finally, the GDPR also grants data subjects, including employees, effective and robust rights related to their personal data. For example, employees have the right to access the personal data processed by their employer and, among others, have a right to know the purposes for the processing, a right to rectification and erasure of the personal data, a right to restrict its processing, and a right to portability. In addition,

as mentioned above in connection with Section 3. of this Annex, employees also have the right to oppose automated decision making, including profiling, in the event that automated decision making is exceptionally allowed by Article 22 of the GDPR. The GDPR also requires that the controller informs data subjects of their rights and facilitates the exercise of data subject rights.

Most importantly, as described in Articles 12-14, the GDPR also guarantees transparency for employees. Among others, said articles require that the employer provides employees with the information and communication required by the GDPR that relates to the processing of their data in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. This information includes always, among others, the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing, the possible recipients or categories of recipients of the personal data, and the fact that the controller intends to transfer personal data to a third country or international organisation, if any, and the existence of automated decision making and the logic, significance, and envisaged consequences related to such processing of personal data. Furthermore, if the data controller (i.e., employer) intends to further process personal data for a purpose other than that for which the personal data was originally collected, the data controller must inform the data subject (i.e., employee) of this other purpose prior to such further processing and provide all relevant additional information as stipulated by the GDPR.⁴

In addition, as stated above, all AI systems that are intended to be used to make decisions affecting terms of employment relationships, the promotion or termination of employment relationships, to allocate tasks based on individual behaviour or personal traits or characteristics, or to monitor and evaluate the performance and behaviour of employees, are classified as high-risk AI systems. Correspondingly, all AI systems that are remote biometric identification systems (with the exception of those that are intended to be used only for biometric verification of employees' identity), AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics, and AI systems that are intended to be used for emotion recognition, are classified as high-risk AI systems. For the sake of clarity, emotion recognition in a workplace is prohibited, unless it is intended to be used for medical or safety related purposes. This means, in practice, that all AI systems by which an employer may collect, process, or storage data of its employees, or at very least the vast majority of them, including all the most significant ones affecting to the employees, whether the data collected is classified as personal data or not, are classified as high-risk AI systems for which the AI Act stipulates the rigorous precautionary and ex-post control as described in Section 2. of this Annex. These include, among others, obligations concerning data and data governance, record keeping, transparency, human oversight, accuracy, and cybersecurity. These requirements determined in the AI Act also enhance the protection of the employees' privacy and related rights granted by the GDPR and especially blocks the unjustified surveillance of workers.

To summarise, the current EU legal framework effectively narrows down the collection, processing, and storage of personal data related to the employees to only what is absolutely necessary and simultaneously prevents violations of the employees' privacy, whether an AI system is deployed in a workplace or not. As described above, said legal framework prevents both disproportionate and undue surveillance at work and abuse of

⁴ Employers' obligations related to cooperation with the employees are described in Section 5. below.

data protection and privacy of employees by using an AI system in a way that guarantees the privacy of employees when they are not at work either. In other words, the current EU legal framework concerning the above-mentioned matters related to the employees' privacy needs no additional regulation.

5. Cooperation with Employees

The third major concern related to the use of AI systems in workplaces is that the employees do not have sufficient possibilities to participate in decision-making concerning the deployment of AI systems or the decision-making made by AI systems. However, as described below, the relevant EU legislation concerning cooperation with employees robustly guarantees that employees, if they so desire, are able to participate in the decision-making of the employer in an effective manner whether such decisions are related to AI systems.

Directive 2002/14/EC establishing a general framework for informing and consulting employees in the European Community ("**Information and Consultation of Employees Directive**") and Directive 98/59/EC on the approximation of the laws of the Member States relating to collective redundancies ("**Collective Redundancies Directive**") are technology-neutral and already adequately address the need for employee involvement in issues and consequences related to the use of AI systems in the workplace at EU level.

