Department DAA (Digital Working Worlds and Work Reporting)
Department REC (Legal)

21 June 2021

Initial assessment

of issues relevant to labour policy on the

Draft of the EU Commission on a European AI regulation

(ARTIFICIAL INTELLIGENCE ACT)
21 April 2021

1) In principle, DGB welcomes that the EU Commission generally classifies AI systems as high-risk in the context of labour and employment and thus makes them subject to special approval conditions. This includes AI systems "used in employment, management of workers and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons" (Recital 36). However, it is unclear whether work organised on digital platforms falls within the scope of this regulation. This must be ensured.

   DGB is also generally pleased that AI systems "used in education or vocational training, notably for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education" (see Recital 35) are to be classified as high-risk.

2) However, DGB criticises the EU Commission's planned massive restriction of the high-risk classification through 'Annex III' to (a) AI systems for recruitment or selection (notably for advertising vacancies), screening or filtering applications, evaluating candidates in the course of interviews or tests, and in (b) Making decisions on promotion and termination of work-based relationships, for task allocation and for monitoring and evaluating performance and behavior.

Instead, DGB calls for AI systems to be generally classified as high-risk if personal information in the employment relationship is affected. This concerns both the realm of human resources administration (such as the initiation of employment relationships), including the involvement of social security systems and, in particular, the interaction of employees with AI systems in the work process (e.g. embodied intelligence). It is crucial to prevent delimitation issues that primarily relate to new forms of human-machine interaction or human-robot collaboration or imply algorithmic forms of control. It is necessary to clarify whether this can be dealt with by the machinery regulation which is appropriate for the sector.

DGB also calls for the legal exclusion of analysis procedures in the area of HR that turn employees into objects by collecting information that cannot be deliberately controlled ("unacceptable risk" category).

DGB further calls for a legal regulation according to which the use of personal information in the employment context, in the case of AI use, requires not only individual consent but also an additional agreement under collective rights that includes a transparent objective, access and usage regulations and their limitations. If there is no works council or no collective bargaining agreement, the approval of an authority could be obtained specifically or the "approval under collective rights" could be granted on the basis of standard examples formulated by the supervisory authority.

3) DGB expressly criticises the fact that the EU Commission's proposal does not include any process requirements for participation and co-determination options for the operational use of AI systems. This concerns the participation of social partners, and co-determination as well as the participation of affected employees. The EU Commission already determined in the White Paper for the 2020 regulatory proposal that "involvement of social partners [...] is a crucial factor in ensuring a human-centred approach to AI at work". In the draft that is now currently being submitted, the participation of social partners is no longer mentioned.

   DGB therefore calls for procedural regulation on operational use to enable preventive, non-discriminatory, gender-sensitive and holistic work design, including, in particular, an operational impact assessment (risk management system), the intended testing procedures (Article 7 (5)), the quality management system (Article 17) for sufficient transparency and traceability and continuous evaluation of the learning systems in the organisation and intervention options. Consideration of collective agreements can and should be integrated in a manner that is analogous to the GDPR (Article 88). The impact on operational work processes (employment prospects, profile changes, occupational health and safety, etc.) must be explicitly considered in the 'risk management system' required for high-risk applications. The opportunities for employees and their representatives to participate in shaping the process must urgently be reinforced and be binding and process-oriented in order to resolve conflicts in objectives in a socially acceptable manner and to prevent unintended side effects in working life that contradict European values. It should be clearly stipulated that company use of such technology can only take place with mandatory participation of employee representatives, e.g. through the conclusion of collective agreements. This must apply to the rollout of the technology and to its operational implementation. It must be ensured that employee representatives have access to the relevant information throughout the entire AI "supply chain", that is, all the way up to the "provider".

DGB requests that the individual skills learned by employees regarding the interaction with AI systems are usable for them in order to enable portability of expertise.

4) DGB calls for an association right, for unions in particular, to take legal action in the first step for disclosure of the functionalities of the algorithms in AI systems used in companies and the source code behind these algorithms. Such an enforceable right to disclosure for unions is necessary to also be able to examine the data collectively recorded by AI systems and thus avert any damage to employees. In addition, it must be ensured that sanctions for employees under labour law that could theoretically result from interaction with AI systems (especially when dealing with proposed decisions) must be excluded in a binding manner.

