The use of AI in human resources management: Orientation in the jungle of AI regulation

November 6, 2024 | Deloitte Legal Webcast

Introduction & Agenda

Contributors

Anna M. Bock
Lawyer specialized in Employment Law /
Senior Associate
Employment Law & Benefits
Deloitte Legal
Hannover, Germany

Tel.: +49 511 307559315
E-Mail: abock@deloitte.de

Roland Schiller
Lawyer / Associate
Digital Law
Deloitte Legal
Frankfurt am Main, Germany

Tel.: +49 69 71918 8473
E-Mail: rschiller@deloitte.de

Agenda

AI Act
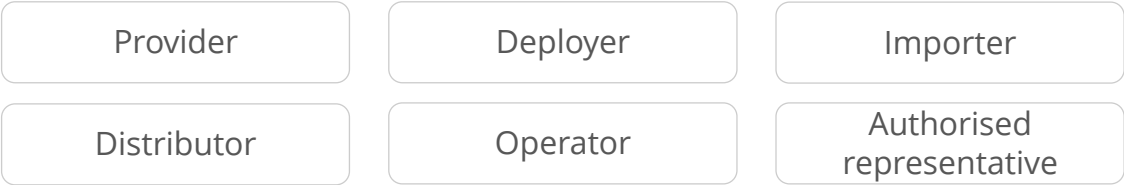# Regulation (EU) 2024/1689

The EU AI Act an overview

1

Is it an AI system within the meaning of Art. 3 (1) of the AI Act?

An "AI System" means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

2

In which risk category does the AI system fall into?

Prohibited AI practice

High-risk AI system

Limited risk

Minimal risk

3

What kind of 'actor' are we talking about?

Provider

Deployer

Importer

Distributor

Operator

Authorised representative

4

Is the AI system a General-Purpose AI model (GPAI)?

GPAI „normal"

GPAI with systemic risk (> 10^25 FLOPS)
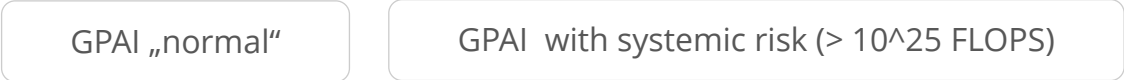
Promoting human-centred and reliable AI to protect health, fundamental rights, democracy and the environment - while supporting innovation and European SMEs

