Federal Ministry
Labour, Social Affairs, Health,
Care and Consumer Protection
Republic of Austria

research
institute

Enlightenment 4.0: Human understanding of AI decision-making

Report on the theoretical basis of the right to explanation of individual decision-making under Article 86 AI Act

Research Institute – Digital Human Rights Center

Enlightenment 4.0 – Human understanding of AI decision-making

Report on the theoretical basis of the right to explanation of individual decision-making under Article 86 AI Act

Vienna, 28 February 2025

Project management:	Madeleine Müller Christof Tschohl
Authors:	Jan Hospes Madeleine Müller Philipp Poindl Robert Rothmann Heidi Scheichenbauer David M. Schneeberger
Graphic design:	Andreas Czák

Consolidated report on the legal, social science and ethical foundations of the right to explanation of individual decision-making pursuant to Article 86 AI Act in conjunction with the relevant provisions of the GDPR in the context of the project "Enlightenment 4.0 - Human understanding of AI decision-making", which was carried out by the Research Institute - Digital Human Rights Centre on behalf of the Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection.

IMPRINT

Media owner and publisher:
Research Institute AG & Co KG
FN: 355966f, HG Vienna
Amundsenstraße 9, 1170 Vienna

The Research Institute (RI) is an independent research organisation at the interface of technology, law and society. The Institute's activities include scientific research and teaching as well as consulting.

Web: https://researchinstitute.at
E-Mail: office@researchinstitute.at
Mastodon: mastodon.researchinstitute.at/@researchinstitute

1 Table of contents

2 Management Summary

This report on the project “Enlightenment 4.0 - Human understanding of AI decision-making” (original title in German: “Aufklärung 4.0 - Entscheidungen der KI als Mensch verstehen”), carried out by the Research Institute - Digital Human Rights Center on behalf of the Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection, documents the legal basis of the right to explanation as enshrined in Art. 86 of the Regulation of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (“AI Act”[1]). In order to gain a more comprehensive understanding of this right, the report also includes related social science and ethical considerations. The primary objective of this report is to establish synergies between existing data protection law, in particular the General Data Protection Regulation (GDPR)[2], and the right to explanation of individual decision-making pursuant to Art. 86 of the AI Act (henceforth referred to as the “right to explanation” for the sake of brevity). Furthermore, the report contains a comprehensive review of relevant literature and case law in conjunction with selected use cases to establish theoretically well-founded practical relevance.

In consideration of the aforementioned aspects, this report provides a theoretical foundation for two manuals that were also developed in the framework of the project and address the implementation of the right to explanation in practice. One manual focuses on the perspective of the affected person or of the consumer, as consumers are among the main addressees of the right to explanation under Art. 86 AI Act. Conversely, it is also essential to adopt the perspective of companies and other institutions, as these are precisely the entities that require special training in dealing with the rights of persons affected. It is the employees of these organisations who are confronted with claims from affected persons and often do not know exactly how to deal with them appropriately. This is particularly evident in the context of new legal provisions for which no specific guidelines yet exist. Consequently, the second manual addresses this target group. In order to ensure the practical relevance of the manuals and improve the practical enforceability of the right to explanation, stakeholder workshops were held as part of the project to include both the consumer perspective and that of companies and other organisations.

---

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act/KI-VO), OJ L 2024/144, 1.

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

3 The project “Enlightenment 4.0 - Human understanding of AI decision-making”

3.1 Project background

The Regulation of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (“AI Act”) was officially published in the Official Journal of the European Union on 12 July 2024 and entered into force in August 2024. The AI Act follows a risk-based approach, categorising AI systems into distinct risk categories according to their type, scope of application and potential risks to the safety, health and fundamental rights of affected persons.[3] This categorisation entails different obligations and legal consequences, in addition to determining the regulations’ date of applicability (ranging from six to 36 months after entry into force).

For a considerable number of companies and other entities this means a significant change and the integration of a broad set of normative standards into their activities. This is particularly true with regard to dealing with the rights of the affected persons, as many AI-based systems used in day-to-day business often involve an affected individual, who interacts with it. A broad use case is AI-based systems of which the output is used to make decisions that subsequently impact individuals or groups of people. Examples of certain (groups of) individuals who may be subject to the decision of an AI-based system include those in the area of credit scoring and the conclusion of health and life insurance policies (see Annex III (5) AI Act, which classifies such systems as “high-risk AI systems”). Another case considered high-risk according to Annex III (5) AI Act concerns the use of AI-based systems to assess whether natural persons are entitled to public services and benefits. The list of potential use cases could be extended to include a significant number of additional cases, thereby illustrating how frequently natural persons and groups of persons will in the future be subject to decisions by AI-based systems that are categorised as high-risk or are already affected by them.

Art. 86 AI Act provides for a “right to explanation of individual decision-making”, according to which persons affected by a high-risk AI-supported decision are entitled to information regarding the main elements of the decision and the role of the AI system in the decision-making procedure (hereinafter: “right to explanation”). However, Art. 86 AI Act does not provide detailed instructions on how companies must fulfil this right in practice or what specific information must be provided. There is (naturally) no case law on Art. 86 AI Act yet, although an initial request for a preliminary ruling has been submitted.[4] However, it is imperative that companies and associations, and in particular public institutions, fulfil this right in an appropriate manner in terms of compliance with the principles of transparency and

---

[3] Cf. *Metikos/Ausloos*, The Right to an Explanation in Practice. Insights from Case Law for the GDPR and the AI Act, Law, Innovation, and Technology 2025, iE, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4996173 17.2 2025 (as at 24 October 2024).

[4] Reference for a preliminary ruling ECJ 25. 11. 2024, C-806/24, *Yettel Bulgaria*, ECLI not yet assigned.

accountability.

In addition to the legal obligations imposed by the AI Act on the relevant bodies, the requirement to comply with ethical principles has also found its way into the debate on artificial intelligence and has become a central cornerstone of Austria's AI strategy. This is where the project at hand becomes pertinent, with the aim of developing concrete guidelines for dealing with the right to explanation and thus taking appropriate account of the high legal and ethical standards to which Austria has committed itself in its national AI strategy. In accordance with an approach orientated towards the common good and developed on the basis of fundamental and human rights, trust in the use of artificial intelligence is to be strengthened and a responsible approach to its use guaranteed.

The right to an explanation is considered a central pillar for the realisation of such an approach, as it is often the prerequisite for the persons affected to be able to exercise their rights such as claiming compensation or taking legal action. The development of specific guidelines on Art. 86 AI Act thus forms the basis not only for ensuring transparency and accountability, but also for complying with the rule of law and strengthening democratic values. It is therefore crucial to create a foundation that is comprehensible and easily accessible to all people, and which will strengthen the general understanding of how artificial intelligence works.

3.2 Methodical approach to the project development

The present report forms part of a series of several documents that have been compiled within the framework of the project “Enlightenment 4.0 - Human understanding of AI decision-making”.

The project was divided into different phases, each with different objectives (refer to figure 1 for more details). Firstly, this substantiated theoretical report was prepared, which includes a legal analysis of the right to explanation in accordance with Art. 86 of the AI Act. The legal provisions on decision-making by AI-based systems partly coincide with existing provisions, such as Art. 22 GDPR on automated decisions in individual cases and the corresponding right to access under Art. 15(1)(h) GDPR. Consequently, synergies with the existing data protection law were established and built upon in the preparation of this report. Using relevant literature and current case law, these were expanded to include new instructions so that they can act as a kind of manual for a wide variety of bodies, employees and affected persons alike, and clearly reflect who is subject to which obligations and who is entitled to which rights. In order to ensure practical relevance as early as possible, concrete practical examples were selected to illustrate the sometimes abstract legal considerations in an understandable and practical way. The legal analysis was complemented by sociological and ethical considerations to provide a more comprehensive understanding of the relevance of the right to explanation in practice.

Building on this, a manual with specific guidance for businesses has been developed so that these can be trained in complying with the right to explanation under Art. 86 of the AI Act and have access to easy-to-follow instructions. A second manual was developed for consumers and their interest representatives so that they are aware of what information they can request, the questions they can ask and the options available to them in the event of inadequate information.[5]

In order to best reflect the perspectives of both the affected business sectors and consumers, the project included an extensive stakeholder consultation process. The results of several workshops held in this context were in turn incorporated into the key project documents as described. The project ran from June 2024 to April 2025 and concludes with the presentation of the two manuals and the report and a pilot training course on how to use them.

---

[5] Both manuals and the report can be downloaded from the website of the Austrian Federal Ministry of Labour, Social Affairs, Health, Care and Consumer Protection, where current studies and reports on consumer policy are published.

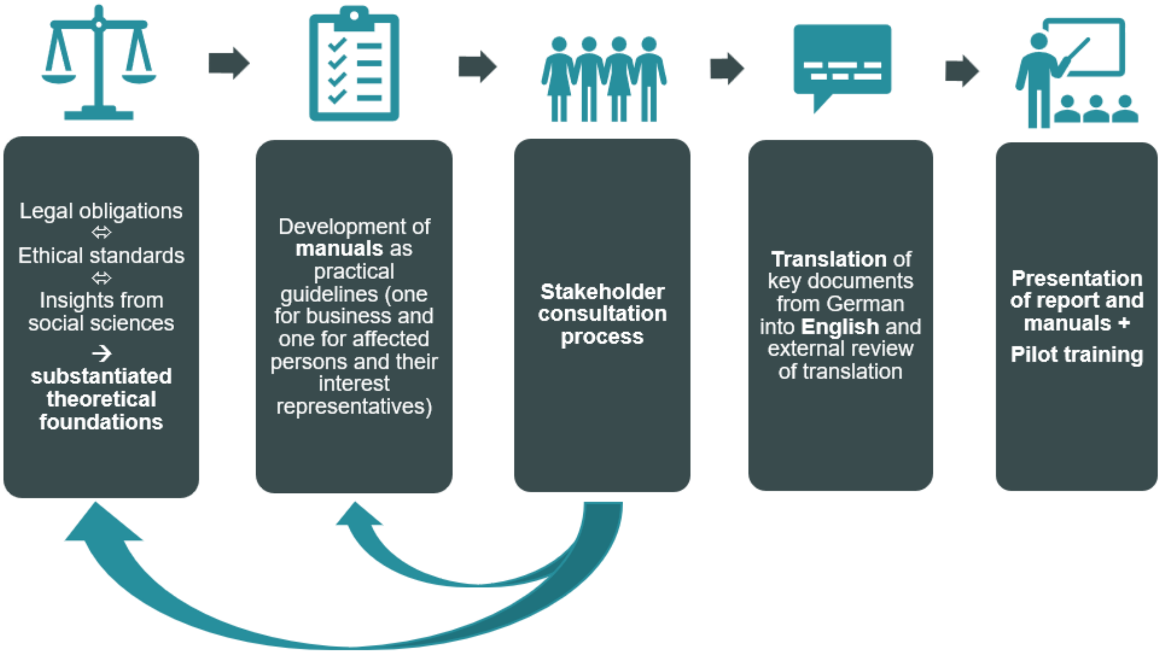

Legal obligations
⇔
Ethical standards
⇔
Insights from social sciences
→
substantiated theoretical foundations
Development of manuals as practical guidelines (one for business and one for affected persons and their interest representatives)
Stakeholder consultation process
Translation of key documents from German into English and external review of translation
Presentation of report and manuals +
Pilot training

Figure 1: Organisational steps of the project

3.3 Stakeholder consultation process

In order to ensure the practical relevance of the report and the associated manuals, the stakeholder consultation process represented a central component of the project, involving both business and consumer organisations. A number of stakeholder workshops were held in order to incorporate the perspectives of both consumers and businesses, as well as other relevant entities, and to improve the practical enforceability of the right to explanation. The participants' perspectives not only provided crucial insights for developing the theoretical foundations but also provided valuable input for the formulation of the use cases and the structure and design of the manuals.

In total three workshops were held between September 2024 and November 2024 to involve relevant stakeholders, during which perspectives, challenges and interpretations were shared and practical questions were discussed.

4 Introduction

The right to explanation of a decision as a right of the affected person, or rather the corresponding obligation of decision-makers to state reasons, has the function of making the legality of decisions verifiable and of giving the affected persons the opportunity to obtain sufficient information about a decision concerning them as well as to protect their rights. In addition, the right to explanation is an important premise to exercise other rights of the persons affected, as can be illustrated using the example of the GDPR: Art. 15 GDPR regulates the right to access of persons whose personal data is processed. This right is among the most frequently exercised rights under the GDPR and represents a “gateway” to the exercise of other relevant rights, such as the right to erasure and the right to rectification of data.[6]

In the age of the increased use of AI-based systems in decision-making procedures, it is important to rethink the right to explanation and to address the associated challenges in the interest of the persons affected. AI-based systems often operate in a way that is difficult for humans to understand. Since they frequently utilise opaque mechanisms, comprehensible explanations of the underlying rationale behind specific outcomes are often lacking.[7] This so-called “black box problem” emphasises the need to make AI-supported decisions more transparent and has led to the emergence of an entire field of research, “eXplainable AI” (XAI). Even if there is no standardised definition of XAI to date, this field basically comprises two dimensions: On the one hand, XAI refers to the development of white/glass-box or ante-hoc interpretable models that provide generic (global) explanations of mechanisms and thus can be interpreted in their entirety, detached from an individual decision.[8] On the other hand, it refers to the focus on AI systems that not only make precise predictions or decisions, but can also provide (local) explanations of how a specific decision or conclusion was reached (so-called post-hoc interpretability).[9] This implies that XAI should be able to explain the operations it performs, predict the next steps and disclose the sources of information used for decision-making so that users can understand the reasons for an automated decision.[10]

In both areas there are numerous different models (linear/logistic regression, decision trees) and techniques. These include the highlighting of the most significant features (feature-importance/feature-salience, i.e. e.g. colour coding of the most important pixels in image recognition), the provision of examples or information on which features would have to change

---

[6] Cf. *Datenschutzkonferenz*, Deutsche Datenschutzaufsichtsbehörden beteiligen sich an CEF 2024. Beginn der koordinierten Aktion zum Auskunftsrecht, https://datenschutzkonferenz-online.de/media/pm/2024-02-28_DSK-PM_CEF-2024-Auskunftsrecht.pdf (last access: 14 February 2025).

[7] Cf. *Winikoff/Sardelic*, Artificial Intelligence and the Right to Explanation as a Human Right, IEEE Internet Computing 2021, 108 (108).

[8] Cf. *Winikoff/Sardelic*, IEEE Internet Computing 2021, 108 (108).

[9] Cf. *Cervera Navas*, Explainable Artificial Intelligence needs Human Intelligence, https://www.edps.europa.eu/press-publications/press-news/blog/explainable-artificial-intelligence-needs-human-intelligence_en (as at 2 June 2023).

[10] Cf. *Cervera Navas*, Explainable Artificial Intelligence needs Human Intelligence, https://www.edps.europa.eu/press-publications/press-news/blog/explainable-artificial-intelligence-needs-human-intelligence_en (as at 2 June 2023).

minimally to alter the outcome of the decision (counterfactuals) and, since the spread of Large Language Models, increasingly also explanations in natural language.[11] XAI and the explainability of decisions are widely regarded as an essential component of transparency, which in turn supports trust in AI-based systems.[12] The obligation to explain decisions is thus a common element in establishing accountability.[13] For this reason, the right to explanation was included in the AI Act and enshrined in Art. 86 in the final version of the regulation as the right to explanation of individual decision-making in the form of a right of the affected persons. Art. 86 AI Act grants persons affected by a decision made by the deployer on the basis of the output of certain high-risk AI systems the right to receive a clear and meaningful explanation of the role of the system in the decision-making procedure and the main elements of the decision. In this way, the AI Act aims to grant further protection to affected persons who are already in a vulnerable position in relation to organisations using AI, as they have no insight into the organisations' AI-based processes and the complexity of these mechanisms, and to redress, at least to some extent, the resulting imbalance of power between the parties involved.[14] In addition, the explanation of an AI-based decision allows the affected person to legally challenge the decision, offers developers insight into possible negative side effects of the system and generally contributes to increasing the legitimacy of the decision.[15] However, Art. 86 AI Act does not provide precise instructions as to what information the explanation must contain and what form it must take. The subsequent section will therefore analyse this provision and its essential components in conjunction with the relevant data protection provisions. To this end, the legal background of the relevant legal frameworks - namely the GDPR and the AI Act - is first explained and their relevance to the present project is demonstrated. This is followed by a description of the selected use cases, which were concretised and formulated in more detail during the stakeholder workshops. The focus is on the following use cases:

1. Pricing in life and health insurance (Use Case 1)

2. Customer churn prediction (Use Case 2)

3. Evaluation of creditworthiness and credit scoring (Use Case 3)

4. Emotion recognition in marketing and sales promotion (Use Case 4)

Subsequently, the relevant data protection provisions are explained. The core of this report is

---

[11] With further references *Molnar*, Interpretable Machine Learning. A Guide for Making Black Box Models Explainable², https://christophm.github.io/interpretable-ml-book/ (as at 31 July 2024).

[12] Cf. e.g. *AI HLEG*, Ethics Guidelines for Trustworthy AI (2019), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425.

[13] *Yeung/Ranchordas*, An Introduction to Law and Regulation. Text and Materials² (2024) 372 et seq.

[14] Cf. *Dirutigliano*, Some considerations on the relationship between the right to a reasoned decision and the right to explanation in the proposal of the Artificial Intelligence Act, https://digi-con.org/some-considerations-on-the-relationship-between-the-right-to-a-reasoned-decision-and-the-right-to-explanation-in-the-proposal-of-the-artificial-intelligence-act/ (as at 4 October 2023).

[15] Cf. *Asghari/Birner/Burchardt/Dicks/Faßbender/Feldhus/Hewett/Hofmann/Kettemann/Schulz/Simon/Stolberg-Larsen/Züger*, What to explain when explaining is difficult? An interdisciplinary primer on XAI and meaningful information in automated decision-making (2022) 1, https://graphite.page/explainable-ai-report/.

the analysis of the right to explanation under Art. 86 AI Act, the essential content of which is elaborated and illustrated by means of the above-mentioned use cases. Finally, social science and ethical aspects of the right to explanation are presented in order to provide a broader picture of both the rights of the persons affected and the corresponding obligations of companies that use AI-based systems in decision-making procedures.

5 Legal analysis of the right to explanation

5.1 Introduction

The right to explanation in relation to automated or AI-based individual decision-making, as outlined in Art. 86 AI Act, is not a recent development. The GDPR already contains provisions on automated decision-making and provides for a corresponding right of access. Pursuant to Art. 22 GDPR, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless certain conditions are met. Art. 15(1)(h) GDPR enshrines a corresponding right to access, which is defined as the obligation of the controller to provide data subjects with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing.