5) DGB takes issue with the fact that, according to the proposal of the EU Commission by Article 43 with reference to Annex III for implementation of the requirements for AI providers in the context of work, an establishment of independent bodies and corresponding audits for the area of work has not explicitly been provided for.

   DGB calls for independent AI agencies to be set up on the national level, specifically for the area of labour and employment, to support company stakeholders in consultation, testing, evaluation and complaints, and for these agencies to be equipped with sufficient resources.

6) The establishment of a European AI authority (European Artificial Intelligence Board, Title VI, Chapter 1 Article 56 et seq.) appears to be a logical step in view of the multitude of coordination and control tasks that will arise directly as a result of the creation of a uniform regulatory framework for the use of AI.

7) The sanction regime of Article 71 of the regulation is similar to the GDPR in terms of its systematic structure: the maximum amount of the fine is based on the global annual turnover of the company. This is to be welcomed, because it promises to have an adequate deterrent effect if the punishment is efficient. For effective penalties that are to be imposed for violations (Recital 84) in order to ensure effective protection of employee rights, the penalties should be of a certain minimum level.

Issues to be clarified:

- Legally sound terminology for "classification"

  In Article 7, the regulation grants the EU Commission the additional authority to supplement the list of high-risk systems in Annex III on the basis of vaguely defined criteria. Both the criteria and the classification to be applied here require a transparent and democratically monitored procedure.

  The regulation of "prohibited" AI applications in Article 5 contains many undefined legal terms, leaving much room for interpretation. For example, there is the question of whether it is possible to determine on a legally sound basis what exactly is meant by "AI systems" that exploit any of the vulnerabilities of a specific group of persons due to their physical disability in order to influence their behaviour with the result of psychological harm. It is important to ensure that evaluation of union activity in public spaces using AI as a union-busting strategy is prevented.

  The following areas are of further relevance to the world of work and thus to the classification as high risk: Social law (Recital 37), "law enforcement authorities" (Recital 38), border control management (Recital 39) and administration of justice and democratic processes (Recital 40). It is to be welcomed that AI systems intended for administration or for democratic processes are assessed as high risk. With regard to works council elections, AI systems should only be permissible under very narrow conditions.

  We appreciate that the rules are also to apply to applications established outside the EU. This already is the case of many systems used in the world of work. The exception of Article 2(4) is problematic due to complete exclusion of authorities from third countries and international bodies that are active in the area of law enforcement. Particularly in law enforcement and police operations, unlimited and unregulated use of AI can lead to massive violations of the law under certain circumstances.

  It is unclear whether and which mechanism shall take effect if a high-risk application develops the criteria of a "prohibited" system in the course of "learning" (that is, the data-driven further development of its properties), i.e. if, on the basis of the collected data, the conduct of a person can be subliminally influenced. In this regard, neither Title II (prohibited applications) nor Title III (high-risk applications) regulations contain resolution mechanisms.

- Rollout of biometric real-time monitoring "through the back door" – including the working life

  The exception to the regulation under Article 5(1)(d), which corresponds to the general exception under Article 2(4) is particularly problematic as it allows the use of remote biometric identification systems in "real time" in publicly accessible spaces for the purpose of law enforcement, such as for the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a terrorist threat. This legitimises expansion of surveillance options using the collection of biometric real-time data, such as using the argument of a constant threat to physical safety in the context of a pandemic, for example. Employees working in the public realm – such as the police, emergency services, street cleaners or local public transport – would also be subject to surveillance possibilities in the employment relationship that go further than the surveillance permitted in the employment

relationship on the basis of data protection law. The criteria that subsequently (under Article 5(2)) lay down the conditions for the admissibility of real-time biometric surveillance are defined in very broad terms and are not really actionable. On this basis, there is a threat of EU-wide legitimisation of biometric surveillance in public spaces.

- Data access

  From the perspective of the DGB, there is a need for discussion with regard to access to the data sets (Recital 45). As relevant stakeholders, social partners and the works councils need access to the data, especially to the documentation in the event of high-risk applications (Recital 48).