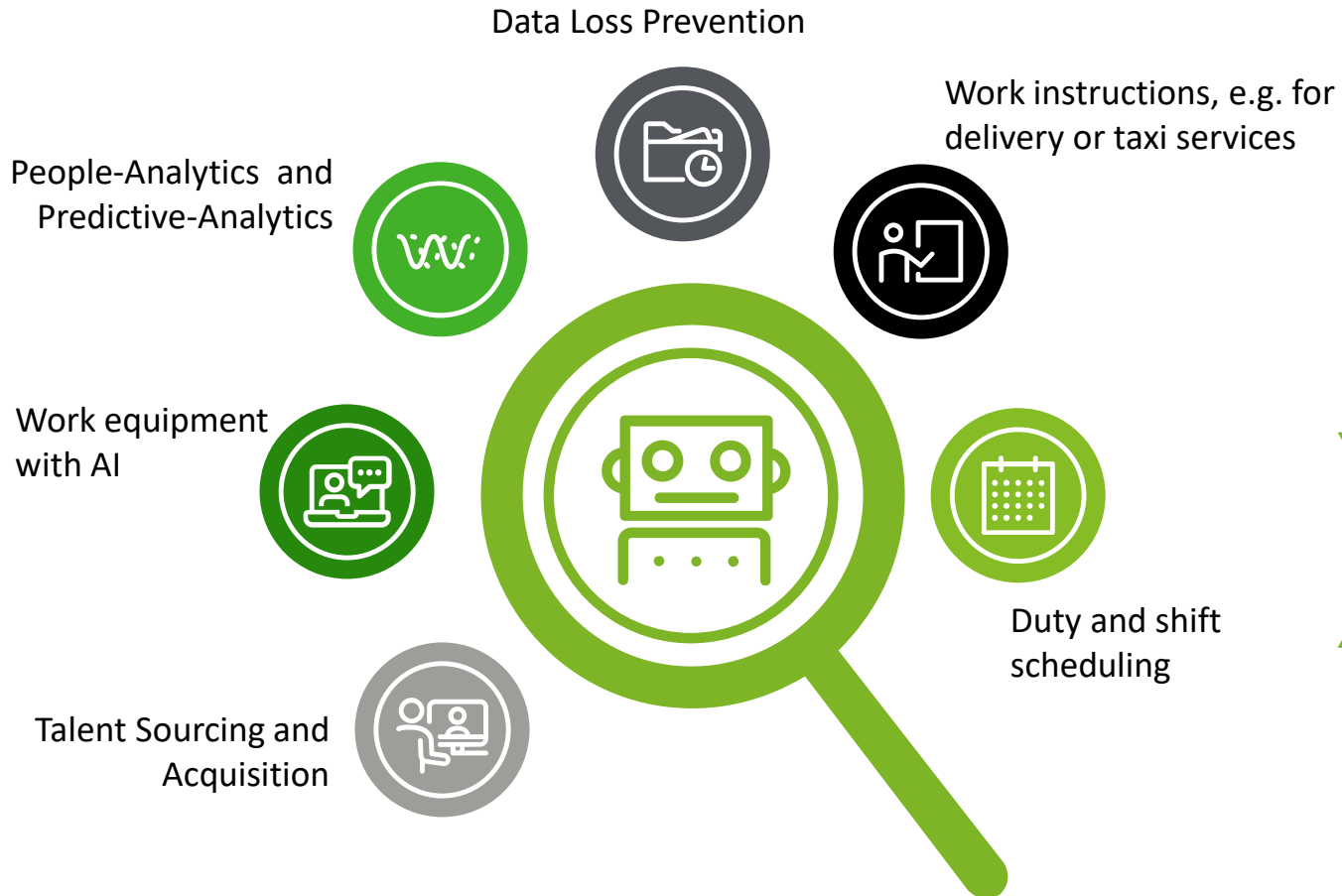| Risk category	Cosequences	Application timeline	Administrative fines up to …
Unacceptable risk • Social Scoring • Biometric identification in real time • Recognising emotions in the workplace[a]	Restrictions	6 month	**€ 35 million or 7% of global annual sales** • Unacceptable use cases (Art. 5)
High-risk AI systems • Credit decicions • Critical infrastructure • Risk to fundamental rights • **The specific areas listed in Annex III**	Conformity check, Governance, supervision, recording	24 bis 36 month [b] 12 month (GPAI-systems)	**€ 15 million or 3% of global annual sales** • Non-compliance with deployer obligations for high-risk AI systems
Limited risk • Chatbots • „Deep Fakes"	Transparency obligations	24 month	**€ 7.5 million or 1% of global annual sales** • Incorrect, incomplete or misleading response to a request from the NCB/NB[c]
Minimal Risk • Internal use cases • Procedural tasks	Voluntary standards	n.a.	

[a] Except for medical or safety reasons such as fatigue or pain; b) Up to 36 months if the use case is included in the EU Product Safety List; c) NCB = national competent authority, NB = notifying authority.
Products that were already on the market before the AI Act came into force are technically excluded from the scope unless they are already on the market and (i) subsequently undergo 'significant changes' or (ii) are a GPAI. In addition, an extended implementation period of 36 months applies to GPAIs that were already on the market before the AI Act.

Examples of the use of AI in HR and as work equipment

Data Loss Prevention

Work instructions, e.g. for delivery or taxi services

People-Analytics and Predictive-Analytics

Work equipment with AI

Talent Sourcing and Acquisition

Duty and shift scheduling

High-risk systems according to Annex III

[...]

Employment, worker's management and access to self-employment:

a) **Recruitment** or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;

