45th Closed Session of the Global Privacy Assembly

October 2023

Resolution on Artificial Intelligence and Employment

This Resolution is submitted by the sponsors on behalf of the Working Group on Ethics and Data Protection in Artificial Intelligence.

SPONSORS:

- Information Commissioner's Office (ICO), United Kingdom
- Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI), Germany
- Data Protection Authority (Garante per la protezione dei Dati Personali - GPDP), Italy

CO-SPONSORS

- The Federal Data Protection and Information Commissioner (FDPIC), Switzerland
- National Data Protection Commission (Commission Nationale de l'Informatique et des Libertés – CNIL), France
- Data Protection Authority (Unidad Reguladora de Control y Actos Personales – URCDP), Uruguay
- National Institute for Transparency, Access to Information and Personal Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales – INAI), Mexico
- Data Protection Authority of Québec (Commission d'accès à l'information du Québec), Canada
- Information and Privacy Commissioner of Ontario, Canada
- Office of the Information and Privacy Commissioner for British Columbia, Canada
- Office of the Privacy Commissioner of Canada
- Council of Europe
- Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong, China
- National Commission for the Protection of Personal Data Protection (Commission Nationale de Contrôle de Protection des Données à Caractère Personnel – CNDP), Morocco
- European Data Protection Supervisor

The 45th Annual Closed Session of the Global Privacy Assembly:

Noting that employment activities may involve the search for and recruitment of candidates, the entering into an employment agreement between the employer and employee, the monitoring and management of employees' performance, development and behaviour in the workplace by the employer, and the termination of an employment relationship, and may include the recruitment and management of gig workers, contractual employees, trade unions, as well as taking care of health and safety at work and compliance with labour and social protection requirements;

Recalling the Declaration on Ethics and Data Protection in Artificial Intelligence made by the 40th International Conference of the Data Protection and Privacy Commissioners on 23 October 2018, and the Resolution on Accountability in the Development and Use of Artificial Intelligence adopted at the 42nd closed session of the GPA conference;

Acknowledging the potential efficiencies and benefits to the scale of operations that the use of Artificial Intelligence (AI) can bring to decision-making across the employment lifecycle, which organisations are exploring in various employer-driven activities, including but not limited to the initial search and screening of prospective job candidates, employee monitoring and management;

Highlighting that AI used in an employment context may pose a high risk to individuals,[1] groups, representatives of workers (such as trade unions), communities and organisations. When that use is opaque, misapplied, incorrectly designed or inappropriately relied upon it may lead to harms or infringement of fundamental rights and freedoms, including privacy, human dignity, equality of rights such as unfair discrimination. This may significantly impact a worker's personal and professional development and result in the denial of equality of opportunity to access employment due to the use of biased historical data to train some AI tools or the use of inappropriate or unlawful parameters or values in the AI system;

Highlighting further risks such as the disproportionate or unauthorised collection of personal data to make solely automated or AI-assisted decisions about the performance of an employee or the allocation of work or any other decisions such that may also affect the rights of persons. These include but are not limited to:

- the right to private and family life (for example if AI systems are used to monitor homeworkers or entail excessive micro-management of workers and surveillance in the workplace)
- adversely affect health and wellbeing,
- the freedom of assembly and association (for example if trade union membership data or inferences are used to the detriment of employees or candidates)
- the ability of an individual to exercise their right to not be subjected to a decision based solely or partially on automated decision making or to exercise other individual rights to privacy or data protection, and
- the infringement of individual rights to information and data protection, for instance when there is a lack of transparency, which means that the candidates or employees are not aware of the fact that AI is being used and/or of the extent of its use;

Reinforcing the importance of transparency to ensure employees and unions are informed about the use of AI systems in the workplace before their introduction, providing sufficient detail to enable these employees and unions to understand their purpose, how they work, and the metrics used;