- The relationship between the regulation and national regulations

  The regulation limits the authority of national regulators in making decisions regarding the conditions for approval of AI applications. The regulation focuses on extensive technical requirements and on regulations on the approval and certification process for high-risk AI applications, which include those implemented in the context of employment relationships. Recital 67 states that for high-risk AI systems permitted under the regulation, Member States should no longer be entitled to restrict their use or deployment. For example, as soon as a personnel selection application has undergone an approval procedure in accordance with Article 43 of the regulation and has CE certification in accordance with Articles 48 and 49 of the regulation, its use cannot, in principle, be restricted on the national level. In this context, it is not clear to what extent the regulation restricts the decision-making prerogative of Member State stakeholders regarding the deployment and use of certain AI applications in business practice. EG 67 states: "*High-risk AI systems should bear the CE marking to indicate their conformity with this regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to placement on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this regulation and bear the CE marking.*" According to Article 3 (11), the phrase "putting into service" is to be understood as "the supply of an AI system for first use directly to the user for its intended purpose", that is, the use at the user's premises. Against this backdrop, clarification is required: The decision on the use of AI applications that meet the requirements of the regulation and thus gain market access, must be left to stakeholders in the Member States, including company stakeholders. This also appears to be imperative – as far as the storage, processing and transfer of employee data is affected – against the backdrop of the provisions of the GDPR and the possibilities that the national lawmakers have to regulate employee data protection pursuant to Article 88 of the GDPR. Since it is not permitted to set aside the GDPR standards, the same must apply to an AI directive. The AI directive may not, either covertly or overtly, take away from the "GDPR guarantee" for the national regulations on employee data protection with regard to AI use. This clarification should be explicitly included in the regulation.

- Scope

  According to Article 2(1)(c), the regulation shall apply to AI systems that are placed on the EU market (a), used by users within the EU (b) or linked to an output within the EU. The arrangement often encountered in the world of work, in which AI systems set up outside the EU are used in the working relationship between an employee residing in the EU and their employer are not expressly dealt with. Although Recital 10 of the regulation clearly states that the rules of the regulation shall also apply in this case, this clarification remains legally non-binding. The scope of application of the regulation should therefore be extended to be legally binding in instances of arrangements in which the rights and interests of EU citizens are affected, even if the output (work result) is produced in a third country (such as in the case of company headquarters/platform registration outside the EU).

- Evaluation of the very extensive regulations of technical requirements for AI systems and their review and approval mechanisms (Title IV, Chapters 3 to 5) is not possible without technical expertise. For this reason, this extensive portion still needs to be completed.

Background

Risk-based approach of the Commission proposal

The draft of a legal framework for AI presented by the EU Commission is based on a four-tier risk-based approach:

- **Unacceptable risk**: AI applications that violate EU values are to be prohibited. This pertains to the assessment of social conduct by public authorities (social scoring), the exploitation of children's vulnerability, techniques for subliminal influencing and, with narrow exceptions, real-time biometric remote identification systems intended for law enforcement purposes in public spaces.

- **High risk**: AI systems that may adversely affect people's safety. Safety components of products covered by the sectorial legislation of the EU are included in these systems. They are always considered to pose a high risk if they are required to undergo a third-party conformity assessment under this sectorial legislation.

  A high-risk assessment is present for the following areas:

  a) Critical infrastructure (such as transportation) where the lives and health of citizens could be put at risk

  b) Education in school or **vocational training** if a person's access to education and professional life could be affected (such as assessment of examinations)

  c) Safety components of products (such as an AI application for robot-assisted surgery)

  d) Employment, human resource management and access to self-employment (such as software to evaluate CVs for hiring processes)

  e) Important private and public services (such as credit scoring that prevents citizens from obtaining a loan)

  f) Law enforcement that could interfere with people's fundamental rights (such as evaluation of the reliability of evidence)

  g) Migration, asylum and border control (such as checking the authenticity of travel documents)

  h) Administration of legal and democratic processes (such as application of legislation to specific facts and circumstances)

- **Low risk**: Certain AI systems must comply with transparency obligations if there is a risk of manipulation (such as the use of chatbots). Here, it is necessary to indicate that the user is communicating with a machine.

- **Minimal risk**: This relates to AI systems that are not subject to the previously mentioned classifications. The objective here is to provide the opportunity to undergo voluntary "certification" as a trusted AI and to comply with voluntary codes of conduct.