b) **Decisions** affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships
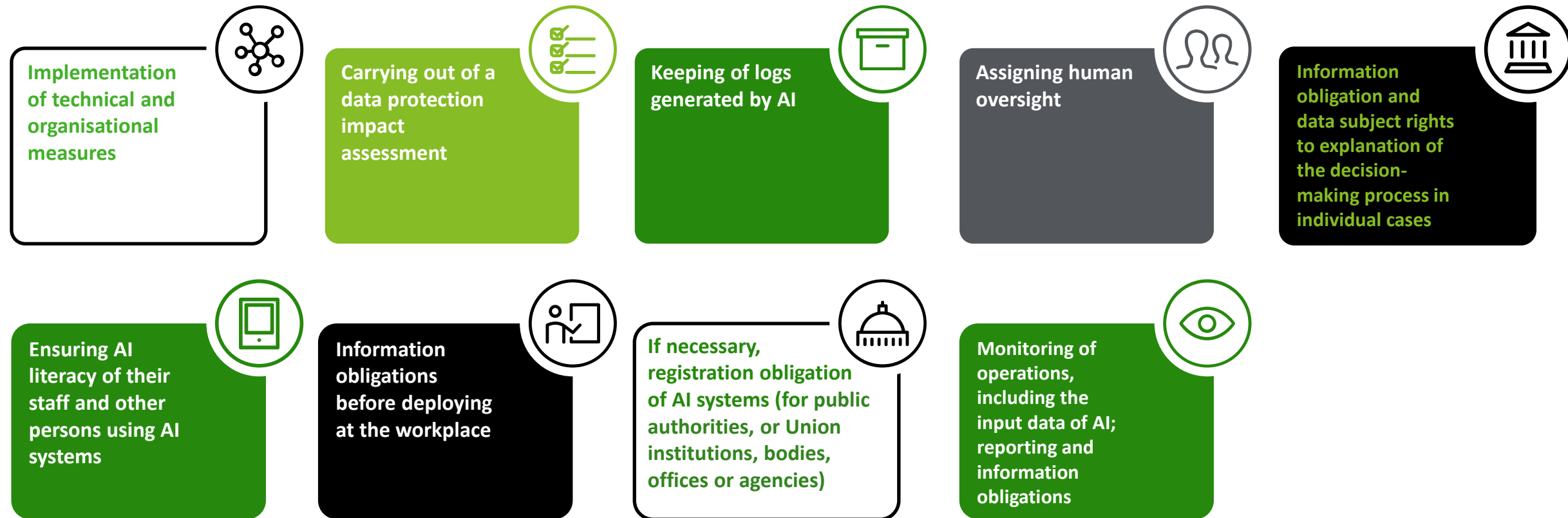
Exception: no significant risk of harm to the health, safety or fundamental rights of natural persons, in that the AI system does not materially influence the outcome of decision-making, among other things.
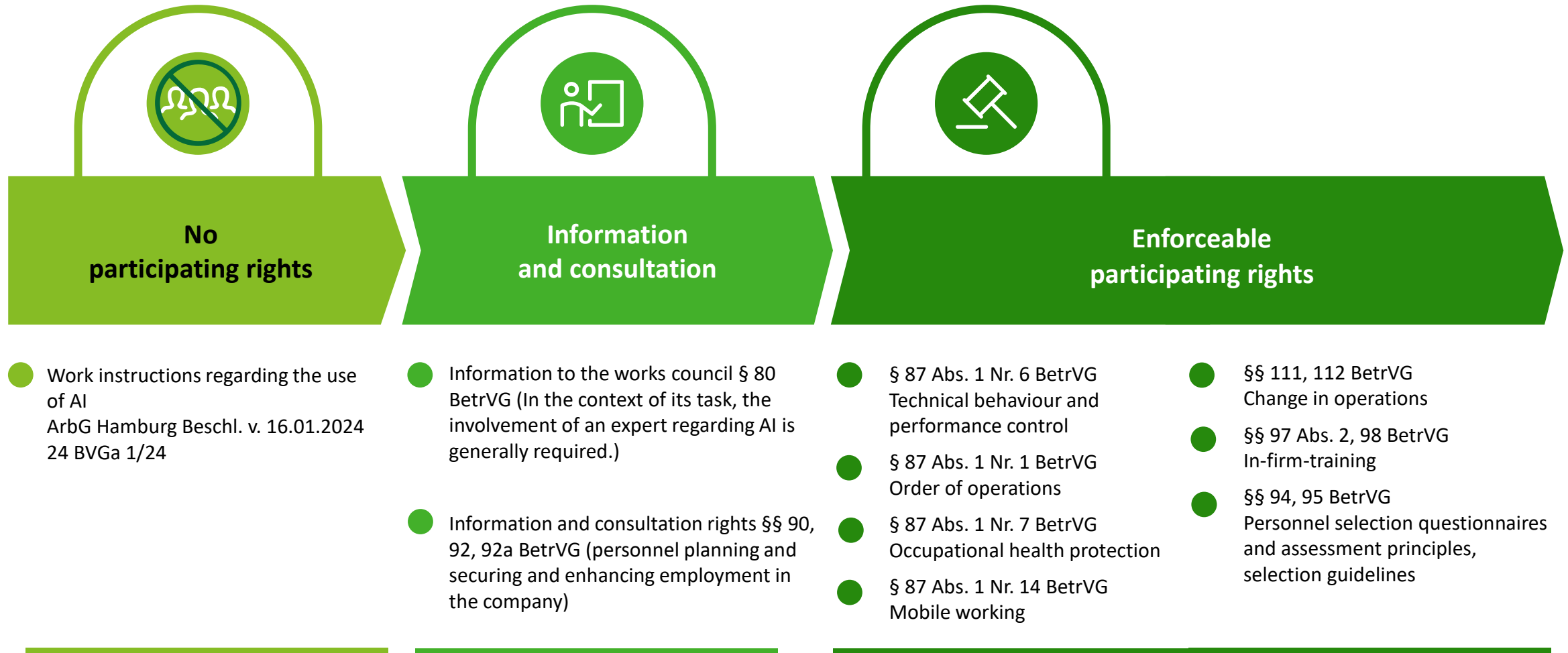
Obligations of the deployer*