Emphasising that AI systems used by organizations for employment purposes must be explainable in a manner that is comprehensible to those subject to decisions made solely or with assistance by those systems, as well as those utilising the AI systems. Organizations deploying such systems, as a core part of their accountability responsibilities as well as of their obligations under the applicable labour, social protection, health and safety law, should provide for such explainability and mechanisms, as may be detailed in a dedicated organisational policy for the use of AI. Employees, candidates or workers should be able to understand the logic of the decision-making process through these mechanisms and

[1] Risk can be assessed in reference to tools such as the Artificial Intelligence Risk Management Framework released by the US National Institute of Standards and Technology earlier this year, and the ISO/IEC 23894:2023 Guidance on risk management for AI, among others. See also the Global Privacy Assembly AI Working Group's Risks for Rights and Freedoms of Individuals Posed by Artificial Intelligence Systems – Proposal for a General Risk Management Framework.

policies, as well as seek help and redress in cases where, for example, issues regarding discrimination, bias and opacity are observed;

Noting that most AI applications developed for or deployed in an employment context will process personal data in the development or in the deployment phase. While the sources, distribution and nature of the data processed in those different stages may differ, all phases of such AI in the employment life cycle are in most cases bound to engage data protection, privacy and labour rights considerations;

Concerned that the use of AI in employment may entail high data protection and privacy risks that may impact on, inter alia, recruitment and monitoring of workers. Those risks may include, inter alia:

- a lack of transparency
- presence of bias-led discriminatory patterns
- lack of consideration over the necessity and proportionality of using AI in the specific employment context
- lack of meaningful human intervention
- lack of adequate training and relevant expertise in operating AI systems and navigating high-risk decision-making in the employment ecosystem
- lack of valid general or employment specific legal basis
- individuals' loss of control over the collection and processing of their personal data
- difficulties faced by employees in exercising their data rights
- lack of specific safeguards
- poor data security
- function creep
- the processing of sensitive data such as health or biometric data without respect for the proportionality principle or for human dignity;

Highlighting that the use of AI systems to infer emotions of a natural person[2], and more generally any form of 'biometric categorisation', is high risk and should in most cases be prohibited in the employment context, and if used in limited and defined cases must be subject to appropriate safeguards including robust testing and/or other assessments to ensure that such systems use valid and reliable methodologies and operate as intended;

Emphasising that as organisations in the private and public sectors more frequently rely on AI in the employment context, and that AI systems and services may be provided remotely and across borders, it is important for data protection and privacy authorities, together with the competent labour and health and safety authorities, to gain insight in terms of where AI systems derive their training data from, how their development and operation complies with domestic legal frameworks and how employees' data protection and privacy rights are impacted both domestically and internationally;

Noting the important contributions of data protection and privacy authorities, governments and international bodies to the global debate through publication of laws, policy and guidance documents;

Recognising that different uses and applications of AI in employment pose different types and levels of risk and therefore require careful consideration through their deployment and lifecycle in order to identify appropriate safeguards in each context and use;

[2] For instance in the case of emotion recognition systems used at a workplace to monitor the mood of employees.

Recalling that the Global Privacy Assembly has previously identified the need to work towards global policy, standards and models and to ensure greater levels of regulatory cooperation to enhance the efficient prevention, detection, deterrence and remedy of data protection and privacy issues and to ensure consistency and predictability in the system of oversight in the data-driven economy;

Affirming the need for data protection and privacy enforcement authorities to coordinate their efforts, together with the competent labour and health and safety authorities, to influence the development and implementation of those data protection and privacy approaches across the globe, and to take action where appropriate; and

Reaffirming the Resolution on Privacy by Design adopted by the 32nd Conference in 2010 in Jerusalem, the Resolution on Profiling adopted by the 35th Conference in 2013 in Warsaw, the Resolution on Big Data adopted by the 36th Conference in 2014 in Fort Balaclava, the Declaration on Ethics and Data Protection in AI adopted by the 40th Global Privacy Assembly in 2018 in Brussels, and the Resolution on Accountability in the Development and Use of AI adopted by the 42nd Global Privacy Assembly in 2020 online.