To be more specific, the Information and Consultation of Employees Directive improves social dialogue. It sets minimum principles, definitions, and arrangements for the information and consultation of employees at the enterprise level within each Member State. Given the range of industrial relations practices across the Member States, they enjoy substantial flexibility in applying the Directive's key concepts (e.g., employees' representatives, employer, employees) and implementing the arrangements for information and consultation, which can be considered the right solution for the reasons mentioned above. Management and labour play a key role in deciding these arrangements. Information and consultation are required on a) the recent and probable development of the undertaking's or the establishment's activities and economic situation; b) the situation, structure and probable development of employment within the undertaking or establishment and any anticipatory measures envisaged, in particular where there is a threat to employment; and c) decisions likely to lead to substantial changes in work organisation or in contractual relations. The directive also includes provisions on procedural manners, protection of the representatives of the employees, and adequate sanctions that guarantee that the objectives of the directive are reached. To avoid undue burdens on small and medium-sized enterprises, the directive applies only to undertakings employing at least 50 employees, or to establishments employing at least 20 employees, according to the choice made by the Member State.

The Collective Redundancies Directive includes similar provisions concerning situations where an employer is dismissing employees on grounds not related to them. In addition, Directive 2009/38/EC concerning European Works Councils ("**European Works Councils Directive**") strengthens the participation of employees in larger and multinational companies.

Furthermore, Article 35 of the GDPR requires that employers must hear employees or their representatives about intended processing activities of personal data and it makes

no exception in connection with AI systems processing personal data.

In addition, the **European Framework Directive on Safety and Health at Work** (Directive 89/391/EEC) obligates the employer to i) consult workers on the introduction of new technologies (such as AI systems); ii) designate worker(s) to carry out activities related to the protection and prevention of occupational risks; iii) inform and consult workers and allow them to take part in discussions on all questions relating to safety and health at work; and iv) ensure that each employee receives adequate safety and health training. As further described in Section 8., said directive also applies to risks related to mental health and such risks must be taken into account when the employer fulfils the above-mentioned cooperation obligations.

In summary, it is clear that the current EU legislation provides robust and comprehensive cooperation and participation mechanisms for employees in a way that guarantees significant opportunities for employee influence, independently whether these matters are related to usage or intended usage of AI systems or not. The above-mentioned obligations also heavily increase the transparency and information provided to employees, preventing the feared negative effects, if any, of deployment of an AI systems in a workplace, such as employees' loss of trust, job satisfaction, motivation, and autonomy. Briefly, the current EU legal framework concerning said rights of employees needs no additional regulation.

6. Ensuring that Employees are Equipped with the Necessary Skills

Another common fear related to the usage of AI systems in workplaces is that employers would not ensure that employees receive the necessary skills and knowledge for being able to operate in an environment that involves AI systems or that employees lose professional capacities in a way that paves the way to long-term unemployment. However, the current EU legal framework provides more than sufficient coverage for employees in this sense too.

Before the AI Omnibus, Article 4 of the AI Act stipulated that all *"Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used."* Further to this, the AI Act continues to define AI literacy as meaning *"skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause."*

In the recitals of the AI Act, this obligation is further elaborated: *"In order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems. Those notions may vary with regard to the relevant context and can include understanding the correct application of technical elements during the AI system's development phase, the measures to be applied during its use, the suitable ways in which to interpret the AI system's output, and, in the case of affected persons, the knowledge necessary to understand how decisions taken with the assistance of AI*

will have an impact on them. In the context of the application this Regulation, AI literacy should provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement."

However, in connection with the AI Omnibus, said obligation of Article 4 was specified and brought to more concrete level by replacing the providers' and deployers' above-mentioned obligation to "... take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons..." with an obligation to "... take measures to support the development of AI literacy of their staff and other persons...". Furthermore, it has been explicitly clarified that organizations are not required to guarantee a specific level of AI literacy to any individual. On the other hand, the Commission and Member States are now obligated to support and facilitate those efforts of providers and deployers of AI systems, including through offering training opportunities, providing informational resources, and allowing exchange of good practices and other initiatives. In addition, the European Artificial Intelligence Board shall issue recommendations to the Commission and the Member States based on the EU's competence frameworks to support their said objective. In other words, as a result of the Omnibus, responsibility for developing AI literacy is now partly transferred to the Commission, Member States, and the European Artificial Intelligence Board which can be deemed as a positive development giving the strategic importance of ensuring that EU citizens are equipped with the skills needed in the age of AI. In recitals of the updated version of Article 4 of the AI Act transferring some of the responsibility for development of AI literacy in the above-mentioned way was deemed necessary also due to an additional compliance burden the previous version of Article 4 produced, particularly for smaller enterprises.