„deployer"means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity

Implementation of technical and organisational measures

Carrying out of a data protection impact assessment

Keeping of logs generated by AI

Assigning human oversight

Information obligation and data subject rights to explanation of the decision-making process in individual cases

Ensuring AI literacy of their staff and other persons using AI systems

Information obligations before deploying at the workplace

If necessary, registration obligation of AI systems (for public authorities, or Union institutions, bodies, offices or agencies)

Monitoring of operations, including the input data of AI; reporting and information obligations

*) The obligations of the deployer described correspond to the 'Obligations of deployers of high-risk AI systems' in accordance with Art. 26 of the AI Act. The Conference of Independent Federal and State Data Protection Supervisory Authorities (DSK) has issued guidance on 'Artificial intelligence and data protection' (version 2.0 dated 17 October 2024), which examines the use of AI systems by data controllers from a data protection perspective.

Employment law:
Participating Rights In The Introduction Of AI

Key participation rights of the works council in the introduction of AI

No participating rights

- Work instructions regarding the use of AI
  ArbG Hamburg Beschl. v. 16.01.2024
  24 BVGa 1/24

Information and consultation

- Information to the works council § 80 BetrVG (In the context of its task, the involvement of an expert regarding AI is generally required.)

- Information and consultation rights §§ 90, 92, 92a BetrVG (personnel planning and securing and enhancing employment in the company)

Enforceable participating rights

- § 87 Abs. 1 Nr. 6 BetrVG Technical behaviour and performance control

- § 87 Abs. 1 Nr. 1 BetrVG Order of operations

- § 87 Abs. 1 Nr. 7 BetrVG Occupational health protection

- § 87 Abs. 1 Nr. 14 BetrVG Mobile working

- §§ 111, 112 BetrVG Change in operations

- §§ 97 Abs. 2, 98 BetrVG In-firm-training

- §§ 94, 95 BetrVG Personnel selection questionnaires and assessment principles, selection guidelines

Paticipating rights of the works council in the introduction of AI

Information and consultation

- Works council does not need to agree

- Arbitration board cannot be invoked in principle

- The employer must inform the works council, consult with the works council and seriously consider the matter. If the employer rejects the proposals, it must justify this (in writing), if necessary

- In the event of a breach, a claim for fulfilment can be enforced in judicial resolution procedure and sanctioned with a fine in accordance with § 23 (3) BetrVG

Enforceable participating rights

- Works council must give its consent
  → works agreement

- Arbitration board becomes active at the request of one party
  → The decision of the conciliation committee replaces the agreement with the works council

- Disposal- and injunctive relive
  → Exists in the event of a breach of co-determination rights under § 87 (1) BetrVG
  → Enforcement possible through the courts, includinginterim injunction

Participating rights in the implementation of employer obligations under the AI Regulation

Employee information

- Before commissioning or using a high-risk AI system in the workplace, deployers who are employers must inform the employee representatives and the affected employees that they will be subject to the use of a high-risk AI system (Art. 26 (7) AI Act)

Complementing policies, manuals

- Implementation of the requirements of the AI Act through corresponding additions to policies and manuals
- If applicable, co-determination right from § 87 (1) No. 1 BetrVG

AI literacy training Art. 4 AI Act

- Introduction and implementation of AI literacy training:
- Co-determination in accordance with §§ 97, 98 BetrVG

Information about and explanation of the decision-making process

- If deployers take a decision on the basis of data from a high-risk AI system that has legal implications or similarly materially affects the data subject concerned by the decision in a way that they consider to be detrimental to their health, safety or fundamental rights, the data subject concerned has the right to receive a clear and meaningful explanation from the deployer about the role of the AI system in the decision-making process and the main elements of the decision taken (Art. 86 AI Act) and information from data subjects (Art. 26 (7) AI Act)
- Participating rights of the works council pursuant to § 87 (1) No. 1 or No. 6 BetrVG