The potential scope of application of Art. 22 GDPR (in conjunction with Art. 15(1)(h) GDPR) for a variety of AI systems gives rise to the question of the interaction of these provisions with Art. 86 AI Act.[16] This is because, in principle, the AI Act applies alongside the GDPR and does not affect the application of the GDPR, whereas in other areas there may be overlaps between the two regulations.[17] One such area could be the right to explanation, if an AI system processes personal data (as defined by Art. 4(1) GDPR) and takes a solely automated decision (as defined by Art. 22 GDPR). In such cases, both the GDPR and the AI Act may be applicable.[18] An illustrative example would be an AI-based system employed in the evaluation of the creditworthiness of natural persons, wherein an individual's 'credit score' is determined by the AI system through an analysis of specific personal attributes, including but not limited to age, gender, marital status and registered address, and consequently utilised to determine the approval of a loan application.[19]

It is evident that there is a close link between the provisions of the GDPR and the AI Act with regard to algorithmic individual decision-making and the right to explanation. This is why the chapter at hand focuses on the analysis of the legal framework of these norms, as well as their intersections. The subsequent elaborations are intended to furnish readers with a comprehensive understanding of the extent to which elements of the right of access under Art. 15(1)(h) GDPR are reflected in Art. 86 AI Act. Furthermore, this chapter will indicate the conclusions that can be drawn from the extant literature and case law on the relevant provisions of the GDPR and its application to the AI Act.

---

[16] Cf. *Paal/Hüger,* Die KI-VO und das Recht auf menschliche Entscheidung, MMR 2024, 540 (542).

[17] Cf. *Paal/Hüger,* MMR 2024, 540 (542).

[18] Cf. *Paal/Hüger,* MMR 2024, 540 (542).

[19] Cf. the decision of the ECJ on the German credit reference agency SCHUFA, which provides its contractual partners with information on the creditworthiness of third parties, in particular, consumers: ECJ 7 Dec. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957.

5.2 Legal framework

5.2.1 General Data Protection Regulation (GDPR)

The GDPR, which was adopted in 2016, has been directly applicable since May 2018 and aims to eliminate the fragmentation of data protection within the EU Member States and the resulting legal uncertainties.[20] The GDPR is therefore part of a comprehensive EU approach to the digitalisation of society and the economy. The overarching objectives of this approach are to preserve the freedoms and fundamental rights of individuals, democracy and the rule of law in the face of digital change, and to ensure that natural persons remain in control of their own data.[21] A fundamental component of the GDPR is the protection of personal data whilst also enabling the free movement of data[22], rendering this legal act an essential source of knowledge for the interpretation of the fundamental rights guaranteed in the CFR, in particular Art. 8.[23] On the one hand, the GDPR is based on the so-called market place principle, which provides that European consumers and data subjects are protected by its regulations, regardless of the location of data processing.[24] In addition, the establishment principle, as outlined in Art. 3 (1) GDPR, stipulates that the GDPR applies to data processing that occurs in the context of the activities of a European establishment of a company or other institution.[25] A pivotal aspect of the GDPR is the promotion of transparency for data subjects. Additionally, the GDPR enshrines the principles of data protection by design ("privacy-by-design") and data protection by default ("privacy-by-default"), emphasising the incorporation of these principles into technological frameworks to safeguard personal information. The GDPR employs a risk-based approach, necessitating a data protection impact assessment prior to certain high-risk data processing operations (cf. Art. 35 GDPR).[26] The GDPR also comprises a catalogue of data subject rights, including the right of access (Art. 15), the right to rectification (Art. 16), the right to erasure (Art. 17), the right to restriction of processing (Art. 18) and comprehensive information obligations (Art. 13 and 14).

With regard to the subject matter (i.e. the material scope of application), the GDPR governs the protection of personal data when it is processed.[27] According to Art. 4(1), the GDPR defines this as "[...] any information relating to an identified or identifiable natural person". A person is identified if the data user can identify the respective person, for instance through the allocation of an identifier such as a name, an identification number, geographical location data or an online identifier.[28] A person is considered identifiable if they are not currently identified, but can be identified directly or indirectly with a reasonable effort based on existing information, e.g.

---

[20] Cf. *Voigt/Bussche*, EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch² (2024) 2.

[21] Cf. *Köllmann*, Implementierung elektronischer Überwachungseinrichtungen durch Betriebsvereinbarungen vor dem Hintergrund der DSGVO (2021) 184; *Weichert* in *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG. Kompaktkommentar³ (2024) Einleitung para. 24.

[22] Cf. also the objectives of the GDPR in Art. 1.

[23] With further references *Weichert* in *Däubler et al,* EU-DSGVO³ Einleitung para. 24.

[24] For the territorial scope of the GDPR, cf. Art 3.

[25] Cf. *Köllmann*, Implementierung 197.

[26] *Weichert* in *Däubler et al,* EU-DSGVO³ Einleitung paras 27 et seq.

[27] *Scheichenbauer*, Datenschutz für Vereine² (2023) 1.

[28] *Scheichenbauer*, Datenschutz für Vereine² 11.

by association with an identifier such as a name or other characteristics that are an expression of physical, economic, cultural, etc. identity.[29]

In order to fall within the scope of protection of the GDPR, personal data must be processed. This includes any operation which is performed on personal data, such as the collection, recording, organisation, storage, retrieval, etc. of such data (Art. 4(2) GDPR). It does not matter whether the processing is carried out using automated or digital means, which is why, for example, the organisation of personal data in paper files can also constitute processing within the meaning of the GDPR, if certain conditions are met.[30]

In terms of personal scope, the GDPR applies to "controllers", which includes any natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data (Art. 4(7) GDPR). The GDPR imposes specific obligations on the role of the controller. For example, under certain conditions, the controller is obliged to conduct a data protection impact assessment prior to certain data processing. Additionally, data subjects are entitled to exercise their rights against the controller. The controller must also take appropriate technical and organisational measures to ensure that personal data is processed lawfully. If there are several controllers, they must conclude an agreement on the allocation of data protection obligations (Art. 26 GDPR). However, if an entity only carries out the data processing on behalf of a controller and does itself not determine the purposes and means of the processing, the entity in question is the processor (Art. 4(8) GDPR). It is imperative to differentiate the allocation of roles in order to accurately determine the appropriate benchmarks with regard to data protection obligations.[31]

Data protection is a fundamental right, thus the GDPR is predicated on the principle that the processing of personal data is generally prohibited, unless there is a legal basis authorising it. The possible legal bases for data processing are listed exhaustively in Art. 6 GDPR and include, for example, the consent of the data subject, the protection of vital interests of the data subject or the legitimate interest of the controller.

---

[29] Cf. Art. 4 (1) GDPR and *Scheichenbauer*, Datenschutz für Vereine² 11.

[30] Cf. *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 13.

[31] Cf. *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 25.

Article 6 GDPR

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

If the processed data are special categories of personal data within the meaning of Art. 9 GDPR - so called "sensitive data" - the GDPR applies stricter standards.[32] Sensitive data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation (Art. 9(1) GDPR). The processing of these categories of personal data is particularly sensitive, as they concern the most intimate areas of life and their processing may entail significant risks for the fundamental rights and freedoms of data subjects (Recital 51 GDPR), which is why their processing (in addition to the existence of a legal basis under Art. 6(1) GDPR[33]) is only allowed under the strict conditions of Art. 9(2) GDPR (e.g. with the explicit consent of the data subject or for reasons of public interest based on Union or national law).

In any case, data processing is required to be conducted in accordance with specific general

---

[32] Cf. *Scheichenbauer*, Datenschutz für Vereine² 33.
[33] Cf. ECJ 21. 12. 2023, C-667/21, *Krankenversicherung Nordrhein,* ECLI:EU:C:2023:1022.

principles that are pertinent across the scope of the GDPR.[34] Article 5(1) GDPR enumerates specific processing principles that, despite their abstract nature, are directly applicable obligations, thereby adding an objective dimension to the rights of data subjects.[35] They can be regarded as a "brief description of the GDPR" in the form of binding basic principles, which are predominantly concretised in Art. 5 ff GDPR.[36]

1. **Lawfulness, fairness and transparency:** Processing must be carried out in a manner that is comprehensible to the data subject and may only take place if it is permitted by one of the previously described legal bases. The principle of transparency assumes particular significance for this report, in that it already prohibits surreptitious data processing,[37] and that the provision of information pertaining to data processing to data subjects must be conducted in a manner that is unambiguous and readily comprehensible, which is the core of the information obligations under Articles 13 and 14 and the right of access under Article 15 GDPR.[38] Compliance with this principle requires that data subjects are comprehensively informed about the purposes for which their data is processed and are properly and comprehensively informed about the conditions of data collection.[39] This applies to both past and future data processing.[40]

2. **Purpose limitation:** Data processing is permitted only for specified, clear and legitimate purposes, and further processing of data must not be undertaken in a way that is incompatible with these purposes. The purpose must be documented specifically and not in a generalised manner and must be legally compliant.[41] While the purpose can be defined by the controller, this definition must be documented internally (in the records of processing activities) and disclosed externally (to the data subject).[42] The reason for this purpose limitation is to protect the data subject by limiting the unrestricted and uncontrolled use of data.[43]

3. **Data minimisation:** Data processing must be relevant to the purpose and limited to what is necessary. This principle assumes particular significance in the context of the increasing importance of big data applications, as the processing of vast quantities of data becomes increasingly feasible, and thus a limitation by law is required.[44] The principle of data minimisation is considered to be adequately taken into account when the data processing promotes the defined purpose and, conversely, data is not processed if the processing purpose can be achieved without it.[45] In this context, it is

---

[34] Cf. *Köllmann*, Implementierung 198.

[35] Cf. *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. Kommentar^4 (2024) Art 5 DSGVO para. 1

[36] *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG^8 (2024) Art 5 DSGVO para. 1.

[37] Cf. *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung^4 Art 5 DSGVO para. 18.

[38] Cf. *Voigt/Bussche*, EU-Datenschutz-Grundverordnung^2 164.

[39] Cf. *Scheichenbauer*, Datenschutz für Vereine^2 18.

[40] With further references *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer^8 Art 5 DSGVO para. 17.

[41] Cf. *Köllmann*, Implementierung 203; *Voigt/Bussche*, EU-Datenschutz-Grundverordnung^2 165.

[42] Cf. *Scheichenbauer*, Datenschutz für Vereine^2 19.

[43] Cf. *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer^8 Art 5 DSGVO para. 23.

[44] Cf. *Köllmann*, Implementierung 205.

[45] With further references *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung^4 Art 5 DSGVO para. 57.

imperative to consider whether the purpose can also be achieved with aggregated data (value intervals as opposed to precise values) or with anonymised data, for example.[46] The requirement of appropriateness of data processing refers to whether the intended purpose of the processing can be achieved at all with the envisaged personal data. The principle of relevance asks about the suitability of certain types of data for the purposes pursued.[47]

4. **Accuracy:** Data must be factually correct and - where necessary - up to date. The guiding principle is that the processed data must reflect reality as accurately as possible at all times.[48] Measures must be taken to delete or correct any data that does not fulfil this requirement. This principle corresponds to the right to rectification laid down in Art. 16 GDPR and the right to erasure under Art. 17 GDPR.[49] Furthermore, specific updating obligations arise, particularly in the context of long-term storage, although the controller is not obligated to make a significant effort in each instance.[50]

5. **Storage limitation:** Data that enables a data subject to be identified may not be stored for longer than is absolutely necessary for the processing purposes. Personal data should therefore only have a limited "lifetime"[51] and either be deleted after a certain period of time or their personal reference removed.[52] In order to implement the principle of storage limitation, the controller should ensure the regular review of the data and deadlines for erasure and also communicate these in accordance with the information obligations under Art. 13 and 14 GDPR.[53]

6. **Integrity and confidentiality:** It is imperative that adequate security measures are implemented to ensure the protection of personal data during processing. This involves safeguarding against unauthorised or unlawful processing, accidental loss, destruction or damage. This implies the obligation to protect personal data from falsification ("integrity") and from unauthorised access ("confidentiality").[54] This principle is concretised in Art. 32 GDPR through specific requirements for secure data processing.[55]

Art. 5(2) GDPR stipulates that the controller must be **accountable** for and able to demonstrate compliance with these processing principles. This results in a substantial augmentation in the workload involved in fulfilling the associated documentation obligations. For instance, consent must be verifiable, and the data controller must document the fulfilment of the data subject

---

[46] Cf. *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung^4 Art 5 DSGVO paras 57 et seq.
[47] With further references *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer^8 Art 5 DSGVO paras 39 et seq.
[48] Cf. *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 168.
[49] Cf. *Köllmann*, Implementierung 205.
[50] Cf. *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer^8 Art 5 DSGVO paras 44 et seq.
[51] Cf. *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer^8 Art 5 DSGVO para. 50.
[52] Cf. *Scheichenbauer*, Datenschutz für Vereine² 20.
[53] Cf. *Voigt/Bussche*, EU-Datenschutz-Grundverordnung² 169; *Köllmann*, Implementation 206.
[54] Cf. *Kramer* in *Eßer/Kramer/Lewinski*, Auernhammer^8 Art 5 DSGVO para. 55.
[55] Cf. *Köllmann*, Implementierung 206.

rights and information obligations.[56]

This extract from the most important principles of the GDPR clearly demonstrates their main purpose, namely the strengthening of data subjects' rights, which the GDPR lists in the taxative enumeration in Chapter III (Art. 12 to 23).[57] In addition to the data subjects' rights that require filing a request, such as the right to rectification or access, the information obligations under the GDPR also play an important role. This is because a person is only able to enforce their rights if they are aware of the processing operations concerning them, thus the information obligations must be fulfilled by the controller regardless of a request.[58] Therefore - as can also be seen from Recital 39 GDPR - providing data subjects with information should increase the transparency of processing operations and enable the effective exercise of data subjects' rights.[59] The provisions relevant to this report are presented in detail in Section 5.4.

---

[56] Cf. *Scheichenbauer*, Datenschutz für Vereine² 21.
[57] Cf. *Scheichenbauer*, Datenschutz für Vereine² 70.
[58] Cf. *Scheichenbauer*, Datenschutz für Vereine² 70.
[59] Cf. *Voigt/Bussche*, EU General Data Protection Regulation² 240.

5.2.2 AI Act

5.2.2.1 Introduction

As previously stated in the introduction, the AI Act, which was published in the Official Journal of the European Union in July 2024, represents the culmination of the EU's efforts to establish the first Europe-wide horizontal regulation of AI, that is to say, a regulation that is sector-independent. This development follows a series of initiatives at EU level, which have become increasingly specific and range from declarations and ethical guidelines to the White Paper on Artificial Intelligence.[60]

The initial conception of the AI Act as a product safety law,[61] akin to the Medical Devices Regulation,[62] served as the primary foundation for its development. This approach was subsequently “enriched”, primarily due to the endeavours of the European Parliament (EP), which resulted in the incorporation of rights of the affected persons, including the right to explanation.

The AI Act is a multifaceted piece of legislation that aims to achieve a number of objectives. Firstly, it seeks to “improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence”. On the other hand, it aims to ensure “a high level of protection of health, safety, fundamental rights enshrined in the Charter [...] against the harmful effects of AI systems in the Union and supporting innovation” (Art. 1(1) AI Act).

5.2.2.2 Scope of application

In terms of the **material scope** of the AI Act, the primary focus concerns the concept of an AI system (Art. 3(1) AI Act). The definition of an AI system was a principal point of discussion in the “legislative process.”[63] The final version of the AI Act defines AI systems on the basis of various characteristics, including the following: machine-based system, varying degrees of autonomy, possible adaptiveness after deployment, inputs, explicit or implicit objectives, inference of outputs that can influence physical or virtual environments.

---

[60] With further references *Hilgendorf*, Entstehungsgeschichte und Leitwerte, in *Hilgendorf/Roth-Isigkeit* (eds.), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 1 (10 et seq.); *Zenner*, Entstehungsgeschichte, in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) para. 1 (paras 1 et seq.).

[61] The AI Act follows the so-called New Legislative Framework (NLF), an EU concept of product regulation with uniform core elements (conformity assessment procedures, frequently controlled self-regulation, essential requirements are defined and concretised by standards), with further references *Ebers*, Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag, RDi 2021, 588 (589); *Veale/Zuiderveen Borgesius*, Demystifying the Draft EU Artificial Intelligence Act, CRi 2021, 97 (102).

[62] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) 178/2002 and Regulation (EC) 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (MDR), OJ L 2017/117, 1.

[63] With further references *Burtscher/Fellner/Raabe-Stuppnig*, Klassifizierung und Risikobewertung von KI-Systemen nach dem Entwurf für ein EU Gesetz über Künstliche Intelligenz, ZIIR 2023, 382 (382); *Fülöp*, AI Act. Das Ende europäischer Innovation oder Gefahr für den Datenschutz? Dako 2023, 82 (82); *Gless/Janal*, Anwendungsbereich und Adressaten, in *Hilgendorf/Roth-Isigkeit* (eds.), Die neue Verordnung der Europäischen Union zur Künstlichen Intelligenz (2023) 15 (18 et seq.).

Definition AI

‘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 (Cf. Article 3(1) AI Act).

The most significant distinguishing feature among these is the capacity to “infer”,[64] a capability that can be fulfilled by both machine learning and logic- and knowledge-based systems. According to Recital 12 of the AI Act, the definition of AI system “should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations" and should help to distinguish them "from simpler traditional software systems or programming approaches". On 6 February 2025, the European Commission published (non-binding) guidelines to clarify the term AI system.[65] These clarify, among other things, that simple machine learning approaches such as linear or logistic regression methods do not qualify as AI systems.

In terms of the **temporal scope of application** of the AI Act, its provisions regarding prohibited practices apply from 2 February 2025 and the provisions related to high-risk AI systems will become applicable on 2 August 2026, with the exception of systems pursuant to Art. 6(1) in conjunction with Annex I AI Act (Art. 113 AI Act). However, Art. 111 (2) AI Act contains a so-called "grandfathering" clause, according to which the AI Act only applies to operators of high-risk AI systems that were placed on the market or put into service before 2 August 2026 if those systems are subject to significant changes in their design. Consequently, the right to explanation pursuant to Art. 86 AI Act would not apply to high-risk AI systems, which have been placed on the market or put into service before 2 August 2026 and have not been subject to significant changes. However, it should be noted that in many cases an adaptation of the system and thus a significant change in the design will be necessary in order to maintain compliance with other legal provisions (e.g. anti-discrimination law, the legislator’s obligation of protection, data protection law). For instance, the algorithm of the Austrian Public Employment Service, the so-called "AMS-Algorithmus" has been criticised for its inability to reflect the present state of the labour market, as it was developed prior to the COVID-19 pandemic.[66] In such a case, the system would require an update, causing it to fall within the scope of the AI Act. This would mitigate the risk of an "abuse" of this clause by permanently

---

[64] With further references *Wendehorst/Nessler/Aufreiter/Aichinger*, Der Begriff des "KI-Systems" unter der neuen KI-VO, MMR 2024, 605.

[65] Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 924 final.

[66] *Wimmer*, AMS-Algorithmus. „Seit Corona ist Datenbasis wertlos“, https://futurezone.at/netzpolitik/ams-algorithmus-seit-corona-ist-datenbasis-wertlos/401101638 (As at 18 November 2020).

refusing to update it.

With regard to the **personal scope of application**, a distinction must be made within the relevant actors. Firstly, the AI Act applies to providers of AI systems,[67] i.e. primarily developers. Secondly, the AI Act applies to professional users who use the AI system on their own responsibility, i.e. for their own account or at their own risk (so-called deployers[68]). The majority of the requirements are aimed at providers of AI systems.[69] The scope of application of the AI Act primarily concerns providers who place AI systems on the market or put them into service in the Union, irrespective of whether these providers are established or located within the Union or in a third country. Deployers of AI systems that have their place of establishment or are located within the Union are also covered. With this wording, the AI Act intends to cover both legal entities and natural persons and links its applicability to the place of establishment or habitual residence.[70] Subsidiarily, providers and deployers of AI systems that have their place of establishment in a third country or are located in a third country also fall within the scope of application if the output generated by the AI system is used in the Union.