Nevertheless, AI literacy remains an independent obligation in the AI Act, which underlines its importance. Organisations still remain obligated to take meaningful steps to promote AI literacy. This obligation applies to all organisations developing or using high-risk or other AI systems, including employers. Among many employers, said general obligation to take measures to support development of AI literacy means providing basic skills for all their staff. However, based on the AI Act, tailored supportive measures must also be provided on a role-specific basis (e.g., employees working in Human Resources if AI systems are used for recruitment). Supportive measures are also required on a project- and system-specific basis for all those employees who need to use a particular AI system. When designing training and other supportive measures, employers are obligated to assess the needs in terms of the employer's industry, the technical skills, education, and experience of its employees, the AI systems used by the employer, and the risks and impacts associated with them. In other words, the AI Act especially takes into account employees that are in vulnerable position (e.g., elderly employees and employees who do not have technical training or experience).

In summary, Article 4 of the AI Act itself causes that employees are provided with the necessary skills and knowledge required in order for them to flourish in workplaces in which AI systems are deployed. In other words, the current EU legal framework ensures in a sufficient manner and in a way that supports long-term, internal, and external employability that employees are proficient in operating within environments that include AI systems, do not lose their autonomy, and can adapt to changes while paying special attention to vulnerable workers. Said legal framework also ensures that, to the extent necessary, all employees, and especially employees who perform the human oversight of high-risk AI systems (Articles 14 and 26 of the AI Act themselves guarantee this), are equipped to understand the AI systems that they are

working with or that they are subject to, the AI systems' purpose, how the AI systems function, and how they can control it, as well as the AI systems' capabilities and limitations. The above-mentioned obligations of the employer also simultaneously increase the transparency of AI systems and measures related to them. In addition, it should be noted that employers have particularly strong incentives to train employees to use the AI systems that they have been provided with in the best possible way because otherwise the employers won't receive the maximum of the benefits that the AI systems are offering. Furthermore, in practice, complying with the AI Act is not possible without organisation-wide AI literacy. Briefly, the current EU legal framework concerning the above-mentioned matters needs no additional regulation.

7. Equality of Employees

The deployment of AI systems in workplaces has also raised concerns whether the equal treatment of employees is endangered. In particular, there are concerns whether different minorities among employees may face discrimination and other adverse consequences due to the usage of AI systems. However, the current EU legal framework effectively prevents these concerns from becoming reality.

First of all, the AI Act specifically prohibits the usage of AI systems that exploit any of the vulnerabilities of a natural person or a specific group of persons (i.e., including employees and groups of employees belonging to a certain minority group), due to their age, disability, or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm. In addition, the AI Act also prohibits the deployment of such biometric categorisation systems in workplaces that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation. This provision of the AI Act also helps to prevent privacy violations of the employees' privacy. In addition, in connection with all high-risk AI systems (that encompass all AI systems making decisions that affect to the terms and conditions of the employees as described in Section 3. of this Annex) all deployers (e.g., employers) must, to the extent the deployer exercises control over the input data, ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system.