Best Practice

If applicable, cooperation with the works council in the creation of AI principles

Consistently coordinated interdisciplinary implementation of the AI System from a labour law, data protection / IT law and technical perspective

Best Practice

Involve the works council at an early stage and provide clear information on data protection law, regulatory and technical aspects when implementing the IT System

Consideration of works agreement negotiations in the implementation schedule
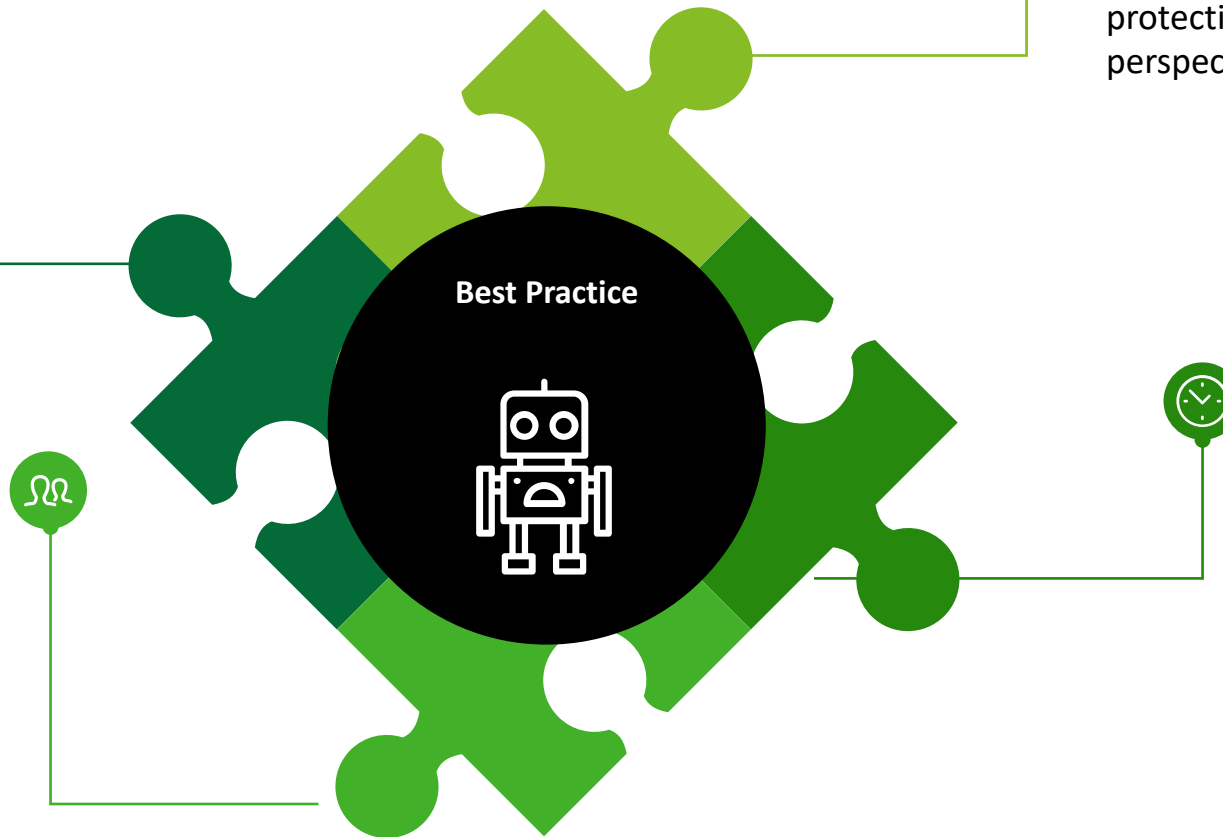
Data Protection:
Principles And Their Significance For AI

AI and data protection
Relationship between the AI Act and the GDPR

⚠ The fundamental rights and freedoms of data subjects must be protected effectively. For the development and use of AI systems in which personal data is processed, the requirements of the GDPR must therefore be observed in addition to the AI Act.

GDPR

- Protection of personal data takes centre stage
- GDPR remains unaffected by the AI Act
- Reviewing the data set in accordance with Art. 10 AI Act is already a processing of personal data and must be based on a legal basis in accordance with Art. 6 GDPR

AI Act

- Provides a framework for the general handling of data (data governance)
- Central regulatory provision on data processing: Art. 10 AI Act
- If high-risk AI systems are trained with data, corresponding quality criteria must be fulfilled

- Both regulations apply in full
- If personal data is used in the development of high-risk AI systems, providers of AI systems must comply with both the requirements of the AI Act and the GDPR, so-called 'double obligation'."