The AI Act follows a risk-based approach, with the objective of ensuring proportionality in the implementation of regulatory measures.[71] The severity of the risk, as determined primarily by its impact on fundamental rights, corresponds to the extent of the regulatory measures employed. With this, the AI Act intends to prevent unnecessary impediments to innovation. The category of high-risk AI systems is particularly pertinent to the present project, as Art. 86 AI Act only applies to certain high-risk AI systems. Furthermore, the AI Act prohibits certain practices as they are contrary to the fundamental values of the Union. It is important to note that these practices may overlap with the relevant high-risk AI systems in certain areas or regarding specific AI systems and thus have to be distinguished from each other.

Additionally, transparency obligations are imposed on systems with lower risk potential than those in the preceding levels.[72] It should be highlighted that the transparency obligations may also apply (to a limited extent) to high-risk AI systems. Consequently, they do not constitute a separate, detached level. Irrespective of the categorisation of the AI system, the requirements for the necessary AI literacy pursuant to Art. 4 AI Act also apply. The regulations on AI regulatory sandboxes (Articles 57 to 61 AI Act) are also not explicitly aimed at a specific risk level.

---

[67] I.e. "a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge" (Art. 3(3) AI Act).

[68] I.e. "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" (Art. 3(4) AI Act).

[69] It should be noted that pursuant to Art. 25 AI Act it is possible for a deployer to become a (new) provider under certain circumstances, e.g. in the event of a change of purpose.

[70] *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 2 para. 21.

[71] With further references *Kaminski*, Regulating the Risks of AI, Boston University Law Review 2023, 1347.

[72] Cf. Recital 26 AI Act.

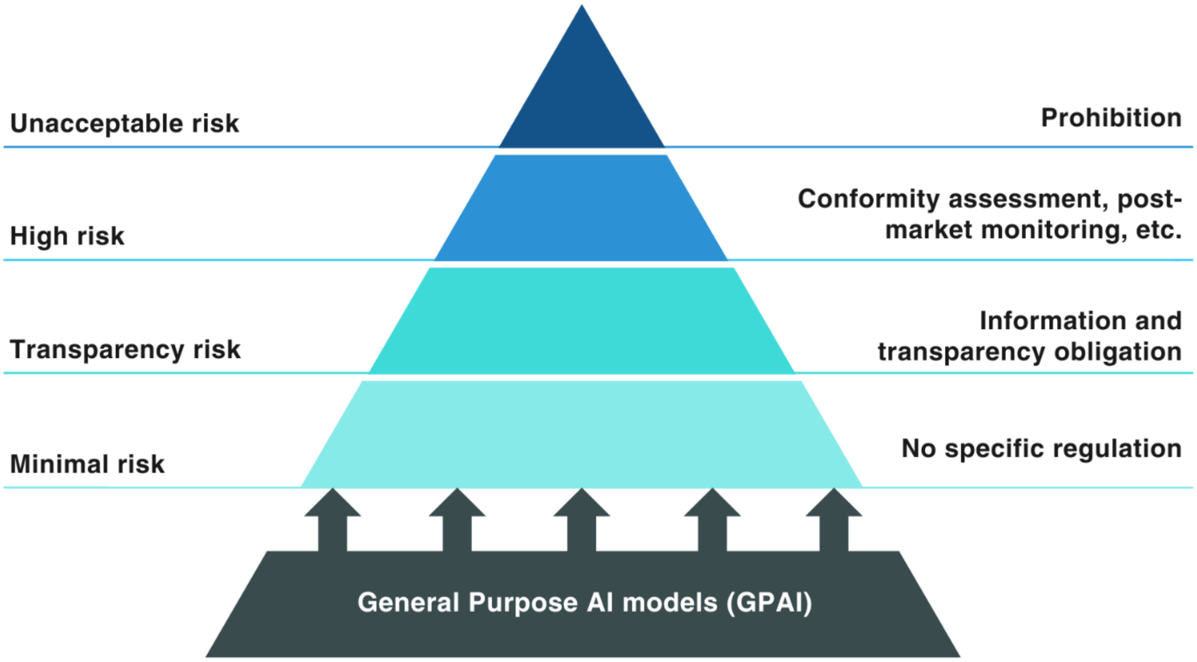

Unacceptable risk
Prohibition
High risk
Conformity assessment, post-market monitoring, etc.
Transparency risk
Information and transparency obligation
Minimal risk
No specific regulation
General Purpose AI models (GPAI)

Figure 2: Own illustration of the risk levels of the AI Act based on the EU Commission's pyramid[73]

5.2.2.3 Prohibited AI practices

As Recital 28 states, AI "can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices." As these practices are "particularly harmful and abusive", they should be "prohibited because they contradict Union values". The focus, therefore, is on AI practices that present an unacceptable risk.[74] These prohibited practices are listed in Art. 5 AI Act.[75]

The following prohibited practices are of particular relevance to the project, as they pertain to similar areas such as some of the use cases and thus must be distinguished accordingly.

- AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is

---

[73] Vorlage: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

[74] Cf. in particular Recitals 26 and 179 AI Act; Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union acts, COM(2021) 206 final), 5.2.2.

[75] With further references *Neuwirth*, Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA), CLSR 2023, 1 (3 et seq.); *Rostalski/Weiss*, Verbotene KI-Praktiken, in *Hilgendorf/Roth-Isigkeit* (eds.), Die neue Verordnung der Europäischen Union zur Künstlichen Intelligenz (2023) 35.

reasonably likely to cause that person, another person or group of persons significant harm. (Art. 5(1)(a) AI Act)

- AI systems that exploit any of the vulnerabilities of a natural person or a specific group of persons 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. (Art. 5(1)(b) AI Act)
- AI systems to infer emotions of a natural person in the areas of workplace and education institutions. (Art. 5(1)(f) AI Act)

This raises the question of whether, for example, the placement of advertising (e.g. to people with a gambling addiction) exploits their vulnerability and would therefore be prohibited. Additionally, complex problems of demarcation arise in relation to emotion recognition, which is prohibited in the areas of workplace and education institutions, but outside of these areas falls into the group of high-risk AI systems (refer to Section 5.3.4. for further details).

5.2.2.4 High-risk AI systems

Within the framework of the AI Act's risk levels, "high-risk AI systems" are designated as the subsequent tier following prohibited AI practices, and are subject to the majority of the regulatory provisions (Articles 6 to 49 AI Act).

AI systems can classify as high-risk in two cases:

- Firstly, so-called "embedded high-risk AI systems", i.e. product or safety components as defined in Art. 6(1) AI Act, which already fall within the scope of EU product safety law (e.g. medical devices).[76] This category is not relevant to the present project.
- Secondly, "stand-alone high-risk AI systems" as defined in Art. 6(2) in conjunction with Annex III AI Act, which describes eight high-risk application areas and specific use cases.

Section 9.1 provides a list with an overview of the respective high-risk AI areas listed in Annex III AI Act with the corresponding specifications.

Notwithstanding the utilisation of an AI system within one of these areas listed in Annex III AI Act, it may be exempt from being categorised as a high-risk AI system provided that “it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making” (Art. 6(3) AI Act).

In this regard, four alternative conditions are listed as follows:

- the AI system is intended to perform a narrow procedural task (e.g. conversion of

---

[76] With further references *Martini*, High-risk AI systems. Risikobasierter Ansatz, in *Hilgendorf/Roth-Isigkeit* (eds.), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 51 (62 et seq.); *Schwartmann/Pottkämper*, Hochrisiko-KI-Systeme gem Art. 6 Abs. 1 KI-VO (Anhang I), in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) para. 152 (paras 152 et seq.).

unstructured data into structured data, categorisation of incoming documents, detection of duplicates)

- the AI system is intended to improve the result of a previously completed human activity (e.g. improving the language of already captured documents, e.g. professional tone or more scientific language style)
- the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review (e.g. review of a teacher's grading pattern to subsequently check whether the teacher may have deviated from the grading pattern and, consequently, to alert possible inconsistencies or irregularities)
- the AI system is intended to perform a preparatory task to an assessment (e.g. intelligent solutions for processing files such as indexing, searching, text and language processing or linking data with other data sources; AI systems used to translate source documents)

Providers who consider that AI systems referred to in Annex III are not high-risk must document the corresponding assessment before these systems are placed on the market or put into service. This documentation must be submitted to the competent national authorities on request, and these providers are subject to the registration obligation pursuant to Art. 49(2) AI Act (Art. 6(4) AI Act).

Based on the selection of use cases, the following areas in Annex III are relevant to this project:

- "Biometrics", including "AI systems intended to be used for emotion recognition" (Annex III point (1)(c) AI Act)
- “Access to and enjoyment of essential private services and essential public services and benefits”, which includes "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score" (Annex III point (5)(b) AI Act)and "AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance" (Annex III point (5)(c) AI Act).

The areas of application resulting from points 1 and 5 are outlined below.

Emotion recognition systems

The term *emotion recognition system* refers to "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data" (Art. 3(39) AI Act). Biometric data means "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data" (Art. 3(34) AI Act).[77] This could involve the processing

---

[77] According to *Schwartmann/Keber/Steinbrück*, Emotionserkennungssysteme, in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) Rz 89 (Rz 90) or *Hansen/Nägele/Steinbrück*, Biometrische Identifizierung, Kategorisierung und Emotionserkennung natürlicher Personen, in *Schwartmann/Keber/Zenner*

of data pertaining to gait, voice, keystrokes, eye movements, gestures, heart rate, body temperature and skin conductivity.[78]

As outlined in the AI Act, emotion recognition encompasses the identification and analysis of various emotional responses, excluding physical states such as pain and fatigue. It also excludes simple obvious emotions like laughter, simple gestures, and speaking volume (refer to Section 5.3.4. for further details).[79]

Annex III point (1)(c) AI Act on emotion recognition supplements the prohibition of Art. 5(1)(f) AI Act, i.e. "AI systems to infer emotions of a natural person in the areas of workplace and education institutions"[80]. This could be relevant in the present project when using emotion recognition systems, especially at work, and would lead to a prohibition of such practices.

Creditworthiness and credit score

The assessment of creditworthiness can have serious effects on an individual's access to financial resources or essential services such as housing, electricity and telecommunication services. Consequently, AI systems used to evaluate the creditworthiness of natural persons are classified as high-risk AI systems. AI systems that calculate a credit score, e.g. by the credit reference agency SCHUFA, are also subject to this regulation.[81]

Risk assessment and pricing in the case of life and health insurance

Risk assessment and pricing in the case of life and health insurance, as outlined in the AI Act at the initiative of the European Parliament,[82] is intended to secure a non-discriminatory standard of living.[83] The inclusion of relevant AI systems as high-risk AI systems not only fosters equal treatment but also safeguards against opaque decision-making processes and related challenges in accessing legal protection.[84]

The classification of those AI systems as "high-risk" leads to improved risk mitigation, in particular through data quality requirements (Art. 10 AI Act), which can impact algorithmic discrimination, the necessity to establish a risk management system (Art. 9 AI Act), system

---

(eds.), KI-VO. Leitfaden für die Praxis (2024) Rz 165 (Rz 165), in general, the definition of biometric data under data protection law (Art. 4(14) GDPR) is applicable, but without restriction regarding unique identification; see section 5.3.4 for details.

[78] *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* para. 89 (paras 90 et seq.).

[79] With further references *Hansen/Nägele/Steinbrück* in *Schwartmann/Keber/Zenner* para. 165 (para. 171).

[80] Except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons.

[81] *Schwartmann/Köhler*, Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen, in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) para. 222 (para. 224).

[82] At this point, see already the call for the classification as a high-risk AI system in *Wendehorst*, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective (2021), https://www.sozialministerium.at/dam/sozialministeriumat/Anlagen/Themen/Konsumentenschutz/Konsumentenpolitik/The-Proposal-for-an-Artificial-Intelligence-Act-COM2021-206-from-a-Consumer-Policy-Perspective_dec2021__pdfUA.pdf.

[83] *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner* para. 222 (para. 229).

[84] *Ruschemeier* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Anhang III para. 48.

transparency requirements (Art. 13 AI Act) and human oversight requirements (Art. 14 AI Act). At the level of deployers, this classification also results in enhanced protection, as the right to explanation under Art. 86 AI Act is applicable to those systems. Furthermore, deployers of high-risk AI systems are obliged to carry out a fundamental rights impact assessment, provided that the conditions of Art. 27 AI Act are met.

5.2.2.5 Requirements for high-risk AI systems

Articles 8 to 15 of the AI Act contain the fundamental requirements for high-risk AI systems. These are primarily addressed to the providers of such systems and verified through a designated conformity assessment procedure. Regarding the project objective, the discussion below will focus exclusively on the requirements associated with Art. 86 AI Act and the subject of transparency. As Art. 86 AI Act is directed at deployers, and provider obligations are not at the centre of the project, the following elaborations are kept brief.

Technical documentation (Art. 11 AI Act)

Art. 11 AI Act states that before a high-risk AI system is placed on the market or put into service, technical documentation must be drawn up and kept up to date. The technical documentation primarily serves as a tool in the conformity assessment procedure, substantiating the AI system's compliance with Articles 8-15 AI Act. It is intended for notified bodies responsible for assessing conformity and (national) authorities. The minimum content requirements are outlined in Annex IV.[85] Additionally, the technical documentation could be pertinent for deployers, such as enabling them to conduct their own risk assessments.[86]

Record-keeping (Art. 12 AI Act)

In terms of traceability[87], Art. 12 AI Act stipulates that high-risk AI systems must technically allow for the automatic recording of events over the lifetime of the system, i.e. logging. This also addresses the black box problem.[88]

This function must enable the recording of events relevant for the identification of situations that may result in the high-risk AI-system presenting a risk or in a substantial modification, the facilitation of post-market monitoring and the monitoring of the operation of the high-risk AI-system.

---

[85] With further references *Spindler*, Anforderungen an Hochrisiko-KI-Systeme (außer Transparenz), in *Hilgendorf/Roth-Isigkeit* (eds.), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 93 (104 et seq.).

[86] *Hansen*, Technical Documentation (Art. 11 KI-VO) in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) para. 309 (para. 312).

[87] *Schwartmann/Keber/Köhler*, Aufzeichnungspflichten (Art. 12), in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) para. 319 (paras 319 et seq.).

[88] *Kumkar*, Transparenzanforderungen an Hochrisiko- und andere KI-Systeme, in *Hilgendorf/Roth-Isigkeit* (eds.), Die neue Verordnung der EU zur Künstlichen Intelligenz (2023) 109 (112).

Transparency and provision of information to deployers (Art. 13 AI Act)

The strongest link between Art. 86 AI Act and the requirements for high-risk AI systems is Art. 13 AI Act. This provision lays down transparency obligations for providers of high-risk AI systems towards deployers and consists of two components. On the one hand, Art. 13(1) AI Act states that high-risk AI systems must be "designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately". This is a functional form of transparency, intended to contribute to the usability of the system and compliance with the (other) requirements of the AI Act.[89] As noted in the literature, since the provision does not contain any specific measures, its (specific) implementation is left to the providers.[90] This leads to a certain degree of legal uncertainty. For example, reference is made to the specifications provided by (future) technical standards, guidelines and case law.[91]

On the other hand, Art. 13(2) AI Act stipulates that high-risk AI systems "shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers".

Art. 13(3) AI Act enumerates the minimum components of these instructions for use, including the characteristics, capabilities and limitations of performance of the high-risk AI system, the measures taken to ensure human oversight, including the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI systems by the deployers and, where applicable, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs.[92]

This information from the instructions for use might logistically be an important source for the right to explanation under Art. 86 AI Act.

---

[89] *Kumkar* in *Hilgendorf/Roth-Isigkeit* 109 (113).

[90] With further references *Schneeberger*, Machine Learning in der Verwaltung. Rechtsfragen der Black-Box-Problematik (2024) 424.

[91] *Schwartmann/Keber/Köhler*, Transparenz und Bereitstellung von Informationen für die Betreiber (Art. 13), in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) para. 329 (para. 332).

[92] *Schwartmann/Keber/Köhler* in *Schwartmann/Keber/Zenner* para. 329 (para. 335 et seq.).

5.3 Use cases and legal classification

The abstract nature of the law can often present a challenge when it comes to translating legal analyses into practice. To make the legal relevance of the requirements under discussion more tangible, the present report employs case studies. The use cases were selected with a view to illustrate areas of application of the legal provisions that are relevant and add practical value for companies and consumers.

To this end, first a detailed description of the selected use cases is provided, including an initial legal subsumption under the scope of application of the GDPR and the AI Act. These remarks form the basis for the further legal analysis of Art. 86 AI Act, which is carried out based on the selected case studies. The respective section (Section 5.5) therefore repeatedly refers to these use cases. In addition to a theoretical discussion, it also includes a step-by-step examination of whether the use cases fall within the scope of Art. 86 AI Act and how its requirements can be practically illustrated. The most important findings of the analysis of Art. 86 AI Act and the solution of the use cases are then summarised in Section 5.7 and presented in a comparative table with regard to the individual use cases.

5.3.1 Pricing of life and health insurance (Use Case 1)

5.3.1.1 General information

Personalised or dynamic pricing is increasingly finding its way into many areas of the private sector, such as the hotel industry,[93] the airline industry or online shops.[94] Insurance companies are also using approaches such as profiling to assess risk when issuing policies (e.g. in the case of automobile liability insurance based on the driving style risk profile or in the case of health insurance taking into account possible health risk factors).[95]

For example, a health or life insurance company might receive data on the purchasing behaviour of its policyholders and use it to identify "cost-intensive" policyholders through profiling analyses (e.g. identification of policyholders who are very likely to suffer from a serious illness).[96]

The processing of data from social networks is frequently employed for the purposes outlined above. For instance, life insurers have reportedly tried to calculate their customers' life expectancies based on their activities in social networks. Information from these networks can indicate whether a person leads an active lifestyle or has many interests, which speaks in favour of better health, or whether the person primarily stays at home. Moreover, profiling can be used in the insurance sector to identify those customers who continuously cause high

---

[93] *red*, Mehr Umsatz. Forscher rät Hoteliers zu KI, https://salzburg.orf.at/stories/3269685/ (as at 20 August 2024).

[94] With further references *Hafner-Thomic*, Personalisierte Preise im Online-Handel. Eine Untersuchung aus datenschutz-, verbraucher- und wettbewerbsrechtlicher Sicht (2024) 1 et seq.

[95] *Hafner-Thomic*, Preise 33.

[96] *Lorentz*, Profiling. Persönlichkeitsschutz durch Datenschutz? Eine Standortbestimmung nach Inkrafttreten der DSGVO (2020) 150.

claims.[97]

In the insurance sector in particular, there are concerns that the traditional solidarity principle inherent in social insurance could be undermined by personalised pricing if all members no longer pay the same contribution to cover the individually unknown health risks of all contributors.[98] These concerns also overlap with non-discrimination law issues.[99]

5.3.1.2 Legal assessment

For the purpose of pricing of life and health insurance, personality profiles are frequently utilised.[100] This process can therefore be considered a form of profiling, frequently occurring in the context of automated decision-making as outlined in Art. 22 GDPR.