In addition, providers of high-risk AI systems must ensure that among the used data sets it is taken into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural, or functional setting within which the high-risk AI system is intended to be used. In addition, providers of high-risk AI systems must, among others, apply the following appropriate data governance and management measures to the training, validation and testing data: a) an examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under EU law, especially where data outputs influence inputs for future operations; and b) appropriate measures to detect, prevent, and mitigate possible biases identified in connection with the above-mentioned examination. Providers must also develop high-risk AI systems in a way that the person(s) responsible for human oversight are capable to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system, in particular for high-risk AI systems used to provide information or

recommendations for decisions to be taken by natural persons. Finally, the AI Act also demands that providers of such high-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures. Therefore, these provisions of the AI Act effectively prevent that AI systems would make discriminatory decisions concerning employees due to their sex, age, religion, or other such discriminatory grounds because of the input data or because it is not processed in a way that filters said biases. Most importantly, when making decisions concerning the terms and conditions of employment of employees, a human is always *de facto* in control as described in Section 3. of this Annex which also effectively prevents discrimination of employees.

Said protection against discrimination of employees is further robustly strengthened by Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin ("**Anti-Racism Directive**"), Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation ("**Equality Directive**"), and Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation ("**Equal Treatment Directive**") that are all technology neutral and effectively protect employees against the risks of discrimination associated with the use of AI systems in the workplace at EU level.

To be more specific, the Equality Directive sets up a general framework for equal treatment in employment and occupation. To this end, it prohibits direct and indirect discrimination (including harassment and instructions to discriminate) based on religion or belief, age, disability, and sexual orientation in the field of employment and occupation. In particular, the directive lays down minimum requirements prohibiting discrimination in: i) conditions for access to employment, to self-employment or to occupation, including selection criteria and recruitment conditions, whatever the branch of activity and at all levels of the professional hierarchy, including promotion; ii) access to all types and to all levels of vocational guidance, vocational training, advanced vocational training and retraining, including practical work experience; iii) employment and working conditions, including pay and dismissals; and iv) membership of, and involvement in, an organisation of workers or employers or any organisation whose members carry on a particular profession including the benefits provided for by such organisations. The Equality Directive also includes provisions concerning victimisation and revised burden of proof. This directive is complemented by the Anti-Racism Directive which establishes a framework for equal treatment irrespective of racial or ethnic origin in employment and occupation, among other areas. It correspondingly forbids both direct and indirect discrimination, harassment, instructions to discriminate, and victimisation and includes the requirement of revised burden of proof. A corresponding level of protection against direct and indirect discrimination, harassment, and sexual harassment based on gender is offered by the Equal Treatment Directive of 2006.

In summary, the current EU legal framework robustly prevents and prohibits discriminatory treatments on the basis of biased algorithms of AI systems and it also compels employers to ensure that data sets that are fed into the algorithms of AI systems are complete and to a maximum extent unbiased. Generally speaking, the current EU legal framework also effectively prevents, among others, direct and indirect discrimination and instructions to discriminate done by or executed with an AI system.

In addition, the current EU legal framework guarantees that a human is *de facto* in control in connection with making decisions concerning the terms and conditions of employees which also provides the same level protection against discrimination and unequal treatment as if AI systems were not deployed. Therefore, the current EU legal framework concerning the above-mentioned matters needs no additional regulation.

8. Health and Safety of Employees

Concerns have also been raised about the impact of the use of AI systems on the physical and psychological safety and health of employees, particularly in terms of excessive workload on workers. However, the current EU legal framework already protects employees from such dangers in most effectively way.

There are numerous general and sector specific EU directives that provide sufficient coverage for employees also on matters related to occupational health and safety in connection with the usage of AI systems, including the **Working Time Directive** (Directive 2003/88/EC) and the European Framework Directive on Safety and Health at Work (Directive 89/391 EEC) that are technology neutral and sufficiently prevent psychosocial hazards as well at EU level.⁵

One of the common fears of deployment of AI systems in workplaces is that the employees would work longer days due to usage of such systems (e.g., because the AI systems allocate tasks in a way that requires employees to work extra hours). However, the Working Time Directive imposes strict obligations concerning, among others, daily and weekly rest periods, breaks during the working day, maximum amount of work per week (including overtime), and night work. These obligations also automatically limit the amount of daily work at EU level. In addition, the employees are entitled to and compelled to have annual holiday as determined by said directive.

In connection with doubts related to the health and safety of the employees, it should be remembered that the AI Act especially pays attention to health and safety in addition to fundamental rights as described in Section 2. of this Annex.