Data protection principles and significance for AI (selection)

1 * Collecting training data

2 Processing of training data, including 'fine-tuning'

3 Provision of AI systems

Use of input data for training purposes

4 Use of AI systems

5 Utilisation of results from AI systems

Purpose limitation

It must be determined in advance which field of application is intended for the AI. Is the processing of personal data necessary to achieve the purpose?

„Privacy by Design" and „Privacy by Default"

e.g. restriction of the processing of personal data used in live operation for the subsequent training of AI

„Integrity and confidentiality "

In particular, protection against model inversion attacks and membership inference attacks

Data minimisation

Restricting the processing of personal data to what is absolutely necessary

Data accuracy

The processed data must be checked for accuracy in advance. Subsequent correction of incorrect data must be effectively possible.

Use Case: Personnel Measures

Application management

CV-Parsing

- Identification of key parameters
- Eliminate unsuitable applications

Candidate Journey

- Using of a chatbot
- Creation of personality profiles by analysing text and speech
- Analysing speech, facial expressions and gestures

Expected benefits

- Efficient use of resources
- Cost reduction
- Increased objectivity in the selection process (bias reduction) through data-based decisions instead of subjective impressions

Risks

There are considerable risks of overt/hidden discrimination, especially when using the "wrong" data set:

- "biased" data set; consideration of discriminatory parameters such as gender or origin
- Overrating of certain criteria (certain key words are used more frequently by men or women)

Application management

AI Act (selection)

- Is the AI system high-risk or is the use exceptionally not associated with high risk?
- AI competence of employees must be ensured.
- Employees and affected persons must be informed about the use of an AI system.
- Decisions made by the AI system must be explainable.

Prohibited practice in the sense of Art. 5 AI Act ?

Data protection (selection)

- Processing only on the basis of a legal basis; is the use of AI necessary?
- The processing of special categories of personal data (e.g. voice/facial expression) is only permitted under stricter conditions.
- Particular challenges arise in relation to the voluntary nature of consent in a superior-subordinate relationship.
- Human intervention in decisions made by AI must be ensured (Art. 22 GDPR).
- Carrying out a data protection impact assessment.
- Data subjects' rights must be effectively enforceable.
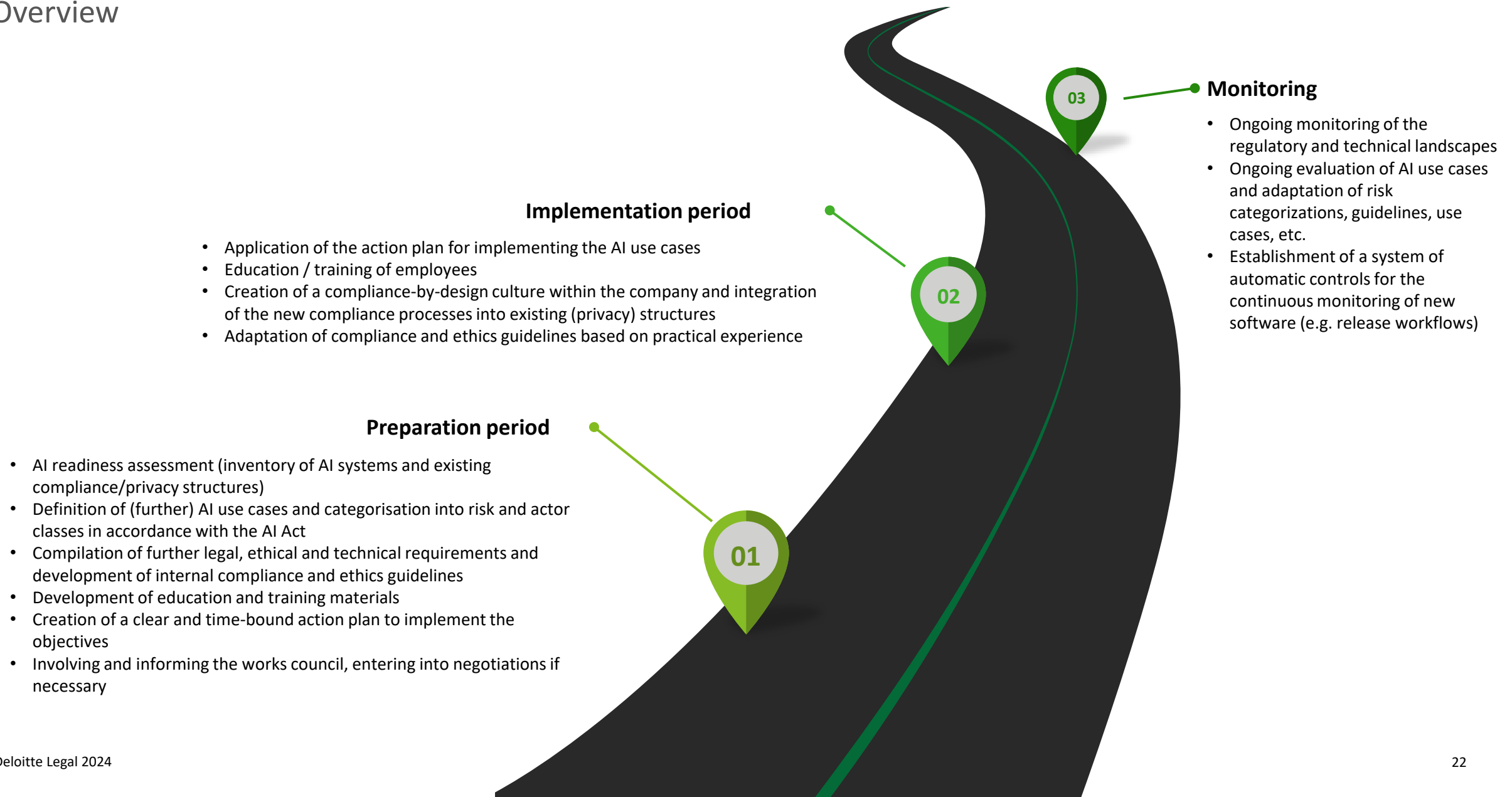
Employment law (selection)