The AI Act designates this area as high-risk AI systems. It falls under the category of "Access to and enjoyment of essential private services and essential public services and benefits" (Annex III point (5)(c) AI Act), "AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance". Rec. 58 AI Act justifies this categorisation by stating that "AI systems intended to be used for risk assessment and pricing in relation to natural persons for health and life insurance also have a significant impact on persons' livelihood and if not duly designed, developed and used, can infringe their fundamental rights and can lead to serious consequences for people's life and health, including financial exclusion and discrimination."

5.3.2 Churn Prediction (Use Case 2)

The primary objective of churn prediction is to facilitate the development of customer retention strategies. Churn prediction models aim to identify early indications of customer attrition and predict which customers may potentially depart from the company. Churn prediction serves as a useful and effective instrument for identifying customers who are at risk of leaving, and subsequently persuading them to remain by implementing suitable measures.[101]

The purpose of processing in customer retention is therefore frequently to avoid the termination of contracts through target group-oriented advertising measures by offering certain benefits to

---

[97] *Lorentz*, Profiling 22.

[98] *Hidar*, Rechtliche Grenzen smarter Preisgestaltung. Eine Untersuchung der rechtlichen Zulässigkeit dynamischer und personalisierter Preisgestaltung aus datenschutz- und lauterkeitsrechtlicher Perspektive (2021) 350.

[99] With further references *Bekkum/Zuiderveen Borgesius/Heskes*, AI, insurance, discrimination and unfair differentiation. An overview and research agenda[4], https://arxiv.org/abs/2401.11892 (as at 31 January 2025); *Zuiderveen Borgesius*, Price Discrimination, Algorithmic Decision-Making, and European Non-Discrimination Law, European Business Law Review 2020, 401; *Zuiderveen Borgesius/Bekkum/Ooijen/Schaap/Harbers/Timan*, Discrimination and AI in insurance. What do people find fair? Results from a survey, https://arxiv.org/abs/2501.12897 (as at 22 January 2025).

[100] *Lorentz*, Profiling 150.

[101] *Mittelstand-Digital Zentrum Spreeland*, Churn Prediction - Vorhersage von Kundenabwanderung mittels KI, https://www.digitalzentrum-spreeland.de/Kuenstliche-Intelligenz/KI-Blog/Churn-Prediction-Vorhersage-von-Kundenabwanderung-mittels-KI.html (last access: 14 February 2025).

selected (existing) customer relationships. To enable the selection of such customers, aggregated data is created from existing datasets of existing customer relationships on a regular basis in order to derive statements, probabilities and interpretations of customer behaviour. The results are then used to counteract the termination of contracts in time through marketing measures.

In this context, the processing ("cancellation prevention") is frequently divided into several sections that build on each other. Initially, the customer data from the internal data warehouse can be aggregated (A). Subsequently, a score value is calculated for each active customer data record (B). Finally, the software is used to analyse customer groups and determine a target group definition. The actual selection of people can be made in the operational campaign management system in the same way as the previous target group definition (C). In the final step, the offers are sent to the selected customers (D).

Looking at the processing schematically, the following picture often emerges: The data of the persons affected (customers) is used in four steps during processing. In the first step, the data is processed for analysis purposes, sometimes only in aggregated form and sometimes in pseudonymised form. In the second step, a model is created (group formation) with score values as the result. In the third step, the affected persons are assigned to the analysed target groups, and the specific target group is selected for the target group-oriented advertising measures. In the final (fourth) step, the specific advertising of the identified customers takes place.

5.3.2.1 Example of the scoring process

In this step, statistical methods are employed to identify customers with a high probability of cancellation. An artificial neural network is then used to shape the source data ("characteristics") into a model. The developed model is applied to each reference in question. Each reference is given an individual "cancellation score".

The cancellation scoring model compares significant patterns of those who cancel with those of those who do not. The references are then divided into several groups according to their cancellation probability.

5.3.2.2 Example of the application process

The marketing department selects a group of people for the customer loyalty campaign according to the requirements. Such marketing campaigns can be, for instance, "free months on renewal". The focus of the campaign is not on the individual, but on groups of people with a certain score. These groups are not automatically selected "by the system"; there is always a human intervention that can be traced back to a business decision and is determined by the respective head of department or head of marketing.

5.3.2.3 Legal assessment

According to the literature published to date, processing activities for the purpose of customer loyalty can be based on Art. 6(1)(b) GDPR (performance of a contract) or on Art. 6(1)(f) GDPR (balancing of interests), depending on the assessment of the contractual purpose. Consent-based processing is de facto generally not possible. Because it remains unclear how far the purpose of customer loyalty programmes is covered by the performance of a contract, and as the relevant literature predominantly refers to a balancing of interests, the present processing is based on Art. 6(1)(f) GDPR.[102]

According to *Gierschmann*, it should be possible to at least consider the processing that is usual for normal commercial sales (e.g. storage in a CRM system, analysis of purchasing behaviour for clustering into A-B-C customers, analysis of existing contracts to check new offers) as still covered by the original purpose.[103]

If there is compatible further processing within the meaning of Art. 6(4) GDPR, then Art. 13(3) GDPR must be observed according to which the controller must provide the data subjects with information on this other purpose and all other relevant information in accordance with Art. 13(2) GDPR prior to further processing.

For the present Use Case of cancellation prevention/churn prediction, it should be noted that there is usually no (fully) automated individual decision-making in accordance with Art. 22 GDPR, as controllers, through their responsible employees, select customer groups to which specific offers are usually made.

The situation may be assessed differently if the profiling process is particularly intrusive, such as tracking persons across websites, devices or services and where, for instance, groups of people with financial difficulties receive targeted and regular advertising for certain services.

In principle, AI applications in the area of churn prediction/cancellation prevention appear to be profiling. However, they do not seem to qualify as prohibited practices nor (in the absence of being listed in Annex III) as high-risk AI systems within the meaning of the AI Act.

Nonetheless, it should be noted that this categorisation can also be different depending on the specific design. For instance, if an emotion recognition system is integrated in the approach outlined above, this could result in a high-risk AI system within the meaning of the AI Act.

---

[102] (Deutsche) ***Datenschutzkonferenz***, Kurzpapier Nr. 3. Verarbeitung personenbezogener Daten für Werbung 1, https://www.lda.bayern.de/media/dsk_kpnr_3_werbung.pdf (as at 29 June 2017).

[103] *Gierschmann*, Gestaltungsmöglichkeiten bei Verwendung von personenbezogenen Daten in der Werbung, MMR 2018, 7 (12).

5.3.3 Credit scoring (Use Case 3)

Credit scoring is a practice that is carried out in a variety of sectors. From a business's perspective, it plays a central role in the minimisation of the risk of customer payment defaults. In the telecommunications sector, such checks are particularly relevant when hardware is handed over to customers upon the conclusion of mobile phone contracts. Banking institutions, on the other hand, use credit scoring mainly before granting credit. In the energy sector, too, credit scoring is becoming an increasingly significant tool, with credit agencies offering this service to energy suppliers.[104]

A salient issue with credit scoring is the lack of transparency in the scoring methods employed. The algorithms used to calculate credit scores may be based on incomplete or non-representative data.[105] On this basis, certain groups of consumers may be discriminated against due to their affiliation with a particular professional category[106] or the absence of a comprehensive credit history. Consequently, credit scoring systems have the potential to result in (actually) creditworthy applicants being rejected or receiving higher rate offers.[107]

5.3.3.1 Example of the credit scoring process

The process of credit scoring begins when a customer (hereinafter: the person) applies for a loan or wishes to enter into a contract for which the company makes advance payments. The person provides personal and financial information, such as proof of income and existing debts. The lender then obtains information from credit reference agencies that collect data on loans and payment defaults (in particular based on Art. 152 Austrian Trade Regulation Act[108]). Alternatively, the credit scoring can be carried out independently by the company, based on its own service provision or data that is also available to credit reference agencies in accordance with Art. 152 Trade Regulation Act. The information is analysed in conjunction with other factors, including the applicant's income and employment status. A credit score is then calculated on the basis of this data, with the aim of assessing the risk of non-payment. The lender then makes a decision on the application based on the person's creditworthiness. If the loan is granted, data is reported back to the credit reference agency throughout the repayment period.[109]

---

[104] *CRIF*, Energie- & Versorgungsunternehmen, https://www.crif.at/fuer-unternehmen/branchen/energie-versorgungsunternehmen/ (last access: 14 February 2025)

[105] *Chopra*, Current Regulatory Challenges in Consumer Credit Scoring Using Alternative Data-Driven Methodologies, Vanderbilt Journal of Entertainment and Technology Law 2021, 625 (628 et seq.).

[106] *Centaurus Media Ltd*, Bonität und Berufswahl. Einflussfaktoren, https://www.sberbankdirect.de/bonitaet-und-berufswahl-einflussfaktoren/ (last access: 29 January 2025)

[107] eag, Do Energy Suppliers Credit Score Organisations? https://eaguk.org/do-energy-suppliers-credit-score-organisations/ (last access: 14 February 2025)

[108] Gewerbeordnung 1994 – GewO 1994, BGBl 194/1994 idF BGBl I 150/2024 (Austrian Trade Regulation Act).

[109] *Oberwalder*, Bonitätsdatenbanken und deren datenschutzrechtliche Implikationen im Lichte des Verbraucherkreditgesetzes. Diplomarbeit Karl-Franzens-Universität Graz (2011).

5.3.3.2 Legal assessment

The processing of personal data is an inherent aspect of credit scoring, thereby rendering it subject to the GDPR. The legal basis for data processing must be established in accordance with Art. 6(1) GDPR, and, in instances involving sensitive data, also with Art. 9(2) GDPR. The ECJ generally recognises a legitimate interest in data processing in connection with credit rating information in the context of Art. 6(1)(f) GDPR.[110] In some cases, there is also a legal obligation to carry out credit checks (e.g. Art. 7 Austrian Consumer Credit Act).[111] Nevertheless, it should be noted that this does not imply that it is possible for every assessment method to be based on Art. 6(1)(f) GDPR. The ECJ requires a balancing of the respective opposing rights and interests, which generally depends on the specific circumstances of the individual case.[112] The legitimate interest of the creditor or the credit refence agency must be weighed against the interests of the person affected when considering the extent of the data processing. The extent of interference is determined by factors such as the time period of the data utilised or its sensitivity (e.g. health data).

The assessment of creditworthiness could fall under Art. 86 in conjunction with Annex III point 5(b) AI Act as well as under Art. 22 and Art. 15(1)(h) GDPR. From the perspective of the AI Act, it is first necessary to determine whether the system in question constitutes a high-risk AI system, as defined in Art. 6(2). Systems that are utilised for the evaluation of the creditworthiness of natural persons are, in general, regarded as high-risk, as they can have a serious impact on livelihoods.[113] The AI Act also addresses this outside of the recitals by explicitly listing AI systems for the evaluation of creditworthiness and establishment of credit score as high-risk AI systems in Annex III point 5(b), with the exception of AI systems for the detection of financial fraud. The categorisation of this Use Case under Art. 22 GDPR, to which the right to access under Art. 15(1)(h) GDPR is linked, will be addressed again in Section 5.4.1, which deals with the requirements of Art. 22 GDPR in more detail.

---

[110] ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 79.

[111] Bundesgesetz über Verbraucherkreditverträge und andere Formen der Kreditierung zu Gunsten von Verbrauchern (Verbraucherkreditgesetz – VKrG), BGBl I 28/2010 idF BGBl I 1/2021 (Austrian Credit Consumer Act).

[112] ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 83.

[113] Cf. recital 58 AI Act.

5.3.4 Emotion recognition in marketing and sales promotion (Use Case 4)

Algorithms for identifying and processing emotions, sometimes also referred to as *affective computing*, have a wide range of applications. This also applies to marketing, for example by improving the effect of advertising or using the way people react to certain products to make adjustments or improvements to those products or simply to find out how they are received. However, also purchasing decisions could directly be influenced by such techniques.[114]

Particularly from the perspective of data protection and AI-specific regulations, various constellations and situations are conceivable, whereby some possible practical examples will be picked out and discussed as sub-cases of this Use Case of emotion recognition:

1. Use of gesture recognition to determine reactions in sports betting advertising to increase efficiency (Use Case 4.1);
2. Use of emotion recognition based on images of the facial area as part of identity verification (e.g. for flight bookings), whereby identified emotions are reacted to accordingly (e.g. by lowering prices) in order to increase the probability of a purchase (Use Case 4.2);
3. Use of emotion recognition in marketing for goods or services to recognise in how far these could be adapted, for example to increase customer satisfaction (Use Case 4.3);
    a. Sub-case 1: Adjustment of travel offers based on emotional reactions to corresponding advertising videos in order to better match potential individual preferences[115] (Use Case 4.3.a);
    b. Sub-case 2: Inferring emotions on the basis of texts or audio files of voice recordings to analyse and react to the satisfaction of existing customers[116] (Use Case 4.3.b);

---

[114] See in total *Dejam*, Gefühlsdatenschutz. Eine Untersuchung der datenschutzrechtlichen Rahmenbedingungen von Datenverarbeitungen mittels Affective Computing (2023) 37, 59, 60, on other areas of application generally also 50 et seq.

[115] Cf. *Prange*, Kernfragen des Einsatzes Künstlicher Intelligenz im Marketing, WRP 2024, 151 (paras 22 et seq.).

[116] Cf. also a decision of the Hungarian data protection authority in connection with comparable activities of a bank: NAIH 8 February 2022, NAIH-85-3/2022; see also *Manso-Sayao*, NAIH (Hungary) - NAIH-85-3/2022, https://gdprhub.eu/NAIH_(Hungary)_-_NAIH-85-3/2022#Holding (as at 28 February 2023).

5.3.4.1 Data basis and problem of subsumption under the GDPR and AI Act

Analysing emotions initially requires certain data as a starting point and can thereby be based on voice or video recordings or collected body signals such as brain waves.[117] Subsequently, the processing of data on human emotions usually (unless anonymisation is carried out) constitutes a processing of personal data within the meaning of the GDPR.[118]

Also in the context of advertising, depending on the form of data collection or processing, it cannot be completely ruled out - albeit unlikely - that health data within the meaning of special categories of personal data pursuant to Art. 9 GDPR are involved. This would be the case if such data contain health-specific information (in particular about the state of mind from a health perspective).[119]

However, the categorisation of data processed by emotion recognition systems as biometric data is questionable, especially because the GDPR and the AI Act seem to have a slightly different understanding in that regard, respectively appear to contradict each other. This is particularly relevant because it triggers the question, in how far the applicability of pertinent provisions of the AI Act requires the processing of sensitive data within the meaning of the GDPR (Art. 9) or whether, conversely due to corresponding definitions in the AI Act, all data processed by respective emotion recognition systems are now to be regarded as sensitive data pursuant to Art. 9 GDPR.

In this context, at first Rec. 14 of the AI Act is to be mentioned, which states that biometric data, which accordingly should also in the context of the AI Act be interpreted in light of the notion of biometric data as defined in the GDPR[120], "can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons".[121] However, the categorisation of data used in emotion recognition as biometric data (particularly within the meaning of the GDPR) appears to have been at least questionable in the literature before the AI Act became law.[122] This seems comprehensible solely in view of the aspect required by the definition in Art. 4(14) GDPR, that biometric data "allow or confirm the unique identification of that natural person", because after all this does not necessarily

---

[117] See *Dejam*, Gefühlsdatenschutz 45; cf. fundamentally also *Gremsl/Hödl*, Emotional AI. Legal and ethical challenges, Information Polity 2022, 163 (163, 165).

[118] See *Dejam*, Emotional Privacy 79, 83.

[119] See *Dejam*, Gefühlsdatenschutz 252 et seq.; with regard to mental health (respectively corresponding data) and respective applications, cf. fundamentally also *Steindl*, Does the European Data Protection Framework Adequately Protect our Emotions? Emotion Tech in light of the Draft AI Act and its Interplay with the GDPR, European Data Protection Law Review 2022, 311 (312, 313, 317).

[120] Expressis verbis "in light of the notion of biometric data as defined in Article 4, point (14) of Regulation (EU) 2016/679, Article 3, point (18) of Regulation (EU) 2018/1725 and Article 3, point (13) of Directive (EU) 2016/680".

[121] On the treatment of biometrics in the AI Act and in this context also on emotion recognition systems, cf. Rec. 54 AI Act.

[122] No classification as *biometric data* within the meaning of the GDPR e.g. *Dejam*, Gefühlsdatenschutz 259; however, with regard to "*Facial Emotion Recognition*" analysed thereby, also tending to affirm the processing *of biometric data* pursuant to the GDPR relatively comprehensively: *Gremsl/Hödl*, Information Polity 2022, 163 (165, 166); on the discussion of an adaptation or a revision/division of the rigid understanding of *biometric data* under the GDPR in relation to the AI Act in connection with an earlier stage of the legislative procedure, cf. also *Steindl*, European Data Protection Law Review 2022, 311 (312 et seq.).

have to be the case with emotion recognition.[123]

Furthermore, now also Art. 3(34) AI Act defines biometric data, namely as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data" and therefore de facto identically to Art. 4(14) GDPR, with the very difference that such data do not have to allow or confirm the unique identification of the data subject. Therefore, there appears to be a certain contradiction between the understanding of biometric data in the context of the AI Act (or in its Recitals) and that of the GDPR. The background to this is that the proposal for the AI Act originally provided for a definition completely **identical** to Art. 4(14) GDPR (formerly Art. 3(33)), but the aspect of allowing or confirming the unique identification was deleted in the course of the legislative procedure, while Rec. 14 (formerly Rec. 7) AI Act was complemented particularly by the statement that such data could "allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons". Although the clarifications of the relationship between the two regulations' definitions for biometric data remain similar, it is no longer stated that the terms are "in line" and that they have to be interpreted "consistently". It is merely indicated that the term used in the AI Act should be interpreted in light of the notion of the GDPR.[124]

5.3.4.2 Notion of biometric data pursuant to the AI Act also significant for the GDPR notion?

In principle, various considerations can be made with regard to the problem described above. Firstly, it could be argued that the AI Act has (also) adapted the understanding of the GDPR of biometric data to the effect that it would particularly also cover (quasi additionally, regardless of allowing or confirming the unique identification) data from which emotions can be inferred.

Nevertheless, a number of arguments may be advanced in opposition to this, as the interpretation of the term biometric data within the meaning of the AI Act and in particular the cited explanations in Rec. 14 of the AI Act initially appears to be *contra verbis legis* **in the regime of the GDPR**. This is because the latter requires the very aspect of **allowing or confirming the unique identification of data subjects** for the classification as biometric data pursuant to its Art. 4(14). In this regard, it should first be noted that the understanding of the GDPR of the term could arguably not be extended in this way by a Recital in another regulation alone.[125] A further interpretation of the GDPR-term could only be suggested in conjunction with

---

[123] Cf. *Steindl*, European Data Protection Law Review 2022, 311 (314, 315); *Dejam*, Gefühlsdatenschutz 259.