Furthermore, the European Framework Directive on Safety and Health at Work determines that it is the employer's obligation to ensure the safety and health of employees in every aspect related to work and the employer may not impose financial costs to the employees to achieve this aim. Alike, where an employer enlists competent external services or persons, this shall not discharge the employer from its responsibilities in this area. The general principles of prevention listed in the directive are the following: 1) avoiding risks; 2) evaluating the risks; 3) combating the risks at source; 4) adapting the work to the individual; 5) adapting to technical progress (such as AI systems); 6) replacing the dangerous by the non- or the less dangerous; 7) developing a coherent overall prevention policy; 8) prioritising collective protective measures (over individual protective measures) and 9) giving appropriate instructions to employees.

Based on the directive, the employer is obligated to: a) evaluate all the risks to the safety and health of employees, inter alia in the choice of work equipment, the

⁵ For a complete list, please see the following website of the European Agency for Safety and Health at Work: <https://osha.europa.eu/en/safety-and-health-legislation/european-directives>.

chemical substances or preparations used, and the fitting-out of work places; b) implement measures which assure an improvement in the level of protection afforded to employees and are integrated into all the activities of the undertaking and/or establishment at all hierarchical levels; c) take into consideration the employee's capabilities as regards health and safety when they entrust tasks to workers; d) consult employees on introduction of new technologies (such as AI systems); e) designate worker(s) to carry out activities related to the protection and prevention of occupational risks; f) take the necessary measures for first aid, fire-fighting, evacuation of workers and action required in the event of serious and imminent danger; g) keep a list of occupational accidents and draw up and draw up, for the responsible authorities reports on occupational accidents suffered by his workers; h) inform and consult employees and allow them to take part in discussions on all questions relating to safety and health at work; and i) ensure that each employee receives adequate safety and health training. For the sake of clarity, since said directive is technology neutral, employers are compelled to take into account the usage of AI systems in connection with all the above-mentioned obligations of the directive.

It should especially be noted that the European Framework Directive on Safety and Health at Work requires employers to adapt the work to the individual, especially as regards the design of work places, the choice of work equipment, and the choice of working and production methods, with a view, in particular, to alleviating monotonous work and work at a predetermined work-rate, developing a coherent overall prevention policy which covers technology (such as AI systems), organisation of work, working conditions, social relationships and the influence of factors related to the working environment (taking into account the psychosocial work environment). The interpretative document on the implementation of Council Directive 89/391/EEC in relation to mental health in the workplace provides further explanation on the Framework Directive and states that all obligations also apply to the prevention of risks in relation to mental health in the workplace, including conducting psychosocial risk assessments and taking appropriate prevention measures to reduce work-related stress

To summarise, the current EU legal framework effectively forces the employers to take care of the employees' health, safety, capacity to work, and wellbeing also when AI systems are deployed in a workplace. The said legal framework also effectively takes into account and prevents all possible hazards, whether physical or mental, associated to the usage of AI systems in workplaces, such as the employees' excessive workload, stress, insecurity, depression, and anxiety in sufficient way. In other words, the current EU legal framework needs no additional regulation concerning the health and safety of the employees.

Inquiries to the Author:

Ville Leppäniemi (Legal Advisor)

Tel. +358 40 084 1913 / ville.leppaniemi@teknologiateollisuus.fi

Inquiries for EU Policy Questions:

Anna Ranki (Director, Public Affairs)

Tel. +358 50 383 8797 / anna.ranki@teknologiateollisuus.fi

EU Transparency Register ID: 39705603497-38

Technology Industries of Finland (TIF) represents Finnish technology industries and counts over 1,800 member companies, ranging from SMEs and start-ups to world leading MNEs. The technology industry is comprised of five subsectors: electronics and the electrotechnical industry, mechanical engineering, the metals industry, consulting engineering, and information technology. Technology industry is the most important export industry of Finland, with operations constituting over 50 % of all Finnish exports and accounting for 70 % of all private investments in research and development.