- A works agreement must generally be concluded with the works council prior to the introduction of the AI system, § 87 (1) No. 6 BetrVG.
- The establishment of standardised questions and principles of decision-making in the application process by the AI system are subject to co-determination in accordance with § 95 BetrVG.
- The works council must be informed about the use and results of the AI system in the selection of applicants as part of co-determination for individual personnel measures pursuant to § 99 BetrVG.

AI-Governance

Implementation of the AI-Act
Overview

Monitoring

- Ongoing monitoring of the regulatory and technical landscapes
- Ongoing evaluation of AI use cases and adaptation of risk categorizations, guidelines, use cases, etc.
- Establishment of a system of automatic controls for the continuous monitoring of new software (e.g. release workflows)

Implementation period

- Application of the action plan for implementing the AI use cases
- Education / training of employees
- Creation of a compliance-by-design culture within the company and integration of the new compliance processes into existing (privacy) structures
- Adaptation of compliance and ethics guidelines based on practical experience

Preparation period

- AI readiness assessment (inventory of AI systems and existing compliance/privacy structures)
- Definition of (further) AI use cases and categorisation into risk and actor classes in accordance with the AI Act
- Compilation of further legal, ethical and technical requirements and development of internal compliance and ethics guidelines
- Development of education and training materials
- Creation of a clear and time-bound action plan to implement the objectives
- Involving and informing the works council, entering into negotiations if necessary

New Draft Of An Employee Data Act (Beschäftigtendatengesetz - BeschDG)

Draft bill of the Employee Data Act (BeschDG)

Until now, there have been hardly any regulations specifically tailored to the protection of employee data. The BeschDG creates a framework for modern employee data protection that aims to strike a balance between the interests of companies and employees while at the same time ensuring the necessary protection for employees.

Key content

- **Transparent** and **clear regulations** for employee data
- Data security through **technical and organisational measures**
- Prohibition on exploitation of data processed in breach of data protection regulations
- **Strict requirements** for automated data processing

Rights and obligations of the employees

- Collective agreements are excluded as a legal basis for processing under data protection law
- Specification of effective **consent** to the processing of employee data, free revocability
- **Right to information** about data processing and results

AI regulation

- **Transparency obligations / rights of data subjects** for the use of AI
- **Monitoring** of the necessity of processing and for incorrect results as a **technical and organizational measure**

💡 **Outlook**

The Employee Data Act strengthens data protection in the workplace and creates a clear framework for handling employee data. However, future developments in the field of digitalization will require continuous adjustments to the regulations in order to guarantee the protection of employee rights