Therefore the 45th Global Privacy Assembly underlines the importance of:

1. Ensuring the use of AI systems in an employment context is human-centric.
2. The principles of data protection and privacy by design and default in the development of AI tools for deployment in employment contexts, including but not limited to employees, contractual workers, union workers, daily wage workers, and gig workers, recognising the impact that AI systems may have on their personal and professional lives;
3. Recognizing the importance of having an adequate legal basis for the processing of personal data in all phases of the AI lifecycle, and the limitations of consent as a lawful basis in the employment context given potential power imbalances between a candidate or employee and the employer;
4. Detailing adequate safeguards to avoid disproportionate workers' surveillance in breach of the privacy and dignity of the employees when processing their personal data for the relevant purpose of the work to be performed, including the participation of trade unions in decisions on AI work management;
5. The need for full compliance of the development and deployment of AI systems in employment with applicable data protection laws and principles such as necessity, proportionality, data minimisation, purpose specification and limitation, and the right not to be subject to a decision based solely or primarily on automated means, as well as with relevant labour regulations and any other regulations, such as established human rights frameworks, which may hold relevance in a specific context including but not limited to the principles referenced in this resolution;
6. Lawfulness, fairness and transparency in relation to how personal data is processed, including the development, deployment and outcome of that AI related processing, which involves, inter alia, an obligation on the employer to provide an employee – the subject of an AI assisted decision where algorithmic or AI systems are deployed in the employment context with regard to the jurisdiction-specific regulatory frameworks – and the union before deployment of any AI systems with detailed information about the use and functioning of such systems that determine, for instance, a candidate's or employee's ranking, assignment of tasks, management or dismissal, as well as the supervision, evaluation and performance of the employee's contractual obligations, without prejudice to workers' rights for instance to

receive employment-related information, to contest and seek redress for unlawful evaluation of performance, underpayments, and unlawful dismissal;

7. The right of a candidate or employee that is subject to an AI-assisted decision to access information about what data is held about them by an employer and how their personal data is used in connection with such an AI-assisted decision, as well as information about the data that is inferred and the profiles that are built using these AI systems;
8. Explainability of the AI system used at any stage of the employment lifecycle to ensure that employees, candidates or workers impacted by the output of such a system, as well as the employers deploying the AI system, understand the decision made with the AI system and can access that explanation in a straightforward and timely manner, and that the explanation for employees, candidates or workers includes intelligible information about the logic involved, the significance and the envisaged consequences of the use of the AI system, both in general and in the employee's specific case, to ensure that they can lodge informed complaints and exercise their right to redress in accordance with the applicable domestic legal framework;
9. The ability of the data subject affected by an AI system used by an employer at any stage in the employment lifecycle to obtain recorded, meaningful human review of employment decisions made using AI systems, to express his or her point of view and to contest relevant automated or AI-based decisions or to request an independent audit of an AI system used by the employer or any general requirement of third-party auditing;
10. Training users of AI tools, including those who provide human review of AI-assisted decisions, to ensure that those decisions are not subject to automation bias that could lead to excessive trust in AI tools, and that the users of AI tools have the requisite expertise, experience and technical qualifications and consider the risk levels of the task being influenced by the output of the AI system, and tracking or monitoring the use of the AI tools to determine whether such training is effective;
11. Accountability as a principle, requiring that organisations and employers take into account, mitigate and, where necessary, prevent the risks to the rights and freedoms of candidates, employees and workers arising from using AI to process personal data (for instance, the right to association, and to organise in a trade union, which may be hindered by undue monitoring of workers' activities), and demonstrate they have done so;
12. Organisational policies that support pre-deployment AI impact assessments having regard to all reasonably foreseeable risks for candidates, employees and workers stemming from the use of the AI system at the workplace, accreditation or certification of AI systems, AI-specific risk identification and outline whistleblowing and redress mechanisms for AI systems used during the employment lifecycle, also as a means to facilitate oversight by the competent authorities;
13. Reducing and mitigating biases or discrimination, both direct and indirect, when developing and deploying an AI system in the employment context, including by taking reasonable steps to ensure personal data used in the training of a system and in solely automated decision making is representative to the context in which the system will be used, accurate and regularly updated, and implementing appropriate technical and organisational measures to ensure, in particular, that factors in recruitment and work management systems which result in inaccuracies in personal data are corrected and the risk of errors is minimised, as well as compliance with the applicable domestic laws; and