[124] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art. 3 paras 228 et seq., in particular paras 232 et seq.; and in particular the findings that the GDPR is aimed at a narrower range of biometric data, which was considered inappropriate with regard to the AI Act, which in turn is why various possible solutions were subsequently negotiated, whereby finally a certain contradiction has arisen.

[125] Cf. ECJ 21 April 2023, C-10/23, *Remia Com Impex*, ECLI:EU:C:2024:259, para. 51 with further references: "It should be borne in mind that, according to settled case-law, the preamble to an EU act may explain the content of the provisions of that act and that the recitals of such an act constitute important elements for the purposes of interpretation, which may clarify the intentions of the author of that act [...]" and in particular ECJ 13 July 2023, C-376/20 P, Commission/CK Telecoms UK Investments, ECLI:EU:C:2023:561, para. 105 with further references: "However, the preamble to an EU act has no binding legal force and cannot be relied on as a ground either for

the broader wording of Art. 3(34) AI Act compared to Art. 4(14) GDPR. However, a strong counterargument to this is the following: The AI Act, like the GDPR, was indeed adopted by the European Parliament and the Council on the basis of the TFEU, and in this context in particular Art. 16, based on a proposal from the European Commission in accordance with the ordinary legislative procedure. Yet, it was explicitly stated in Art. 2(7) AI Act that the regulation in principle[126] "shall not affect Regulation (EU) 2016/679 or (EU) 2018/1725, or Directive 2002/58/EC or (EU) 2016/680", respectively that "Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation". Accordingly, the GDPR should principally remain unchanged.

Furthermore, the adaptation of Rec. 14 AI Act described above presumably is to be interpreted in such a manner that the AI Act definition of *biometric data* must only be interpreted in the same way as the GDPR definition **to the extent that they actually correspond** (*argumento*: interpretation in light of the notion of the GDPR and no longer "consistently").[127] Accordingly, Rec. 14 AI Act also seems to argue against an extension of the GDPR's understanding of biometric data, and only aims at an interpretation of the AI Act term **that appropriately corresponds to the GDPR's meaning** (but is not identical).

In this context, *Wendehorst* argues that the meaning pursuant to Art. 4(14) GDPR could in theory be extended to the extent that any biometric characteristic could also be used to **confirm** the identity of the data subject, even if this would be inappropriate in practice regarding inaccuracies. At the same time, reference is made to the fact that Art. 9(1) GDPR still only addresses biometric data "for the purpose of uniquely identifying a natural person", which would in any case result in little change with regard to essential links to this provision (and not to the definition of biometric data).[128]

5.3.4.3 Notion of biometric data pursuant to the GDPR also significant for the AI Act notion?

Based on the requirement of biometric data for the definition of emotion recognition systems in Art. 3 point (39) AI Act (see already 5.2.2), it could also be considered whether this means that only those systems should be covered by the AI Act that also process data which in accordance with Art. 4(14) GDPR allow or confirm the unique identification of natural persons (and, **in addition**, allow for identifying or inferring emotions). It should therefore be scrutinised once more specifically, to what extent the GDPR's understanding of the term biometric data is significant for that of the AI Act.[129] Merely in view of the wording of Rec. 14 AI Act, this

---

derogating from the actual provisions of the act in question or for interpreting those provisions in a manner that is clearly contrary to their wording [...]."

[126] Namely "without prejudice to Article 10(5) and Article 59 of this Regulation".

[127] After all, the clarification that the notions are "in line" (and to be interpreted "consistently") was deleted and replaced by the statement that the AI Act term should be interpreted **in light of the notion** of the GDPR.

[128] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 para. 247.

[129] Cf. again *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* para. 89 (para. 90).

interpretation seems conceivable to a certain extent,[130] but following the critical literature (see above), it would at first constitute a clear restriction of that aspect of the scope of application of the provisions. But above all, it appears to contradict the now broader definition of biometric data in Art. 3(34) AI Act, especially since the requirement to allow or confirm the unique identification was only deleted in the course of the legislative procedure, which after all underlines a corresponding intention.[131] This is also emphasised by the above-quoted amendment in Rec. 14 AI Act, whereby the statement that the two terms are "in line" (and should be interpreted "consistently") was modified to the effect that the AI Act term should be interpreted in light of the notion of the GDPR, which, as already explained, suggests a weakening of the common interpretability.[132]

5.3.4.4 Conclusion on the terminology of biometric data

It follows from all of the above that the potential contradiction in the definitions is presumably to be resolved in such a way that the term biometric data used in the **AI Act** is to be understood like Art. 4(14) GDPR, with the exception of the requirement to allow or confirm the unique identification.[133] This could presumably be achieved, inter alia, by the corresponding addition in Rec. 14 AI Act that these data can particularly also "allow for […] for the recognition of emotions of natural persons", as this appears to correspond to the wider wording of the AI Act. Following this further AI Act definition, the aspects of biometric data named in Rec. 14 AI Act are therefore presumably to be understood as several possible variations rather than as cumulative characteristics (e.g. allowing for identification **or** emotion recognition by means of corresponding data).[134]

To summarise, it can therefore be stated that the AI Act's understanding of the term biometric data and its relationship to that of the GDPR is currently unclear to a certain extent. Altogether, however, the GDPR apparently (still) requires allowing or confirming the unique identification of the data subject concerning the definition of biometric data. Even if this definition were to be interpreted as broadly as possible in light of the AI Act, following *Wendehorst,* Art. 9(1) GDPR still refers to biometric data "**for the purpose of uniquely identifying**" natural persons, which will ultimately mean a corresponding restriction of essential provisions in any case. In contrast,

---

[130] Cf. in particular the wording "The notion of 'biometric data' used in this Regulation should be interpreted in light of the notion of biometric data as defined [...] [the GDPR]".

[131] Cf. in this regard again *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 paras 232 et seq. and 245 et seq.

[132] Moreover, such considerations alone would not fully clarify the effects on the understanding of the term *biometric data* under the GDPR. After all (to some extent reserved to the above considerations), not all types of biometric data within the meaning of Art. 4 point (14) GDPR would be suitable for inferring emotions from them (cf., for example, fingerprints for unique identification: cf. in this regard e.g. *Hödl* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 4 GDPR paras 148, 149 with further references [as at 1 December 2018, rdb.at]).

[133] Cf. presumably similar in result: *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 paras 228 et seq.; in this sense also *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* para. 89 (para. 90), respectively *Hansen/Nägele/Steinbrück* in *Schwartmann/Keber/Zenner* para. 165 (para. 165).

[134] To a certain extent, this would also be supported by Rec. 18 AI Act, which, with regard to *emotion recognition systems*, refers to the recognition of forms of expression such as hand movements; after all, such gestures alone would not necessarily result in unique identifiability (cf. also the above considerations and those of the literature in connection with the GDPR).

the AI Act **does not** require anything of the sort for its definition of biometric data. In addition to data that allow for the authentication, identification or categorisation of natural persons, the definition of the AI Act is supposed to also include data that allow for the recognition of emotions of natural persons, but apart from this should in principle presumably be interpreted like the definition under the GDPR.[135] In this context, *Wendehorst* states that, with regard to the AI Act, it will ultimately have to be based on whether the data is processed using specific technical means in such a way that the primary functions of biometric procedures can be fulfilled, which would also include the corresponding recognition of characteristics and thus also emotion recognition.[136]

In any case, the AI Act's understanding of the term emotion recognition systems requires that personal data is used[137] and, according to *Wendehorst,* presumably essentially that it is data that is obtained by specific technical means for emotion recognition by measuring biological signals with regard to certain personal characteristics.[138] This already means a certain restriction.[139]

According to *Wendehorst,* biometric inferences, i.e. derivations of physical, physiological or behavioural characteristics from general personal data, are rather not included.[140] With regard to the required physical, physiological or behavioural characteristics, *Wendehorst* states that these can be classified in various ways and that, in particular, *weak* biometric characteristics (e.g. body signals, gait or interactions with machines), which are not as unique as a fingerprint as a strong biometric characteristic, can be used primarily for emotion recognition, respectively in the context of targeted marketing.[141]

5.3.4.5 Classification of emotion recognition systems pursuant to the AI Act

However, with regard to corresponding algorithms or systems and the application of the AI Act in general, it must first be determined whether a covered "AI system" is used. See in this regard in detail already Section 5.2.2.

If this is the case, particularly the question arises in which of the AI Acts's risk levels (see also Section 5.2.2) such an AI system should be categorised. Here, it is to be noted again that, in addition to the general definition of AI systems, the AI Act also defines emotion recognition systems (Art. 3(39)) as "an AI system for the purpose of identifying or inferring emotions or

---

[135] Fundamentally in this sense also: *Schwartmann/Keber/Steinbrück* in *Schwartmann/Keber/Zenner* Rz 89 (Rz 90) and *Hansen/Nägele/Steinbrück* in *Schwartmann/Keber/Zenner* para. 165 (para. 165).

[136] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 KI-VO para. 245.

[137] Cf. in particular the definitions in Art. 3(34) and (39) AI Act (see also below) aRec. 14; cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 paras 236, 237.

[138] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 paras 238 et seq., 243 et seq.

[139] Cf. furthermore *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 3 para. 280.

[140] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 para. 246; Cf. also: Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C (2025) 884 final, fundamentally similar under 7.4, but under 7.2.1. b) inferences that are not based exclusively on the data collected on the data subject are apparently indeed considered to be covered.

[141] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 paras 238 et seq.

intentions of natural persons on the basis of their biometric data" (see also Section 5.2.2). Rec. 18 AI Act also states that the term "refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement" and should "not include physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents". It also states that this does not address "the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions". In this regard, it is furthermore noted: "Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering".

According to *Wendehorst*, regarding intentions (whereby the definition is aimed at inferring or identifying such) it should presumably be focused on direct derivability from biometric data. The intention to make a specific purchase, could for instance be mentioned in this regard, which may e.g. become apparent from eye movements or changes in posture.[142]

Subsequently, Art. 5(1)(f) AI Act prohibits "the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person i**n the areas of workplace and education institutions, except** where the use of the AI system is intended to be put in place or into the market **for medical or safety reasons**".[143] Fundamentally, Rec. 44 AI Act contains explanations on the background, respectively on the underlying intentions of this provision. It should furthermore be noted that the term "*emotion recognition system*" is avoided in this prohibition, which would have certain implications on the explanations provided here so far; in particular, Art. 5(1)(f) AI Act (in contrast to the definition pursuant to Art. 3 point (39)) only seems to refer to **emotions** and not as well to **intentions**.[144] Moreover, it is argued that biometric data in the sense described above would not necessarily be required as a basis in this regard, but that in principle more general categories of data could also be considered in that context.[145] This prohibition consequently is presumably of little relevance in connection with advertising measures, however not completely irrelevant.

Furthermore, pursuant to Art. 6(2) AI Act, those AI systems that are listed in Annex III AI Act are generally categorised as high-risk systems[146], which according to Annex III point (1)(c) also applies to "AI systems intended to be used for emotion recognition".[147] Subsequently, most of the substantive provisions of the AI Act apply to these. Under certain circumstances, however, categorisations deviating from Art. 6(2) AI Act may be made (cf. in total already 5.2.2 above).

In any case, deployers of emotion recognition systems (or biometric categorisation systems)

---

[142] Cf. in total *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 para. 282.

[143] Emphasis added.

[144] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 para. 279 and in detail *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art. 5 para. 105 et seq.

[145] Cf. in detail *Wendehorst* in *Martini/Wendehorst*, KI-VO Art 5 paras 106 et seq.; cf. overall, with seemingly contrary interpretations, also: Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (in particular 7.2.1. a), 7.4).

[146] Refer to chapter 5.2.2 for further details, in particular on the classification pursuant to Art. 6(1) AI Act.

[147] Cf. also *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 para. 279.

are subject to certain transparency obligations: Pursuant to Art. 50(3) AI Act, they must in principle "inform the natural persons exposed thereto of the operation of the system".[148]

5.3.4.6 Legal assessment

Regarding the use cases mentioned above, the following preliminary legal assessment can be made:

Firstly, all cases, taking into account the explanations above, will presumably as a rule involve the processing of personal data within the meaning of the GDPR, such as by means of video recordings of a person's face. Particularly in the case of the processing of sufficiently anonymous data, e.g. by data aggregation, this might not apply. The extent to which this necessarily also involves biometric data within the meaning of Art. 4(14), respectively Art. 9(1) GDPR, (and thus special categories of data) is questionable to a certain extent following the above discussion, but is in result (at least with regard to special categories of data in accordance with Art. 9(1) GDPR) regularly rather to be negated.[149] In Use Case 4.2, on the other hand, usually also biometric data pursuant to Art. 4(14), respectively Art. 9(1) GDPR, will be involved.

With regard to the AI Act, the systems used would first have to fulfil the general definition of AI systems pursuant to Art. 3(1), which will often be the case. Furthermore, the question arises whether they constitute an emotion recognition system pursuant to Art. 3(39) AI Act, and in that context in particular to what extent data must be processed that (also) allow or confirm the unique identification of the data subjects (i.e. to what extent Art. 4(14) GDPR is pertinent). According to the opinion expressed here, the AI Act presumably does not aim at the latter and therefore allowing or confirming the unique identification of the data subjects is not required (see above for details). In any case, however, biometric data within the meaning of Art. 3(34) AI Act would have to be involved, and thus in particular "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person". Pursuant to Rec. 14 AI Act, these data can particularly also "allow for […] for the recognition of emotions of natural persons".

Therefore, all three use cases mentioned would as a rule involve personal data from which emotions can be inferred. However, this would (following *Wendehorst*) only be relevant to the extent that this data is obtained by (directly) measuring biological signals relating to corresponding personal characteristics using specific technical means that are particularly aimed at such an emotion recognition purpose (cf. above for details). Of course, this must be assessed in each individual case of application, in particular on the basis of the specific technical approach. However, with regard to the use cases, this would most likely be questionable for Use Case 4.3.b in general if only texts were used to infer potential emotions,

---

[148] This excludes "AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law".

[149] This particularly with the argument that at least Art. 9(1) GDPR still requires "data for the purpose of uniquely identifying a natural person"; cf. in detail the explanations above.

because in this case presumably there usually would be no direct measurement of biological signals.[150] The respective analysis of keystrokes in the sense of movement of hands or gestures, on the basis of which emotions are identified or inferred (cf. Rec. 18 AI Act) would be clearer in this context.[151]

Subsequently, the question arises as to whether emotions or intentions of natural persons should be identified or inferred by the AI system based on the corresponding database. With regard to Use Case 4.1, it is particularly relevant in this respect whether **emotional** reactions (respectively intentions, such as the intention to place a bet) are to be recognised on the basis of gestures, or rather merely other circumstances or states (cf. in particular the clarifications in Rec. 18 AI Act). With regard to the other two use cases, this aspect would presumably be clearer again.

As deployers of emotion recognition systems, the actors concerned would therefore have to inform "the natural persons exposed thereto of the operation of the system" as part of the transparency obligations under Art. 50(3) AI Act.[152] This information must be "provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure" and "conform to the applicable accessibility requirements" (Art. 50(5) AI Act).

Regardless of this (cf. Art. 50(6) AI Act), ultimately the question arises as to which of the risk levels of the AI Act the corresponding systems would have to be assigned to.

Firstly, in case of being used in the workplace or in education institutions for marketing/sales promotion purposes (cf. Art. 5(1)(f) AI Act), systems could be prohibited under Art. 5 AI Act. This is not excluded principally but seems rather unlikely.

In particular regarding Use Case 4.1 and the use of AI in sports betting advertising, for example related to persons with a gambling addiction, the question arises, whether this could amount to a prohibited practice pursuant to Art. 5(1)(b) AI Act. The provision is concerned with exploiting any of the vulnerabilities of a natural person or a specific group of persons 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. Accordingly, in the context of Use Case 4.1, it would initially be of particular relevance whether the system exploits the vulnerabilities of persons addicted to gambling with the effect (or objective) of materially distorting their behaviour in a way that is at least reasonably likely to cause them significant harm.[153]

---

[150] Cf. on this aspect again *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 3 para. 246.

[151] Cf. in this regard in total also *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 106; cf. furthermore: Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (in particular 7.2.1. c)).

[152] The exception of "AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law" would, by its nature, presumably not be relevant in the context at hand.

[153] Of course, other constellations could be considered with regard to the variety of the provision in detail, but the one presented appears to be the most relevant with regard to the facts of the case.

According to the wording, the system would therefore have to specifically target to some extent the circumstance from which the respective need for protection originates, which seems questionable when simply recognising emotions in a general target group.[154] This could in our view be relevant, for example, if emotion recognition is only used for a general target group to show a longer advert to people who react positively compared to people who react negatively to it. In this context, *Wendehorst* notes that, although an intention to exploit regarding the behavioural changes would be required, such an intention would be presumed if a corresponding effect occurs objectively. However, according to Rec. 29 AI Act, the respective distortion must not occur quasi due to external circumstances that could not be reasonably anticipated or mitigated by the obligated parties.[155] With regard to Use Case 4.1, it can therefore be assumed that persons addicted to gambling would presumably be more at risk from corresponding emotion recognition than other persons. In this sense an indirect or effective exploitation of this circumstance worthy of protection is conceivable.

Since, for example, spending a longer period of time on social media is considered sufficient for the aspect of materially distorting the behaviour[156], concluding sport bets and the like, contrary to the original intention of the respective person, may presumably also be pertinent in this respect.

Furthermore, there must be a reasonably likely threat of significant harm. According to Rec. 29 AI Act, this can also relate to harms that may be accumulated over time, which means that not every occurrence of harm has to be significant in itself.[157] According to the objective (i.e. most of all regarding the desired protection), the systematics of the AI Act and the prohibited practices in particular, the notion of harm should presumably be understood quite comprehensively.[158] According to *Wendehorst*, harm of any kind is relevant.[159] In this regard, the question is raised whether (increasing the efficiency of) advertising alone is reasonably

---

[154] In addition to the wording of Art. 5(1)(b) AI Act, cf. also the following passage in Rec. 29, according to which the manipulative or exploitative nature of respective AI appears to be an essential element: "In any case, it is not necessary for the provider or the deployer to have the intention to cause significant harm, provided that such harm results from the manipulative or exploitative AI-enabled practices"; however, if only the specific, current emotions of potential customers were to be analysed in a general manner, it therefore seems questionable whether this would already be specifically aimed at exploiting the vulnerabilities of certain persons; cf. also "However, Article 5(1)(b) AI Act does not apply to AI systems that target consumers based on a wide ranging variables that do not tangentially correlate with vulnerable groups in specific socio-economic situations, such as what brand and model of telephone a person has, in how big city they live, how much and where they travel etc. Even if these characteristics may reflect socio-economic situation [sic] of individuals in general, they are not determinative of individuals in a specific socio-economic situation, whose vulnerabilities the prohibition aims to safeguard against exploitation": Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).

[155] See *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 56; cf. also "'Exploitation' should be understood as objectively making use of such vulnerabilities [...]": Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).

[156] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 57.

[157] *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 45.

[158] See in particular Art. 1(1) and Rec. 5 AI Act and, on the prohibited practices, particularly also Rec. 29; cf. furthermore Art. 27 AI Act on risks of harm in connection with fundamental rights, see in this regard for example *Fülöp/Poindl* in *Pehlivan/Forgó/Valcke*, The EU Artificial Intelligence (AI) Act. A Commentary (2024) Art. 27 section 3.2.2 and 3.3.4.4.