Q&A

Thank you
for your
attention

Deloitte Legal

Your Contact

Anna M. Bock
Lawyer specialized in Employment Law /
Senior Associate
Employment Law & Benefits
Deloitte Legal
Hannover, Germany

Tel.: +49 511 307559315
E-Mail: abock@deloitte.de

Roland Schiller
Lawyer / Associate
Digital Law
Deloitte Legal
Frankfurt am Main, Germany

Tel.: +49 69 71918 8473
E-Mail: rschiller@deloitte.de

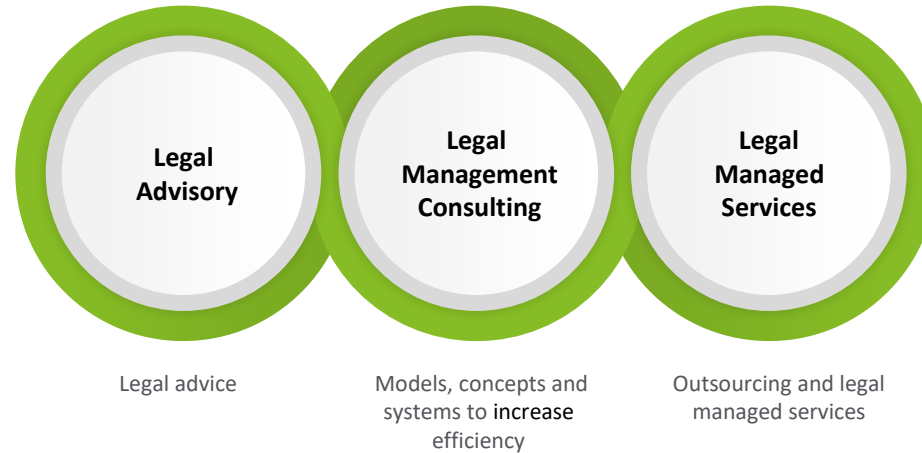# Where legal meets business

Deloitte Legal, these are

more than **2.500** Lawyers

in **75+** Countries

who work closely together
across national borders and together with other Deloitte business units

Services from Deloitte Legal

Our three overlapping service areas enable us to advise our clients when and where needed and in the most suitable form to realize their visions.

Legal Advisory

Legal Management Consulting

Legal Managed Services

Legal advice

Models, concepts and systems to increase efficiency

Outsourcing and legal managed services

We create (added) value

As part of the Deloitte global network, Deloitte Legal works with a variety of other disciplines to provide multinational legal solutions and globally integrated service:

in harmony
with your company-wide vision

customized
for your business units and branches

technology-based
for improved cooperation and transparency

coordinated
to your regulatory requirements

Deloitte Legal has a strong global presence

It can be very challenging to coordinate a large number of legal advisors around the world without losing sight of individual aspects.

As one of the world's leading legal consultancies, Deloitte Legal helps you overcome challenges and realize your vision by being your single point of contact for your global legal needs.

Key

Deloitte Legal footprint

Deloitte Legal practices

1. Albania	15. Chile	29. Gabon	43. Kazakhstan	57. Peru
2. Algeria	16. Colombia	30. Georgia	44. Kosovo	58. Poland
3. Argentina	17. Costa Rica	31. Germany	45. Latvia	59. Portugal
4. Australia	18. Croatia	32. Greece	46. Lithuania	60. Romania
5. Austria	19. Cyprus	33. Guatemala	47. Malta	61. Senegal
6. Azerbaijan	20. Czech Rep.	34. Honduras	48. Mexico	62. Serbia
7. Belgium	21. Dem Rep of Congo	35. Hong Kong SAR, China	49. Montenegro	63. Singapore
8. Benin	22. Denmark	36. Hungary	50. Morocco	64. Slovakia
9. Bosnia	23. Dominican Republic	37. Iceland	51. Myanmar	65. Slovenia
10. Brazil	24. Ecuador	38. Indonesia	52. Netherlands	66. South Africa
11. Bulgaria	25. El Salvador	39. Ireland	53. Nicaragua	67. Spain
12. Cambodia	26. Equatorial Guinea	40. Italy	54. Nigeria	68. Sweden
13. Cameroon	27. Finland	41. Ivory Coast	55. Norway	69. Switzerland
14. Canada	28. France	42. Japan	56. Paraguay	70. Taiwan
				71. Thailand
				72. Tunisia
				73. Turkey
				74. Ukraine
				75. Uruguay
				76. United Kingdom
				77. Venezuela

Deloitte.
Legal