The 45th Global Privacy Assembly resolves to:

1. Urge organisations that develop or use AI systems for use in the employment context to take into account the considerations outlined in this resolution;
2. Call upon all members of the Global Privacy Assembly to work with organisations that develop or use AI systems for use in the employment context in their jurisdictions and globally to help them incorporate the considerations outlined in this resolution;
3. Update, when appropriate, the results of the survey of the Working Group on Ethics and Data Protection in Artificial Intelligence (see the survey report in the Explanatory Note below) in case of possible changes in the legal or technical landscape of the use of AI in employment.

Explanatory note

The GLOBAL PRIVACY ASSEMBLY WORKING GROUP ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE conducted a survey in May to July 2022 to collect the opinions of the members of the Global Privacy Assembly on key risks and enforcement action members have taken in relation to the use of AI in employment. The report is below.

1. Introduction

The last several years has seen a proliferation in the use of artificial intelligence (AI) in employment, including the use of AI in recruitment, in the workplace, and post-employment. AI is an umbrella term for a range of technologies and approaches that often attempt to mimic human thought to solve complex tasks.[3] The term "AI" is often used to describe all kinds of algorithmic tools on the market without a definition, which can lead to "AI washing". From a data protection perspective, it is important to distinguish between the conception or training phase and the application or deployment phase of AI in the employment context. Most AI applications in the employment context will use personal data in both phases, which therefore means that data protection and privacy considerations will apply. These considerations include, among others, transparency issues including the accuracy of data about employees, workers and candidates, questions around ensuring the rights of data subjects and relevant safeguards, the presence of bias and discrimination, the legal bases or the degree of meaningful human intervention, as well as proportionality, trust and fairness.

In 2018, it was reported that Amazon had scrapped an artificial intelligence-powered recruiting tool it was using following evidence that it showed bias against women. The tool was designed to assess and score job applications. However, it was alleged that the AI system penalised applications that included the word 'women's' as in 'women's chess club captain' and downgraded graduates of two all-women's colleges. This was one of the first publicised instances which showed not only that artificial intelligence (AI) was being used to make significant decisions in an employment context, but that it was leading to unjustified harm for individuals.

Since then, there have been more high-profile cases where AI has been used in an employment context, which has resulted in potential harm for individuals. Some examples include:

- A Dutch Court ruling about whether the deactivating of some Uber drivers' licences constituted a solely automated decision with legal or similarly significant effects in the sense of Article 22 of the GDPR and whether meaningful information about the logic involved to make the decision was provided to drivers.[4]
- The Italian Supervisory Authority (Garante) fined food delivery companies for breaching the data protection principles of transparency, security, privacy by design and default and not implementing suitable measures to safeguard its employees' right and freedoms against discriminatory automated decision making when using an automated scoring system to assign delivery slots to riders. This excluded some riders from work opportunities.[5]

Lawmakers and regulators have started to address the potential harms that can be caused by the use of AI in an employment context. For example, the European Commission has proposed treating the use of AI for recruitment as well as for decisions concerning workplace performance and task

[3] Guidance - Part 1 The basics of explaining AI (ico.org.uk)
[4] Dutch court rulings break new ground on gig worker data rights | Financial Times (ft.com)
[5] See the abstract of the Italian SA's order at https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677611; another decision is published at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.

allocation as high-risk; moreover, a proposal concerning digital platform workers is being negotiated.[6] This would mean that employers will have to comply with further requirements in the AI Act compared to other users of AI systems that are not regarded as high risk. The Information Commissioner's Office (ICO) – the data protection authority for the United Kingdom – has committed to investigating concerns over the use of algorithms to sift recruitment applications, which could be negatively impacting employment opportunities of those from diverse backgrounds.