[159] See *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 58.

likely to cause significant harm to affected persons, particularly those with a gambling addiction. However, depending on the circumstances of the individual case, it seems certainly conceivable that the respective advertising increases the likelihood of financial or psychological harm for persons addicted to gambling.

Furthermore, it must be asked whether particularly persons with a gambling addiction can per se be categorised as persons protected by Art. 5(1)(b), especially as the listing therein appears to be exhaustive.[160] Persons with a gambling addiction neither seem generally worthy of protection due to their age, nor do they presumably necessarily fall under a specific social or economic situation. According to Rec. 29 AI Act, this includes e.g. extreme poverty, ethnic or religious minorities, and generally relates to a higher vulnerability to exploitation.[161] Since gambling addiction per se presumably does not necessarily have to be associated with a specific economic situation, the focus with regard to the prohibition must probably be placed less on the gambling addiction itself but rather on whether the person is in an economic predicament or a similar situation (even if due to such an addiction).[162] Principally, however, this also seems conceivable in the corresponding context. One example would presumably be that such a predicament is recognised by the AI system, or that at least such a group of people is actually targeted, whereby it is suggested to the person concerned that they can earn a lot of money quickly with sport betting. As a result, Significant financial harm appears particularly likely. However, the crucial function of the AI would then in particular be to address such an economic predicament in a more or less targeted manner, although this presumably could also be done with the aid of emotion recognition. Naturally, this could also be relevant for other advertising use cases. In addition, persons with disabilities resulting from a long-term physical, mental, intellectual or sensory impairment are protected[163], thus corresponding considerations could also be made in particular on this basis; especially with regard to the definition of gambling disorder as a mental impairment according to ICD-11 (code 6C50).[164]

However, in the case of a generalised use (with a general target group) of emotion recognition to show a longer advertisement to people who react positively than to people who react negatively, the prohibition generally appears to be rather inappropriate.[165] Rec. 29 AI Act also

---

[160] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 53; Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (in particular 3.3.1.).

[161] Cf. *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 55.

[162] Cf. also "5(1)(b) AI Act aims to ensure that AI technologies do not perpetuate or exacerbate existing financial and other social inequalities and injustices by exploiting the vulnerabilities of those people" as well as "For example, an AI-predictive algorithm can be used to target with advertisements for predatory financial products people who live in low-income post-codes and are in a dire financial situation, thus exploiting their susceptibility to such advertisements because of possible despair and causing them significant financial harm": Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).

[163] *Wendehorst* in *Martini/Wendehorst*, KI-VO Art. 5 para. 54.

[164] Cf. https://icd.who.int/browse/2025-01/mms/en#960730313 (last access: 17 February 2024).

[165] Cf. generally also "However, Article 5(1)(b) AI Act does not apply to AI systems that target consumers based on a wide ranging variables that do not tangentially correlate with vulnerable groups in specific socio-economic situations, such as what brand and model of telephone a person has, in how big city they live, how much and where they travel etc. Even if these characteristics may reflect socio-economic situation [sic] of individuals in general, they are not determinative of individuals in a specific socio-economic situation, whose vulnerabilities the prohibition aims

states in this context that "common and legitimate commercial practices, for example in the field of advertising, that comply with the applicable law should not, in themselves, be regarded as constituting harmful manipulative AI-enabled practices".[166] Advertising supported by emotion recognition is presumably not (yet) to be considered common practice. Nevertheless, generalised advertising practices do not necessarily appear to exploit corresponding vulnerabilities in a pertinent manner. Otherwise, this could of course also apply to other advertising use cases (such as Use Case 4.3.a), in which people in economically precarious situations might be more negatively affected. According to the above explanations, however, this is conceivable in areas such as sport betting advertising. Therefore, there may in principle be corresponding cases in connection with emotion recognition that could be subsumed under Art. 5(1)(b) AI Act. However, certain specifics as described above would have to be met.

In specific cases there could also be a connection between emotion recognition and systems prohibited pursuant to Art. 5(1)(a) AI Act.

Otherwise, in principle, presumably all three use cases would generally involve high-risk systems pursuant to Art. 6(2) AI Act, due to the general listing of systems "intended to be used for emotion recognition" in Annex III point (1)(c) AI Act. In principle, the exemption stipulated in Art. 6(3) AI Act must be taken into account in this context. However, with regard to emotion recognition in marketing in general and the use cases mentioned in particular, it appears questionable to what extent a corresponding AI system "does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making".[167] This is because, particularly with regard to Use Case 4.1, there could be an impact on the mental health of people with a gambling addiction in particular, and there could also be an impact on financial health and therefore on private life as well. The latter could possibly also be the case in connection with Use Case 4.2. However, at least in the case of Use Case 4.2, it would certainly also have to be questioned whether this already poses a correspondingly *significant risk*. In addition, the corresponding fundamental rights to data and privacy protection (Art. 7 and 8 CFR) could be affected, particularly regarding the processing of potentially sensitive data or corresponding inferences.

However, at least for Use Case 4.3 in connection with the adaptation or improvement of **completed** services, the condition of Art. 6(3)(b) AI Act could possibly be fulfilled, namely if the system were only "intended to improve the result of a previously completed human activity". In the first sub-case of Use Case 4.3 (3.a), however, this would naturally be different, as the corresponding offers might already be adapted/improved in advance, whereby yet no human activity would have to be involved at all. Depending on the reaction to the emotion inference in the second sub-case of Use Case 4.3 (4.3.b), the application of the exception would also be rather questionable here if, for example, any dissatisfaction was directly addressed with an adapted offer (e.g. better banking conditions) for the person concerned. After all, this would not necessarily constitute a previously completed human activity.

---

to safeguard against exploitation": Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final (3.3.1.).

[166] Here, it should be noted that corresponding restrictions are of course also possible under other (national) laws.

[167] Cf. in total particularly Art. 6(3) AI Act; refer to chapter 5.2.2 for further details.

Thus, all three use cases presumably in principle constitute high-risk AI systems pursuant to Art. 6(2) AI Act, unless – particularly regarding Use Case 4.3 – an exception according to Art. 6(3)(b) AI Act can be claimed. Some constellations, on the other hand, might even constitute practices that are prohibited pursuant to Art. 5 AI Act.

5.4 Relevant provisions of the General Data Protection Regulation (GDPR)

5.4.1 Article 22 GDPR

Article 22 GDPR

(1) The data subject shall have the **right not** to be subject to a decision **based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph 1 shall **not apply if** the decision:

a) is **necessary** for **entering into, or performance of, a contract** between the data subject and a data controller;
b) is **authorised by Union or Member State law** to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c) is based on the data subject's **explicit consent**.

(3) In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall **implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests**, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

(4) **Decisions** referred to in paragraph 2 **shall not be based on special categories of personal data referred to in Article 9(1)**, unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

As explained in Section 5.1, Art. 22 GDPR has already incorporated a provision pertaining to automated decision-making, accompanied by a corresponding right to information.

5.4.1.1 General information

Processing activities under Art. 22 GDPR are enhanced forms of automated processing, namely decisions that are based exclusively on automated processing and are made exclusively by a machine - i.e. without any human intervention regarding its content. This standard - as well as its predecessor provision Art. 15 DPD - thus pursues the approach of protecting people from machine decisions, as the specifications of general algorithms in particular can cause massive impairments for those affected by such decisions.[168] In addition to automated decisions, the legislator has also declared profiling to be a case of application of Art. 22 GDPR.[169] According to Art. 4(4) GDPR, "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". The legislator is thus addressing the risks that the creation of personality profiles based on personal data and the associated prediction of future behaviour pose to the personal rights, autonomy and human dignity of the individuals concerned.[170] This also shows that a relatively large number of data processing activities meet the definition of profiling pursuant to Art. 4(4) GDPR, thereby rapidly opening up the material scope of application of the GDPR. However, in order to be covered by Art. 22 GDPR, the profiling must lead to an automated decision as a "preliminary step" which produces legal effects or similarly significantly affects data subjects.[171]

Example

Use Case 2 can be a case of profiling, where individual customer profiles are created based on certain behavioural characteristics in order to identify customers at risk of churning and initiate appropriate measures. Identification can be carried out, for example, by means of algorithmic evaluation of moods expressed in social media posts (so-called "sentiment analysis"), which are divided into the categories positive, negative or neutral. The customers at risk of churning are then identified by the algorithm based on matching characteristics. On the basis of profiles created in this way, companies can then take targeted measures to mitigate the risk of customer churn in advance.[172]

Even though Article 22(1) GDPR states that the data subject has the right not to be subject to

---

[168] Cf. *Weichert* in *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO und BDSG. Kompaktkommentar³ (2024) Art. 22 DSGVO para. 2 et seq.
[169] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 7.
[170] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 9 et seq.
[171] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 7.
[172] Cf. *Gausling*, Künstliche Intelligenz im digitalen Marketing, ZD 2019, 335 (338).

a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, the term "right" does not mean, in the opinion of the Article 29 Working Party[173] and according to parts of the doctrine[174] , that Art. 22(1) GDPR should only apply if the data subject actively exercises this right. Rather, Art. 22(1) GDPR generally prohibits decision-making based exclusively on automated processing.[175] This prohibition therefore applies regardless of whether the data subject takes action regarding the processing of their personal data.[176] This is intended to take account of the fact that "automated decisions pose a particular risk to the data subject in terms of **transparency and influence**, so that the use of the data evaluation process is considered to be particularly sensitive."[177]

Whilst such processing activities are permitted for the purpose of supporting decision-making, this raises the question of what form of participation by natural persons is required so that the decision is not based solely on automated decision-making. It is generally assumed that Art. 22 GDPR is based on computerised decisions that are made without human intervention, meaning that systems that merely prepare a decision are not covered by its scope.[178] Art. 22 GDPR is not applicable if a manual check of an automated result is carried out before a decision is made, which is subsequently confirmed by a person in consideration of other aspects not included in the automated result.[179]

In this context, the question arises as to whether the algorithm or AI-based system **"significantly"** influenced the decision, as it can be assumed that the scope of Art. 22 GDPR applies if the decision was "significantly" influenced by the machine.[180] In its well-known "SCHUFA ruling" (ECJ Case C-634/21 of 7 December 2023), the ECJ clarified that the automated calculation of a "credit score" by the credit reference agency "SCHUFA" already falls within the scope of Art. 22 GDPR, provided that the subsequent decision to grant a loan is significantly based on this score.[181] The decision is thus based on the differentiation made in Art. 22 GDPR between "fully automated" and "partially automated" decisions. The former are in any case covered by Art. 22 GDPR, while the latter depend on the degree of concretisation of the proposal for the decision serving as the basis for a human decision.[182] For example, suggestion systems that already propose a specific outcome for a decision to

---

[173] The Article 29 Working Party (A29WP) was an independent advisory body to the European Union on data protection issues and was replaced in 2018 by the European Data Protection Board (EDPB), which is tasked with ensuring the harmonised application of the GDPR. The EDPB has confirmed some of the guidelines drawn up by the A29WP.

[174] Cf. for example *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 GDPR para. 16.

[175] Cf. ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 52.

[176] *A29WP*, Guidelines on automated individual decision-making, including profiling, for the purposes of Regulation 2016/679, 17/DE WP251rev.01 (2018) 21, https://ec.europa.eu/newsroom/article29/items/612053.

[177] *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 16.

[178] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 25.

[179] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 25a.

[180] Cf. for example, the ruling of the Administrative Court 21. 12. 2023, Ro 2021/04/0010-11 based on the SCHUFA ruling of the ECJ (7. 12. 2023, C-634/21, *SCHUFA Holding [Scoring]*, ECLI:EU:C:2023:957) on the question of whether the Austrian Public Employment Service's labour market opportunity assistance system "AMAS" is a tool for automated decision-making in accordance with Art. 22 GDPR. The proceedings were referred back to the Federal Administrative Court on the grounds that it still had to clarify whether the decision on a person's labour market opportunities was "significantly" influenced by the system.

[181] Cf. also *Paal/Hüger,* MMR 2024, 540 (541).

[182] Cf. *Paal/Hüger,* MMR 2024, 540 (541).

human decision-makers may fall within the scope of Art. 22 GDPR (such as the calculation of a "credit score" to classify creditworthiness mentioned here), while AI-based systems that process, analyse or visualise information and thus only perform supporting tasks (such as collecting general background information using the well-known language model ChatGPT) are not covered.[183]

In addition, a key indicator of significance in relation to an AI-based decision proposal is the socio-technical phenomenon known as "automation bias", i.e. the particular trust placed in the outputs of AI systems, which is reinforced by the system's lack of transparency and the potential pressure on human decision-makers to justify deviations from the AI-based recommendation (for more information, see Chapter 6).[184]

It should be noted that human involvement must not be merely pro forma in order to exclude the scope of Art. 22 GDPR, and controllers must therefore ensure that it is not just a symbolic gesture, but that decisions are subject to real supervision and that decisions should be made by a person who is authorised and empowered to change them.[185]

5.4.1.2 "Decision"

In principle, Art. 22 GDPR requires a decision. The concept of a decision is not clearly defined in the GDPR, but the ECJ tends to interpret the term "decision" broadly in its case law.[186] Furthermore, the wording of Art. 22 GDPR appears to refer to a single "decision-making moment", disregarding the fact that in practice, several actions or steps often influence the final decision-making process.[187] If one were to follow such an interpretation, it could pave the way for circumventing the legal consequences of Art. 22 GDPR by excluding "preliminary decisions"[188], thereby creating a legal protection gap. For this reason, the ECJ assumes that significant preliminary decisions also fall within the scope of Art. 22 GDPR, provided that the main decision heavily relies on them.[189] The fact that the term "decision" is to be interpreted broadly is also emphasised in the literature, where *Weichert*, for example, assumes that instead of a decision, one can also speak of a measure.[190]

---

[183] Cf. *Paal/Hüger,* MMR 2024, 540 (54 f).

[184] Cf. *Paal/Hüger,* MMR 2024, 540 (542).

[185] *A29WP*, Guidelines on automated individual decision-making 22; *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 25.

[186] Cf. *Metikos/Ausloos*, Law, Innovation, and Technology 2025, tbp, and ECJ 7 Dec. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 45.

[187] Cf. *Metikos/Ausloos*, Law, Innovation, and Technology 2025, tbp.

[188] Cf. *Binns/Veale*, Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR, International Data Privacy Law 2021, 319.

[189] Cf. *Metikos/Ausloos*, Law, Innovation, and Technology 2025, tbp, and ECJ 7 Dec. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 61f.

[190] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO para. 25. Following a similar line of argument: *Haidinger* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art. 22 DSGVO para. 18 (as at 1 December 2022, rdb.at) with reference to Recital 71 sentence 1.

Example

The fact that the term "decision" is to be interpreted broadly and can also include relevant preliminary decisions is expressed in Use Case 3 on creditworthiness and credit scoring. Here, the ECJ assumes that even the determination of a score value as such is to be classified as a decision which produces legal effects concerning a data subject or similarly significantly affects a data subject within the meaning of Art. 22(1) GDPR, provided that this score has a significant influence on the decision.[191]

5.4.1.3 "Legal effect"

In addition, the automated decision-making processes must produce legal effects concerning the data subjects or significantly affect data subjects in a similar manner in accordance with Art. 22 (1) GDPR. According to the Article 29 Working Party, the decision must affect the rights of a person. This could, for example, relate to the freedom of association, the right to vote or the right to take legal action, the legal status of a person or their rights under a contract.

Example

Specific examples include the termination of a contract, the entitlement to or refusal of a certain statutory social benefit such as child benefit or housing benefit or a refusal of entry into a country or the refusal of naturalisation. Practical use cases for decisions that have legal effect also include profiling for the online granting of loans or the implementation of online recruitment procedures (Recital 71 GDPR).[192]

According to the wording, the requirement of legal effect would also include positive effects (see, in contrast, the parallel provision of Art. 11(1) LED, which refers to adverse legal consequences). Some scholars assume that it does not matter whether the legal effect for those affected is positive or negative, as a detrimental effect is not explicitly required.[193] However, the purpose of the provision suggests that only negative legal effects should be covered in this context, i.e. the legal effect must be significantly detrimental.[194] However, it must be taken into account that a "negative" effect always has an inherent subjective

---

[191] ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 50.
[192] *A29WP*, Guidelines on automated individual decision-making 23.
[193] Cf. for example *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 GDPR para. 27.
[194] *Herbst* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG⁸ (2024) Art 15 DSGVO paras 13 et seq.; *Kamlah* in *Plath* DSGVO/BDSG/TTDSG⁴ (2023) Art 22 DSGVO para. 17.

component, which is not always easy to explain from the perspective of the person affected.[195] A decision may be objectively "positive", yet from the data subject's perspective, it could have been significantly more favourable. As a result, the affected person may ultimately perceive it as "negative" (e.g. the automated categorisation in a certain salary scheme when entering a new employment relationship). Furthermore, if an *ex ante* assessment is carried out before a concrete decision is made, there is always the possibility that a concrete decision may have a negative impact, as several outcomes of the decision are possible, and each potential outcome of the decision could have a negative impact on the data subject compared to alternative options. Furthermore, it is not always the case that a decision only has a certain legal effect and can therefore be clearly assessed as exclusively "positive" or "negative". For example, a certain application (e.g. for a building permit) could only be partially granted, which means that the decision includes both positive aspects in the form of a favourable decision and negative aspects in the form of a rejection of certain parts of the application.

To summarise, the positivity or negativity of a legal effect cannot be objectively assessed or described as exclusively "negative" or exclusively "positive". It should also be borne in mind that Art. 22 GDPR – in contrast to Art. 86 AI Act – explicitly stipulates a prohibition, which is why the perspective of the data subject must be considered in particular. And since this dispute has not been conclusively resolved, it is recommended that the requirement of legal effect be interpreted broadly and therefore to include any effect, regardless of whether it is categorised as positive or negative.

5.4.1.4 The term "similarly significantly affects him or her"

According to the Article 29 Working Party, the threshold at which data subjects are significantly affected in a similar way is comparable to the threshold at which a decision has legal effect. The effect must be comprehensive and there must be a possibility that the decision:

- significantly affects the circumstances, behaviour or decisions of the data subjects;
- impairs the data subject over a longer period of time or permanently, or
- in the worst case leads to the exclusion or discrimination of persons.

The following decisions could fall into this category:

- Decisions that affect a person's financial situation, for example their creditworthiness;
- Decisions that affect access to healthcare services;
- Decisions that deny access to jobs or seriously disadvantage people;
- Decisions that affect access to education, such as university admissions

---

[195] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art 22 DSGVO para. 27.

Recital 71

The **data subject** should have the **right not to be subject to a decision**, which may include a measure, evaluating personal aspects relating to him or her which is **based solely on automated processing** and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices **without any human intervention.**

Such processing includes **'profiling'** that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. [...]