AI systems are to be classified as **high risk in the context of work** according to the EU Commission if:

- AI systems are used **in general education or career training**, in particular to **determine the access or assignment of individuals to educational and vocational training institutions or to assess individuals** on the basis of tests as part of or as a precondition for their training or education (see page 26, item 35)

- AI systems are used **in employment, management of workers, and access to self-employment**, in particular for **hiring and selection of individuals, promotion and termination decisions and for task allocation, monitoring or evaluation of individuals** (see p. 26 item 36)

Annex III (p. 4) further specifies this:

a) AI systems **in hiring and selection** (notably for advertising vacancies), screening or filtering applications, **evaluating candidates** in the course of interviews or tests

b) AI in **decisions on promotion of employees or termination of employment relationships**, in **allocation of tasks** and in **monitoring and evaluation of performance and behaviour**.

For AI systems/providers[1] in the high-risk classification, the following requirements apply:

- Appropriate risk assessment and risk mitigation systems
- High-quality data sets that are fed into the system in order to keep risks and discriminatory results to a minimum
- Logging of operations to enable traceability of results
- Detailed documentation with all the necessary information on the system and its purpose so that the authorities can assess its conformity
- Clear and appropriate information for users
- Adequate human supervision to minimise risks
- High level of robustness, safety and accuracy

Providers of AI applications must establish, document and maintain a risk management system for high-risk classifications that operates throughout the entire lifecycle of the AI system and needs to be updated regularly.

[1] Provider: a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge

The tasks are described under Article 9 (p. 46) and include, for example:

- Identification and analysis of the known and foreseeable risks that are associated with every high-risk AI system
- Estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse

According to Article 17 (see p. 53), providers of AI applications must implement a quality management system for high-risk classifications to document compliance with the regulations. The aspects to be documented are also listed under Article 17.

Providers of high-risk AI systems are required by Article 43 to conduct a conformity assessment, which is mostly an internal control process. The establishment of an independent body is only necessary if a conformity assessment by third parties is required by sectorial legislation or, according to Article 43 (see Annex VII), the biometric identification and categorisation of natural persons is affected. According to the EU Commission, independent audits by '*notified bodies*' are therefore not foreseen for the area of labour and employment.

AI providers must register standalone AI systems in an EU database. In principle, this registration will allow competent authorities, users and other interested persons to verify that the high-risk AI system meets the requirements set out in the proposal. To fill this database, AI providers will be required to provide meaningful information on their systems and the conformity assessment performed on these systems. AI users are also to indicate that they are carrying out the aforementioned processes using CE certification.

Member States are to designate one or more national authorities for application and enforcement of the regulation. In order to increase organisational efficiency on the part of the Member States and to create an official point of contact for the public and other counterparts at Member State and EU level, a national authority should be designated as the national supervisory authority in each Member State. Authorities and designated bodies that are responsible on a national level and involved in the application of this regulation shall preserve the confidentiality of information and data obtained in the course of their duties and activities in a manner that protects the following in particular: [...] the effective implementation of this regulation, in particular for the purposes of inspections, investigations and audits (see Article 70). According to Article 23, "Providers of high-risk AI systems shall, upon request by a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements [...], in an official Union language determined by the Member State concerned". However, this requires that the national authority/authorities is/are adequately staffed with competent personnel (Article 30).

In addition, the Commission proposes the establishment of a "European Artificial Intelligence Board". The board is intended to facilitate the implementation of the regulation and perform advisory tasks, such as issuing opinions, recommendations, advice and guidance on matters related to the implementation of this regulation, including on technical specifications or existing standards related to the requirements set forth in this regulation and providing advice to and assisting the Commission on specific questions related to artificial intelligence (see p. 35). The board shall be composed of the national supervisory authorities, represented by the head or equivalent

high-ranking official of each authority, and the European Data Protection Officer. Other national authorities may be invited to attend meetings if the issues discussed are of relevance to them (see p. 72).

Proposed procedure for the use of high-risk AI systems:

Contact:

Micha Klapp
Head of Legal Department
micha.klapp@dgb.de

Oliver Suchy
Head of Department Digital Working Worlds and Work Reporting
oliver.suchy@dgb.de