Many applications of AI used in an employment context will have implications for data protection and privacy. For example:

- Will an AI-derived decision about whether job applicants are successful or unsuccessful be explainable to those affected?
- Will an AI system designed for one purpose (eg to increase safety of employees in the workplace) be used for a separate and incompatible purpose (eg to score the productivity of workers)?
- Can an AI system's decision to dismiss an employee ever be considered fair?

In 2022, the Global Privacy Assembly (GPA), led by the ICO and Germany's BfDI, ran a survey of its members to understand global perspectives on the data protection and privacy implications caused by AI in an employment context. The goals of the survey were:

- To identify key policy and legal issues in relation to the development and use of AI in the employment context, including recruitment, that are important for data protection and privacy authorities around the world.
- To assemble and maintain an international repository of real-life cases of applications of AI technology in the workplace, which are relevant for consideration of privacy, data protection, and AI ethics more broadly.
- To inform the development and promotion of a set of principles and expectations for the use of AI and personal information in the workplace.
- To consider and discuss possible courses of action.

The survey asked about data protection authorities' existing policy positions and guidelines on the use of personal data and AI in the workplace (question 1), information about any enforcement action or investigation into the use of personal data and AI in the workplace (question 2), to what extent members engaged with stakeholders on the subject and what they considered the riskiest purposes of AI in the workplace to be (questions 3 and 4), what they considered to be the greatest privacy and data protection risks (question 5), as well as what an effective regulatory framework would look like (question 6). Finally, the survey asked for examples of uses of AI in the workplace (question 7) and broader areas of impact (question 8).

The survey ran from 11 to 25 May 2022 with the questions being disseminated via email by the GPA secretariat for the Working Group on Ethics and Data Protection in Artificial Intelligence, accompanied by an introductory note. To maximise the number of responses, the survey was sent to all members of the GPA more broadly, rather than to only members part of the Working Group on Ethics and Data Protection in Artificial Intelligence. In total, 29 responses from GPA members were received. The majority of responses came from authorities geographically based in Europe (20/29), followed by Asia and Australia (6/29), North America (1/29), and Central and South America (2/29).

2. Results

[6] Digital platform workers: EU rules one step closer (europa.eu)

The survey resulted in a variety of responses from data protection and privacy authorities. The questions and a summary of the answers received are presented below.

Question one: Has your authority developed any public facing policy positions or guidance on the use of personal data and AI in the workplace?

In total, eight survey respondents answered 'yes' to this question. Additional information that was provided with this question illustrated a range of different publications. For example, some publications focused on the general risks that using AI raises, some on the general risks that processing personal data in the context of the workplace brings, and finally, there were several examples which focused on the use of personal data and AI in the workplace. For example, one response highlighted the considerations required when trying to reconcile the data protection principle of data minimisation with the fairness principle when the method of detecting and countering discrimination requires processing more personal data.

Question two: Has your authority, or other legal or judicial bodies in your jurisdiction, investigated or taken formal regulatory, enforcement or legal action, for any use of personal data and AI in the workplace?

Eight survey respondents answered 'yes' to this question. Examples of issues that were included in these answers were:

- Investigations into online food delivery companies and how they use AI to process personal data of drivers;
- The processing of employee's personal data via advanced data mining techniques for the purposes of identifying possible unjustified sick leave;
- The use of algorithm-based decision-making to decide allocation of teaching positions in schools;
- The use of automatic voice and image analysis during video interviews as part of a job application process;
- The use of biometrics in the workplace; and
- Using AI to analyse data and predict the likelihood of a job applicant declining a job offer.

Question three: Has your authority engaged with any regional, national, or international external stakeholders in developing its policy positions and guidance or progressing regulatory action on the use of AI in the workplace (e.g. industry, trade unions, civil society, lawmakers)?