Recital 71 GDPR mentions the following typical examples: "automatic rejection of an online credit application" or "online recruitment process without any human intervention". Of the use cases presented at the beginning, certain forms of online advertising based on emotion recognition can be mentioned here, which may constitute a form of profiling and would therefore be covered by the scope of application of Art. 22 GDPR.[196] Significant impairment by advertising occurs when people are "tracked" or "followed" across several websites or services and advertising is customised to the expectations and needs of these people.[197] This is probably the case for most forms of advertising if they are displayed across multiple devices or websites or lead to unreasonable harassment of the data subject in the form of "retargeting".[198] However, according to the Article 29 Working Party, in the area of online advertising, the decision to display targeted advertising based on profiling will not significantly affect individuals in a similar way if advertising for an online shop of a mainstream fashion retailer is displayed based on a simple demographic profile. In contrast, discriminatory advertisements, personalised price offers or advertisements that specifically address and exploit the vulnerabilities of those affected are covered,[199] such as advertisements for sports betting aimed at gambling addicts. The situation is therefore considered differently if the profiling process is intrusive in nature or if someone who is known or likely to be in financial difficulties and regularly receives targeted advertising for high-interest loans accepts these offers, potentially leading to additional debt.[200] It is mentioned that the actions of persons other than those to whom the automated decision relates can also trigger similar significant impairments, such as the setting of credit card limits not on the basis of one's own repayment behaviour but on the basis of the behaviour that has resulted from the analysis of other

---

[196] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 31.
[197] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para.31.
[198] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 31
[199] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 31.
[200] *A29WP*, Guidelines on automated individual decision-making 23 et seq.

customers.[201] Another case concerns the automated decision regarding an energy supply contract that is cancelled due to a lack of creditworthiness, despite the absence of negative payment history for the affected person.[202]

5.4.1.5 Exceptions to the ban on automated decision-making

However, Art. 22(2) GDPR also conclusively defines exceptions to the general prohibition of processing. The prohibition of automated processing therefore does not apply if the automated decision-making:

> a) is necessary for entering into, or performance of a contract;
>
> (b) is authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>
> c) is based on the data subject's explicit consent.

If the decision concerns special categories of data defined in Article 9(1), the controller must also ensure compliance with the conditions of Article 22(4), such as the implementation of suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests.

In view of the increasing digitalisation of our legal relationships, automated decision-making processes are increasing in all areas of life, including in contractual relationships.[203] The Article 29 Working Party cites the following example of performance of a contract in accordance with Art. 22 (2)(a) GDPR:

Example

A company publishes a job posting. As the company is a popular employer, tens of thousands of applications are received. Due to the exceptionally high number of applications, the company finds it practically impossible to identify suitable applicants without filtering out unsuitable applications using fully automated processes. In this case, automated decision-making may be required to create a short list of potential applicants with the intention of concluding a contract with a data subject.[204]

Art. 22 (2)(b) GDPR which is referred to as an opening clause, grants a power of concretisation

---

[201] *A29WP*, Guidelines on automated individual decision-making 23 et seq.

[202] Cf. BVwG 23. 4. 2024, W292 22488672-1/5E.

[203] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 43.

[204] *A29WP*, Guidelines on automated individual decision-making 25.

through other legal provisions in Union or national law.[205] Such legislation must be democratically legitimised and often serves certain sovereign objectives, such as combating fraud or national security purposes.[206]

An automated decision is also permitted on the basis of the explicit consent of the data subject, the effectiveness of which is subject to strict requirements in terms of information, specificity of the declaration and voluntariness.[207] The minimum requirement is that at least the logic of the processing, the data input, the purpose of the processing or the decision and the bodies involved are disclosed.[208]

Of particular importance are also the transparency obligations provided for in the GDPR for automated decision-making, such as the right to information or access (in accordance with Articles 13, 14 and 15, in particular the receipt of meaningful information on the logic involved and the scope and intended effects for the data subject) and guarantees such as the right to obtain human intervention or the right to contest the decision (cf. Article 22 (3) GDPR).

---

[205] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 37.
[206] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 37 et seq.
[207] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 46.
[208] Cf. *Weichert* in *Däubler et al,* EU-DSGVO³ Art. 22 DSGVO para. 47.

Example

Practical illustration of Art. 22 GDPR using the Use Case of creditworthiness and credit scoring:

With regard to the practical implications of Art. 22 GDPR, hardly any other case has aroused as much interest as that of the assessment of creditworthiness and credit scoring, in particular due to the "SCHUFA judgement", which has already been cited several times, in which the ECJ interprets the term "automated individual decision-making" broadly.[209]

This is the case when a probability value based on personal data relating to the ability to fulfil future payment obligations is created automatically by a credit reference agency, provided that this probability value has a significant influence on whether a third party establishes, implements or terminates a contractual relationship with this person. In this case, the determination of this value as such is already to be classified as a decision which produces legal effects concerning a data subject or similarly significantly affects a data subject within the meaning of Art. 22 (1) GDPR.[210]

A central point of the judgement is that even the creation of the score can be considered an automated decision within the meaning of Art. 22 GDPR if this score has a significant influence on the decision of a third party (e.g. a bank). This is an important distinction from Art. 86 AI Act, which applies a lower threshold: Here, it is sufficient if the influence is relevant without it having to be "significant" (for more details, see Section 5.5).

One open question that the ECJ has not conclusively resolved is whether purely statistical algorithms also fall under the concept of automated decision-making under Art. 22 GDPR or the concept of AI. Art. 3 AI Act defines AI systems as those that act at least partially autonomously. This means that the system is not based exclusively on static, deterministic rules specified by humans, but that its decision-making logic goes beyond pure data processing by enabling learning, reasoning or modelling.[211]

Autonomy is understood here as a differentiation from classic "if-then systems", whose output is completely determined by rules specified by humans. In AI systems, on the other hand, the decision-making logic is indirectly shaped by machine learning, for example, so that the output is not completely predictable or predetermined by humans. This could be seen as a loophole in the AI Act, as complex deterministic systems created by AI can deliver similar results to autonomous AI systems and humans no longer understand their function or decision logic, but these are not subject to

---

[209] ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957.

[210] ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 50.

[211] Recital 12 AI Act.

regulation.[212]

A clarification must, in any case, be made in accordance with the definitions provided by the AI Act. In the run-up to the publication of the guidelines on the term AI system, there were internal disputes as to whether linear/logistic regression, a simple machine learning technique that is highly relevant in the financial sector, should fall under the term and thus within the scope of the AI Act.[213] The published guidelines stipulate that such common machine learning approaches do not fall under the term AI system.[214]

---

[212] *Rosenthal*, Der EU AI Act – Verordnung über künstliche Intelligenz, Jusletter 5 August 2024, 1 (7).

[213] *Bertuzzi*, Financial sector sees last-minute disagreements over EU's definition of AI system, https://www.mlex.com/mlex/articles/2293541/financial-sector-sees-last-minute-disagreements-over-eu-s-definition-of-ai-system (as at 5 February 2025).

[214] Annex to the Communication to the Commission. Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 924 final 8.

5.4.2 Article 15(1)(h) GDPR

Article 15 GDPR

1. The data subject shall have the **right** to **obtain** from the controller **confirmation** as to **whether** or not **personal data** concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a. the **purposes** of the processing;

b. the **categories** of personal data concerned;

c. the **recipients or categories of recipient** to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d. where possible, the **envisaged period for which the personal data will be stored**, or, if not possible, the **criteria** used to determine that period;

e. the existence of the **right to request from the controller rectification or erasure of personal data or restriction of processing** of personal data concerning the data subject or to object to such processing;

f. the right to **lodge a complaint** with a supervisory authority;

g. where the personal data are not collected from the data subject, **any available information as to their source**;

h. the existence of **automated decision-making**, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful information about the logic involved**, as well as the **significance** and the **envisaged consequences** of such processing for the data subject.

5.4.2.1 Introduction

According to Art. 15 GDPR, data subjects have the right to request confirmation from the controller as to whether personal data concerning them is being processed. If this is the case, the data subject has a right of access to this personal data and to a range of information. As a special case, Art. 15(1)(h) GDPR lists three elements of information that must be provided in relation to automated decision-making: [1.] "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, [2.] meaningful information about the logic involved, as well as [3.] the significance and the envisaged consequences of such processing for the data subject."

5.4.2.2 Logic involved

The following explanations are predicated on the notion of "logic involved", a concept that has sparked numerous discussions in literature and case law. In the literature, the necessary informational elements are often described by other terms such as "logic", "logical structure", "basic assumptions of algorithm logic", "decision logic" or "methods and criteria of data processing" without specifying them.[215]

It is controversial whether, in addition to abstract information about the mode of operation and relevance of the decision-making system, there is also an obligation to justify specific processing results on a case-by-case basis. This is primarily denied by the prevailing doctrine with reference to the consistency with Art. 13 and 14 GDPR, which apply chronologically before the decision-making process.[216]

The guidelines of the A29WP, which were adopted by the EDPB, also seem to speak in favour of the identity of the information: "The controller should have already given the data subject this information in line with their Article 13 obligations."[217] Furthermore: "The controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level) which is also useful for him or her to challenge the decision."[218]

Contrary to this, more recent EDPB guidelines state that "If possible, information under Art. 15(1)(h) has to be more specific in relation to the reasoning that lead to specific decisions concerning the data subject who asked for access."[219] However, this statement is qualified by the addition of "if possible".

Another view in favour of a case-by-case justification is put forward by *Bäcker*, for example, who argues that the purpose of the right to information is to enable the effective exercise of rights and freedoms. Without such a justification, little could be done to counter the black box nature of the decision-making process.[220]

Franck also argues in this direction, according to whom it is not possible to put forward one's own point of view and challenge the decision in the sense of Art. 22 (3) GDPR without appropriate "justification material".[221]

Likewise, according to *Mester*, in addition to the methods and criteria as well as the scope and effects of the data processing, "the evaluation results already determined and the decisions

---

[215] *Schneeberger*, Machine Learning 167.

[216] Fundamental *Wachter/Mittelstadt/Floridi*, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law 2017, 76; mwN *Schneeberger*, Machine Learning 171 et seq.

[217] *A29WP*, Guidelines on automated individual decision-making 27.

[218] *A29WP*, Guidelines on automated individual decision-making 27.

[219] *EDPB*, Guidelines 01/2022 on data subject rights - Right of access version 2.1 (2023) 40, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

[220] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG. Kommentar^4 (2024) Art. 15 DSGVO para. 27b et seq.

[221] *Franck* in *Gola/Heckmann*, Datenschutz-Grundverordnung VO (EU) 2016/679. Bundesdatenschutzgesetz. Kommentar (2022) Art. 15 DSGVO para. 18.

based on them must also be communicated."[222] Similarly, according to *Däubler*, "past analyses and the decisions made on this basis"[223] must also be communicated. According to *Dix*, in light of the objective of enabling data subjects to exercise their rights, the assumption of a (case-by-case) right to information, based on Art. 15 GDPR, is necessary in order to overcome information asymmetries.[224]

Similar lines of argument in favour of the existence of a right to a case-by-case explanation can be found, for example, in *Kaminski*,[225] *Malgieri* and *Comandé*,[226] *Hacker* and *Passoth*[227] and *Selbst* and *Powles*.[228]

According to an interdisciplinary report that looks at the logic involved from a combined technical and legal perspective, there are various ways of presenting the logic involved: "We think that the demand for documenting the input data, architectural choices and evaluation methods falls under what was called the 'structure and sequence of the data processing' in the legal considerations above. We propose to make the design and development process of the ADM system as well as the underlying rationale transparent. This may require obligations to document the processes of data gathering and preparation including annotation or labelling. Ensuring the highest amount of transparency at the input level is arguably one of the best ways to influence and truly understand what is happening in a model. Likewise, instantiating the demand of showing the 'logic involved' by the more concrete requirement of providing local or global explanations of the socio-technical systems can be seen as an operalisation step."[229]

In the field of research of explainable AI, a local explanation refers to the explanation of an individual decision, which is also technically possible for more complex models (e.g. artificial neural networks), e.g. by highlighting the most important features (e.g. pixels in an image). A global explanation that explains a model independently of an individual decision is technically more complex and often only possible for so-called white box models (e.g. linear models, decision trees).[230]

According to a decision of the DSB from 2020, "specifically regarding information pursuant to Art. 15 para. 1 lit. h GDPR, the parameters/input variables of a calculated assignment, their influence on the calculated assignment, i.e. essentially the weighting of the parameters, the information on the origin of the parameters/input variables (e.g. whether the parameter "living

---

[222] *Mester* in *Taeger/Gabel*, GDPR - BDSG - TTDSG^4 (2022) Art. 15 DSGVO para. 12.

[223] *Däubler* in *Däubler/Wedde/Weichert/Sommer*, EU-DSGVO and BDSG. Compact Kompaktkommentar^3 (2024) Art. 15 DSGVO para. 18.

[224] *Dix* in *Spiecker gen. Döhmann/Papakonstantinou/Hornung/Hert*, General Data Protection Regulation. Article-by-Article Commentary (2023) Art. 15 DSGVO para. 19.

[225] *Kaminski*, The Right to Explanation, Explained, Berkeley Technology Law Journal 2019, 189.

[226] *Malgieri/Comandé*, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law 2017, 243.

[227] *Hacker/Passoth*, Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond, in *Holzinger/Goebel/Fong/Moon/Müller/Samek* (eds.), xxAI - Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020 July 18, 2020, Vienna, Austria, Revised and Extended Papers (2022) 343 (348 f).

[228] *Selbst/Powles*, Meaningful information and the right to explanation, International Data Privacy Law 2017, 233.

[229] *Asghari et al*, What to explain 18. With further references regarding such an interdisciplinary approach *Bibal/Lognoul/Streel/Frénay*, Legal requirements on explainability in machine learning, AI and Law 2021, 149; *Brkan/Bonnet*, Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions. Of Black Boxes, White Boxes and Fata Morganas, European Journal of Risk Regulation 2019, 18.

[230] *Schneeberger*, Machine Learning 150 et seq.

environment" was statistically extrapolated), an explanation of why the data subject was assigned to a certain assessment result and an enumeration of profile categories possible for an assignment, an explanation of why the data subject was assigned a particular evaluation result, and a list of possible profile categories for classification must be disclosed [...] or similar information of equivalent informational value must be provided, which enables the data subject to exercise their rights to rectification, erasure and verification of lawfulness of the processing."[231] The DSB based this on statements made by *Zavadil*,[232] who is himself an employee of the DSB.

According to a ruling by the Federal Administrative Court[233] , the data controller "must describe the logic used to the data subject in such a way that the data subject is informed about the parameters used in the evaluation and can recognise which aspects of their person or behaviour are being used. The algorithm itself does not have to be disclosed. The term "logic involved" is to be understood as meaning that only the principle on which such a calculation is based is to be presented, but not the specific "calculation formula". This in turn indicates an explanation that is not specifically focussed on the individual case but provides general information at an aggregated level (in particular the parameters used in the assessment).

This aspect was not specified in the SCHUFA judgement,[234] in which the scope of application of Art. 22 GDPR was concretised. However, the Opinion of the Advocate General *Pikamäe* examined the interpretation of the logic involved in more detail. According to him, the logic involved does not include "any obligation to disclose the algorithm, given its complexity". The Advocate General considers “that the obligation to provide ‘meaningful information about the *logic involved*’ must be understood to include sufficiently detailed explanations of the method used to calculate the score and the reasons for a certain result. In general, the controller should provide the data subject with general information, notably on factors taken into account for the decision-making process and on their respective weight on an aggregate level, which is also useful for him or her to challenge any ‘decision’ within the meaning of Article 22(1) of the GDPR."[235]

This indicates on the one hand a case-by-case explanation ("that led to a **specific** result"). Seemingly contradictory, however, the Opinion states that "general information" should generally be provided "notably on factors taken into account for the decision-making process and on their respective weight on an aggregate level". The reference to the aggregate level would, in turn, argue against a case-by-case explanation.[236] It is possible that this general information should be understood as basic information that needs to be specified with more concrete case-by-case information.

---

[231] DSB 8. 9. 2020, 2020-0.436.002.

[232] *Zavadil*, Das Auskunftsrecht nach Art. 15 Datenschutz-Grundverordnung, Dissertation University of Vienna (2020) 124 et seq.; *Zavadil*, Der besondere Auskunftsanspruch über die involvierte Logik einer Datenverarbeitung, Dako 2020, 55.

[233] BVwG 23. 4. 2024, W292 2248672-1.

[234] ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957.

[235] Opinion of the Advocate General *Pikamäe* 7 March 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:220, para. 56 et seq.

[236] With further references *Schneeberger*, Large Language Models in der Verwaltung, in *Hoffberger-Pippan/Ladeck/Ivankovics* (eds.), Digitalisierung und Recht. Jahrbuch 2024 (2024) 223.

Building on this, Advocate General de la Tour stated in the Opinion to Dun & Bradstreet Austria on the logic involved: "The data subject's knowledge of that context must enable him or her, through knowledge of the essential elements of the method and the criteria used, to understand the result reached by the automated decision. In short, the process, which is technical in nature, that led to that decision must be made intelligible. Only in that way will the data subject be able to exercise his or her rights under the GDPR [...]. The concept of 'meaningful information about the logic involved' in automated decision-making must therefore be understood functionally. [...] Accordingly, I consider that 'meaningful information about the logic involved' in automated decision-making must enable the data subject to exercise the rights guaranteed to him or her by the GDPR and, in particular, by Article 22 of that regulation. That presupposes, in the first place, that that person can obtain information that is concise, easily accessible and easy to understand, and formulated in clear and plain language on the method and criteria used for that decision. In the second place, that information must be sufficiently complete and contextualised […]. I infer from those elements that the controller is not required, under Article 15(1)(h) of the GDPR, to provide the data subject with information of a technical nature which he or she would not be in a position to understand, such as the details of the algorithms used. By contrast, that controller must fulfil its obligation, in each case, to provide that person with both accessible and sufficiently complete information on the process that led to the automated decision in question and the reasons for the outcome of that decision. Thus defined, 'meaningful information about the logic involved' in automated decision-making should in particular **describe the method used and the criteria taken into account and their weighting**. The data subject must therefore be able to understand what information was used in the automated decision-making and how it was taken into account and weighted."[237]

This Opinion also focuses strongly on the method and criteria of the decision. It is also clarified that the concept of meaningful information is to be understood functionally.[238]

Excessively technical information, such as the algorithm itself, would not have to be disclosed, as the information should always remain comprehensible in accordance with the principle of transparency. What is therefore required at a technical level is primarily a feature-importance-explanation, i.e. a description of the most important features. However, the Advocate General only provides limited clarity on the specific implementation. This is because this information could be presented with a focus on the individual decision (local) or detached from it across all decisions (global).

The opinion mentions by way of example, and only in passing: "examples of similar processing operations provided in an anonymised manner, by way of comparison, could enable that person to understand better the automated decision of which he or she was the subject".[239] This would be a form of example-based explanation, which, however, does not address the

---

[237] Opinion of the Advocate General *de la Tour* 12. 9. 2024, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2024:745, paras 64 et seq. (emphasis added by author).

[238] *Kelder*, CK v Dun & Bradstreet Austria (C-203/22). The case that ends the GDPR right to explanation debate? https://digi-con.org/ck-v-dun-bradstreet-austria-c-203-22-the-case-that-ends-the-gdpr-right-to-explanation-debate/ (as at 6 November 2024).