11 respondents answered 'yes'. Engagement included in international fora such as the Council of Europe's Ad Hoc Committee on Artificial Intelligence, the OECD and the Global Partnership on AI, with other national authorities and regulators, businesses and industry bodies, research institutions, trade unions, civil society, and national government departments and ministries.

Question four: From the list of use cases below, which uses of AI in the workplace do you consider pose the greatest privacy and data protection risks?

- **Hiring purposes (eg, CV scraping, gamified assessments, automated interviews, etc.)**
- **Work management purposes (eg holiday allocation, absence management, task and shift allocation, etc.)**
- **Monitoring purposes (eg identity verification, tracking systems, desktop monitoring, etc.)**
- **Other (Please state)**

Respondents were able to choose multiple answers, with many selecting two or three, some choosing only one, and a couple choosing to refrain from answering. Data protection authorities considered AI

being used for monitoring purposes as posing the greatest privacy and data protection risks, followed closely by AI being used for hiring purposes. Some respondents that selected 'Other' considered that all three uses posed a similar level of risk.

In addition, fourteen respondents stated other purposes and/or added additional content in their response. These included that the risks depended on the extent of the infringement of individuals' data subjects' privacy rights and freedoms, rather than the specific scenario in the employment context or a specific purpose. Some attributed a high risk to permanent surveillance with AI facial recognition technologies, particularly around the inclusion of sensitive data such as biometrics, such as for identification purposes or automated employee profiling. There was concern around the lack of scientific proof of claims and promises made by the sellers of such tools, including character and performance predictions of candidates that are not based on quality controlled, scientific methods. Often, respondents found that training datasets are not obtained and processed in a data protection compliant way. They also mentioned concerns around the governance and security of data bases as sources for the data AI collects. Further, respondents stressed that in addition to a concrete risk assessment there must be a valid legal basis, and data protection principles must be respected in any case (i.e. data minimisation, transparency, fairness/anti-discrimination, and the need for the use of AI in the workplace to be proportionate in relation to the concrete purpose, etc.). Respondents also mentioned the necessity for specific safeguards.

Question five: For the use case(s) identified in question four, please select what you consider to be the three most significant privacy and data protection risks.

- **Lack of transparency regarding data collection, including lack of provision of information to individuals.**
- **Large-scale collection of special categories of data.**
- **Bias and discrimination against certain demographics.**
- **Poor data security, including potential breaches of confidentiality.**
- **Function creep (further use of an AI system in the workplace for new, potentially less compelling, purposes).**
- **Individuals' loss of control over collection and processing of data.**
- **Lack of valid legal basis for the processing.**
- **Difficulty for individuals in exercising their data rights.**
- **Lack of specific laws governing use of AI in the workplace.**
- **Lack of consideration over the necessity and proportionality of using AI in the workplace.**
- **Lack of meaningful human intervention for decisions made which have legal or significantly similar effect(s) on individuals.**
- **Broader human rights implications as set out in international instruments such as the International Covenant on Economic, Social and Cultural Rights or domestic law, including the right of freedom of assembly and association.**
- **Other (please specify).**

A lack of transparency was considered by most data protection authorities to constitute the greatest data protection and privacy risk (15 respondents). This was followed by bias and discrimination (10 respondents), lack of consideration over the necessity and proportionality of using AI in the workplace (9 respondents), and lack of meaningful human intervention (8 respondents). Some respondents also selected "lack of valid legal basis" (6 respondents) and "lack of specific laws governing use of AI in the workplace" (5 respondents). Others selected the difficulty for individuals in exercising their data rights (3 respondents) and individuals' loss of control over collection and processing of data (5 respondents).

Poor data security (5) and function creep (4) were also mentioned by several respondents. The risk of large-scale collection of special categories of data was mentioned once. None of the respondents selected 'broader human rights implications'.

Question six: What would an effective regulatory framework for AI in the workplace look like?

Respondents offered a variety of suggestions about what an effective regulatory framework for AI in the workplace would look like. Many authorities (18) suggested new legal regulation or pointed out existing or future legal initiatives in their countries/continents applicable to AI in the employment context. Several authorities (10) additionally or exclusively suggested soft law such as guidelines or education. Some indicative and non-exhaustive suggestions provided were:

- Specific legal **regulation for the use of AI in the workplace**, including, for example, definitions, risk classifications, data protection by design and default, restrictions on the development and/or use of AI in the workplace, such as purpose limitation.
- Ensuring that AI systems used for significant workplace decisions are **explainable**.
- Organisations should be transparent and accountable about their use of AI in the workplace to enable individuals to exercise meaningful choice and control in relation to their personal data.
- Requirements that AI systems and their use by employers are subject to third-party **auditing or another form of external scrutiny, including before deployment**.
- Ensure a regulatory framework for AI in the workplace is consistent and compatible with **labour law and labour agreements**.
- The ability for **workers' representatives to request information** on algorithmic systems.
- **Adherence to article 22 of the GDPR where it applies or similar restrictions** on automated decision-making in the employment context
- Classifying certain uses of AI in employment as high risk, and banning certain systems where there is unmitigated high risk such as unfair bias and discrimination, to ease enforcement.
- **Restricting some uses of AI and prohibiting others** that pose **high or unacceptable risks to individual privacy** (i.e. automated biometric identification systems for AI-based social scoring). Legal restrictions where there is lack of legal basis for processing personal data in an employment context, no proportionality in relation to purposes and difficulty to find measures to mitigate high risks, in order to protect freedoms and rights of data subjects.
- **Legal certainty, protection and effective exercising and due consideration of the individual data protection and privacy rights of applicants and employees.** To enable individuals to exercise meaningful choice and control in relation to their personal information, businesses must first operate transparently and accountably and make AI understandable.
- **Adequate safeguards** provided by law and through regulatory frameworks, soft law and practical tools (guidelines), self-regulatory measures in companies etc.
- The requirement that AI must be reasonably necessary for an entity's functions or activities to fulfil the **proportionality principle**. For example, this could be weighed by considering the degree of sensitivity of the personal data involved, the legitimacy of the organisation's purpose and interest, the existence of less invasive means to achieve the purpose, and the proportionality of the loss of privacy for the individuals affected to the benefits the organisation gains from using the system.
- Restrictions should be in place to ensure that **training data** for AI systems in the employment context are obtained and processed lawfully and transparently.
- Clear statement of acceptable uses of AI in the workplace. Ensuring safe, ethical and practical use of AI in the workplace.

Question seven: Please briefly summarise examples of uses of AI in the workplace in practice in your jurisdiction

Several authorities highlighted the use of AI in recruitment, from sifting CVs, to analysing video interviews, undertaking background checks through facial recognition and photographic comparisons on social networks or large-scale profiling from a vast number of data sources, and the use of games to filter applicants. Some had seen instances of pre-selection and ranking software leading to discrimination. Others also noted AI used to monitor employees, such as through the tracking of vehicles and mobile devices, through the use of AI webcam in monitoring home workers or through keystroke monitoring. There were also mentions of the use of AI to measure individual performance and effectiveness, evaluate employees' well-being or health int the workplace, and attempts to control sick leave based on data mining techniques in order to identify unjustified sick leave applications. Some observed the use of biometric data such as fingerprinting or facial recognition to gain access to work facilities, to control working time, to analyse job interviews, to evaluate personality traits, and the use of video surveillance with facial recognition in entrance areas of buildings. Others were aware of videoconferencing software using AI algorithms without an appropriate legal basis, while others noted that professional social networks rely heavily on matching and selection algorithms.

Question eight: Have you identified broader areas of impact around the use of AI in employment that you would like to raise (impact of consumers, competition, employment law compliance, etc)?

A number of authorities highlighted the need for compatibility with other legal frameworks, such as consumer law and employment law, and broader inequality and unfair discrimination.