[239] Opinion of the Advocate General *de la Tour* 12. 9. 2024, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2024:745, para. 78.

specific decision, but aims to enable conclusions to be drawn by showing similar examples.[240]

Since the Opinion focuses strongly on the element of contextuality and usefulness of the information for the data subject and regarding the wording partly on the specific decision (e.g. "to the automated decision in question"), a local explanation relating to the specific case is considered more suitable for fulfilling these requirements. As a result, a combined explanation consisting of general information (how the mechanism works) and information on the specific decision (the result) appears to be outlined in the Opinion.[241]

On 27 February 2025, the judgment in the *Dun & Bradstreet* case was published.[242] The Court firstly pointed to the ambiguity of the word 'meaningful' and the complementarity of the different language versions.[243] It stated that the term 'involved logic' also encompasses a wide range of logics.[244] The ECJ then primarily derived from this comparison of the different language versions that "involved logic" "covers all relevant information concerning the procedure and principles relating to the use, by automated means, of personal data with a view to obtaining a specific result."[245]

As in the Opinion, reference is made to the role of the principle of transparency, as also embodied in Art. 12 of the GDPR, and it is specified that "'meaningful information about the logic involved' in automated decision-making, within the meaning of that provision, covers **all relevant information concerning the procedure and principles** relating to the use of personal data **with a view to obtaining, by automated means, a specific result,** the obligation of transparency also requiring that that information be provided in a concise, transparent, intelligible and easily accessible form."[246]

The judgment also emphasises the connection between Art. 15 and the rights to which data subjects are entitled in the case of automated decision-making under Art. 22(3) of the GDPR: "In particular, in the specific context of the adoption of a decision based solely on automated processing, the main purpose of the data subject's right to obtain the information provided for in Article 15(1)(h) of the GDPR is to enable him or her effectively to exercise the rights conferred on him or her by Article 22(3) of that regulation, namely the right to express his or her point of view on that decision and to contest it."[247] This is because "If the individuals affected by an automated decision [...] were not in a position to understand the reasons which led to that decision before expressing their point of view or contesting the decision, those rights would not, accordingly, satisfy in full their purpose of protecting those individuals against the

---

[240] *Kelder*, CK v Dun & Bradstreet Austria (C-203/22). The case that ends the GDPR right to explanation debate? https://digi-con.org/ck-v-dun-bradstreet-austria-c-203-22-the-case-that-ends-the-gdpr-right-to-explanation-debate/ (as at 6 November 2024).

[241] *Kelder*, CK v Dun & Bradstreet Austria (C-203/22). The case that ends the GDPR right to explanation debate? https://digi-con.org/ck-v-dun-bradstreet-austria-c-203-22-the-case-that-ends-the-gdpr-right-to-explanation-debate/ (as at 6 November 2024).

[242] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117.

[243] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, paras 40 et seq.

[244] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 42.

[245] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 43.

[246] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 50 (emphasis added by the authors).

[247] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 55.

particular risks to their rights and freedoms [...]"[248] The judgment also confirms, with reference to Recital 71 of the GDPR, that Art. 15 (1) (h) GDPR offers the data subject a **"genuine right to an explanation as to the functioning of the mechanism** involved in automated decision-making of which that person was the subject and of the result of that decision."[249]

Finally, the Court concludes that "the right to obtain 'meaningful information about the logic involved' in automated decision-making, within the meaning of that provision, must be understood as a right to an explanation of the procedure and principles actually applied in order to use, by automated means, the personal data of the data subject with a view to obtaining a specific result, such as a credit profile."[250] The relevant information have to be provided in a precise, transparent, comprehensible and easily accessible form.

The judgment makes it clear, as does the Opinion, that this telos "cannot be satisfied either by the mere communication of a complex mathematical formula, such as an algorithm, or by the detailed description of all the steps in automated decision-making, since none of those would constitute a sufficiently concise and intelligible explanation."[251] This tension between transparency and explanation is again taken up by the ECJ: "Thus, the 'meaningful information about the logic involved' in automated decision-making, within the meaning of Article 15(1)(h) of the GDPR, must describe the **procedure and principles** actually applied in such a way that the data subject can understand which of his or her personal data have been used in the automated decision-making at issue, with the complexity of the operations to be carried out in the context of automated decision-making not being capable of relieving the controller of the duty to provide an explanation."[252]

The court also gives an example of how to fulfil the right to information as it would consider that: "inter alia, [...] it is sufficiently transparent and intelligible to inform the data subject of the extent to which a variation in the personal data taken into account would have led to a different result."[253] In the XAI field, this form of explanation is often referred to as a counterfactual explanation.[254]

Regarding these preliminary questions, the ECJ concludes "that Article 15(1)(h) of the GDPR must be interpreted as meaning that, in the case of automated decision-making, including profiling, within the meaning of Article 22(1) of that regulation, the data subject may require the controller, as 'meaningful information about the logic involved', to explain, by means of relevant information and in a concise, transparent, intelligible and easily accessible form, **the procedure and principles actually applied in order to use, by automated means, the personal data concerning that person with a view to obtaining a specific result** [...]."[255]

---

[248] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 56.

[249] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 57 (emphasis added by the authors).

[250] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 58.

[251] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 59.

[252] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 61 (emphasis added by the authors).

[253] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 62.

[254] For example, *Wachter/Mittelstadt/Russell*, Counterfactual Explanations Without Opening the Black Box. Automated Decisions and the GDPR, Harvard Journal of Law & Technology 2018, 841.

[255] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 66 (emphasis added

As discussed in more detail above regarding the Opinion, the ECJ appears to place more emphasis on the local element, i.e. the individual decision, although the statements leave a certain amount of leeway and therefore the question of local versus global explanations has not been conclusively resolved. Counterfactuals, in particular, are mentioned as a technical implementation. In the interest of emphasizing contextuality, however, this technique may, in other cases in our view, also be insufficient to convey meaningful information.

5.4.2.3 Significance and the envisaged consequences

The third information element, which is not found in this form in Art. 86 of the AI Act, refers to "the significance and the envisaged consequences of such processing for the data subject". The interpretation of this element opens up great scope for interpretation.[256] According to *Paal* and *Hennemann*, it is "comparatively vague".[257] It is therefore rarely discussed in detail in the literature.

According to *Haidinger*, "it is advisable to describe the significance and the envisaged consequences as realistically as possible, e.g. in the case of insurance premiums that depend on driving behaviour, to explain that dangerous driving behaviour can result in higher insurance premiums."[258]

The A29WP also states that in order for this information to be meaningful and understandable, real, tangible examples of the type of potential impact should be provided. Responsible parties could use additional tools in the digital context to illustrate impacts (for example, when setting insurance premiums for motor vehicles automatically based on monitoring the customer's driving behaviour, it could be explained, for example, that dangerous driving can lead to higher insurance fees; this could be done by providing an app that compares fictitious drivers with each other).[259]

The ECJ, which refers to the guidelines, also points out in an obiter dictum that “real, tangible examples” should be provided and that these form part of the context of the “meaningful information about the logic involved”.[260]

According to *Dix*, an online retailer, for example, must inform its customers that it uses their data for profiling purposes in order to draw conclusions about their creditworthiness and, if they have a poor credit rating, only allow them to place orders against prepayment instead of on invoice.[261]

---

by the authors).

[256] *Stollhoff* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG^8 (2024) Art 15 DSGVO para. 23.

[257] *Paal/Hennemann* in *Paal/Pauly*, Datenschutz-Grundverordnung. Bundesdatenschutzgesetz^3 (2021) Art 15 DSGVO para. 31.

[258] *Haidinger* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 15 DSGVO para. 46 (as of 1 December 2021, rdb.at).

[259] *A29WP*, Guidelines on automated individual decision-making 28 et seq.

[260] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 45.

[261] *Dix* in *Simitis/Hornung/Spiecker gen. Döhmann*, Data Protection Law. DSGVO with BDSG (2019) Art 13 DSGVO para. 16.

According to *Bäcker*, who interprets significance and the envisaged consequences synonymously, the data controller must describe what is to be decided on the basis of the data processing, which decision-making options exist, and which processing results lead or may lead to which decision.

According to *Kamlah*, “significance” is to be understood in the sense of “meaning”, which should enable those affected to recognise how the probability value is to be assessed. The data subject should be able to recognise whether the value is a good, average or bad probability value (e.g. via generalising statements such as “above-average” risk).[262]

Information about the significance and the envisaged consequences must therefore be as realistic as possible and contain tangible examples, as well as providing those affected with information about which processing results (may) lead to which decisions and how a probability value is to be assessed.

5.4.3 Information obligations under the GDPR

The GDPR contains various provisions that address transparency towards data subjects. In particular, Art. 13 and 14 GDPR are central to this, which regulate the pre-information obligations of controllers towards data subjects. They are explained in more detail here, as they will be referenced later in comparison with the relevant provisions of the AI Act in Section 5.5.7. The scope of application of the two provisions differentiates according to the origin of the data: While Art. 13 GDPR concerns the duty to provide information "Where personal data relating to a data subject are collected from the data subject", Art. 14 GDPR provides for the obligation to provide information "where personal data have not been obtained from the data subject". General principles of these information obligations are regulated in particular by Art. 12 GDPR, according to which the controller must take appropriate measures to provide the data subjects with the information referred to in Art. 13 and 14 and the communications referred to in Art. 15 in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The two provisions show certain differences with regard to the information to be provided.[263]

---

[262] *Kamlah* in *Plath*, DSGVO/BDSG/TTDSG^4 (2023) Art 13 DSGVO para. 29.

[263] Cf. in principle *Illibauer* in *Knyrim,* Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 14 DSGVO para. 11 (as of 1 December 2021, rdb.at) and in detail below.

5.4.3.1 Article 13 GDPR

According to Art. 13 (1) GDPR, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative; (paragraph 1 lit. a)
- where applicable, the contact details of the data protection officer; (paragraph 1 lit. b)
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (paragraph 1 lit. c)
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (paragraph 1 lit. d)
- the recipients or categories of recipients of the personal data, if any (paragraph 1 lit. e) and
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. (paragraph 1 lit. f)

Unlike in the case of providing access under Art. 15 GDPR, the controller must actively take action under Art. 13 GDPR and provide the data subject with comprehensive information.[264]

According to paragraph 2, the controller must also provide the following information “necessary to ensure fair and transparent processing”[265]:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (paragraph 2 lit. a)
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (paragraph 2 lit. b)
- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (paragraph 2 lit. c)
- the right to lodge a complaint with a supervisory authority; (paragraph 2 lit. d)

---

[264] Cf., for example, *Däubler in Däubler/Wedde/Weichert/Sommer,* EU-DSGVO und BDSG. Compact Commentary³ (2024) Art 13 GDPR para. 1.

[265] The relationship between paragraphs 1 and 2 of both Art. 13 and 14 GDPR or the purpose of the corresponding subdivision is not entirely clear. However, it likely means that the information under paragraph 2 must (only) be provided to the extent necessary to explain the scope of the data processing to the data subject as transparently as possible. According to the A29WP, the information according to the two paragraphs must be provided without distinction; see overall: *Illibauer* in *Knyrim,* Der DatKomm. Praxiskommentar zum Datenschutzrecht Art 13 DSGVO paras 40 et seq (as at 1 December 2021, rdb.at).

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data (paragraph 2 lit. e) and
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (paragraph 2 lit. f)

According to Recital 60 GDPR, this information is only to be provided if necessary for fair and transparent processing, yet there are only few conceivable cases in which this information would not contribute to fair and transparent processing.[266] Therefore, companies are recommended in several places to provide all relevant information in accordance with paragraph 2 in order not to risk a sanction in view of the uncertain legal situation and consequently not to treat paragraph 2 differently from paragraph 1.[267]

In addition, Art. 13 (3) GDPR states: “Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.” When such a change of purpose is permissible is determined by Art. 6(4) GDPR, which regulates the further processing of personal data for compatible purposes.[268] The information on the change of purpose must also include the criteria that weigh in favour of the new purpose and the consequences of the change of purpose (e.g. change of recipient category or transfer to a third country), as this is the only way for the data subject to effectively exercise their rights.[269]

5.4.3.2 Article 14 GDPR

The transparency of data processing is jeopardised in particular if the data was not collected directly from the data subject and without their knowledge.[270] Art. 14 GDPR is therefore to a certain extent a "[...] catch-all provision that does not only cover collection from a third party. Rather, it also covers cases in which the controller does not carry out a 'collection' because the data subject or a third party sends him certain data on their own initiative.”[271]

According to Art. 14 (1) GDPR, the controller must therefore provide the data subject with the following information “where personal data have not been obtained from the data subject”:

- the identity and the contact details of the controller and, where applicable, of the

---

[266] With further references *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO para. 17.

[267] With further references *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO para. 17.

[268] Cf. *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO para. 24.

[269] Cf. *Däubler* in *Däubler et al,* EU-DSGVO³ Art 13 DSGVO paras 25 et seq.

[270] Cf. *Däubler in Däubler/Wedde/Weichert/Sommer,* EU-DSGVO and BDSG. Compact Commentary³ (2024) Art 14 DSGVO para. 1.

[271] *Däubler* in *Däubler et al,* EU-DSGVO³ Art 14 DSGVO para. 2a.

controller's representative; (paragraph 1 lit. a)

- the contact details of the data protection officer, where applicable; (paragraph 1 lit. b)
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (paragraph 1 lit. c)
- the categories of personal data concerned; (paragraph 1 lit. d)
- the recipients or categories of recipients of the personal data, if any; (paragraph 1 lit. e)
- where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available. (paragraph 1 lit. f)

According to paragraph 2, the following additional information “necessary to ensure fair and transparent processing in respect of the data subject”:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (paragraph 2 lit. a)
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (paragraph 2 lit. b)
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; (paragraph 2 lit. c)
- where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (paragraph 2 lit. d)
- the right to lodge a complaint with a supervisory authority; (paragraph 2 lit. e)
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; (paragraph 2 lit. f)
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. (paragraph 2 lit. g)

Art. 14 (4) further provides: “Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.”

In addition, Art. 14 (3) stipulates that the controller must provide the information at the following times:

- within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (lit. a)
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; (lit. b) or
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed. (lit. c)

5.4.3.3 Summary of Art. 13 and 14 GDPR

In conclusion, the provisions of Art. 13 and 14 GDPR provide for certain exceptions to the information obligations, in particular in the event that the data subject already has the relevant information (the only exception with regard to the standard text of Art. 13 GDPR).[272] In addition, the obligation to provide information should not apply if the storage or disclosure of the data is expressly regulated by law or if informing the data subject proves impossible or involves a disproportionate effort (cf. recital 62 GDPR).[273] Furthermore, the information under Art. 13 and 14 GDPR regarding automated decision-making does not have to be provided if this does not result in any disadvantages for the data subject.

With regard to the information to be provided on the logic involved, reference should also be made to the connection between Art. 13 and 14 GDPR with the transparency principle laid down in Art. 12 (1) GDPR, according to which the information must be provided in plain, intelligible and simple language.[274] The term "logic involved" is not defined and the recitals also do not provide any guidance.[275] It is conceivable to refer to the explanations of the old Data Protection Directive, which limits the right to information according to Art. 12 GDPR to the logical structure of the automated processing.[276] The information on the logic involved must be designed in such a way that data subjects gain knowledge, which proves to be a largely unsolved task when using complex profiling algorithms.[277] With regard to Art. 12 (1) GDPR, the information obligation should not refer to mathematical algorithms, but should contain generally understandable explanations in simple language on the basis of the calculation and the methodology.[278] This may mean that - due to the complexity of algorithms - there should be no disclosure of mathematical algorithms, but rather a general, understandable description of the calculation basis and methodology.

The controller must inform the person affected by automated decision-making about the logic involved. This may involve the methods and criteria of data processing - such as the functioning

---

[272] Cf. in detail Art. 13 (4) and Art 14 (5) GDPR.

[273] Cf. *Däubler* in *Däubler et al,* EU-DSGVO Art 13 DSGVO paras 31 et seq. and *Däubler* in *Däubler et al,* EU-DSGVO Art. 14 DSGVO paras 22 et seq.

[274] *Eßer* in *Eßer/Kramer/Lewinski*, Auernhammer. DSGVO. BDSG^8 (2024) Art 13 DSGVO paras 45 et seq.

[275] *Kamlah* in *Plath* DSGVO/BDSG/TTDSG^4 (2023) Art 13 DSGVO para. 28.

[276] *Kamlah* in *Plath* DSGVO/BDSG/TTDSG^4 Art 13 DSGVO para. 28.

[277] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG. Kommentar^4 (2024) Art. 13 DSGVO paras 55 et seq.

[278] *Kamlah* in *Plath* DSGVO/BDSG/TTDSG^4 Art. 13 DSGVO para. 29.

of algorithms used to calculate scores. An explanation of the logic involved, but not a complete disclosure of the data processing system, appears to be required. It is questionable how the tension regarding the protection of the controller's trade secrets can be resolved. A recent ECJ ruling has clarified, at least with regard to Art. 15 GDPR, that provisions such as § 4(6) Data Protection Act (DPA), which exclude, as a rule, the data subject's right of access where such access would compromise a trade or business secret, are contrary to EU law.[279] Unlike in Art. 15 (1) GDPR, the protection of trade secrets is only mentioned in Recital 63 GDPR [and there only with regard to the right of access] but is not anchored in Art. 13 (2) (f) GDPR.[280]

---

[279] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 75.

[280] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG^4 Art. 13 DSGVO paras 54 et seq.

5.5 The right to explanation in the AI Act

Article 86 AI Act

1. 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 thereof, and which produces **legal effects 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.
2. Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance with Union law.
3. This Article shall apply only to the extent that the right referred to in paragraph 1 is not otherwise provided for under Union law.

5.5.1 Scope and application of Art. 86 AI Act

Art. 86 AI Act stipulates that affected persons have the right to demand an explanation of the decision-making procedure employed by the deployer of a high-risk AI system in individual cases where the decision has been made on the basis of the system's output. This right is contingent upon the deployer having taken a decision based on the output of a high-risk AI system. However, there are numerous exceptions to this right. Firstly, the application of Art. 86 AI Act is restricted to high-risk AI systems listed in Annex III AI Act, with the exception of critical infrastructure delineated in point 2. Therefore, in terms of the material scope, Art. 86 AI Act applies to high-risk AI systems that are used for emotion recognition, in the evaluation of creditworthiness or in the pricing in the case of life and health insurance, among other areas.

Furthermore, the systems listed in Annex III are not to be considered to be high-risk where they do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons (see the exemption outlined in Art. 6(3) AI Act, which is discussed in more detail in Section 5.2.2). This includes systems that do not materially influence the outcome of decision-making, and are presumed to pose no significant risk to the health, safety or fundamental rights of natural persons.[281] This is the case, for example, if the system only performs a narrow procedural task, is intended to improve the result of a previously completed human activity, is not meant to replace a human assessment, or only performs preparatory tasks. However, there

---

[281] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO. Verordnung über Künstliche Intelligenz. Kommentar(2024) Art 86 para. 3.

is a counter-exception to this, as according to Art. 6(3) AI Act, AI systems listed in Annex III are to be classified as high-risk in any case if they carry out profiling of natural persons.

In summary, an AI system falls under the scope of Art. 86 AI Act, if considered to be a high-risk AI system pursuant to Annex III AI Act which is not exempted pursuant to Art. 6(3) AI Act, nor listed under Annex III point (2) III AI Act. Consequently, this system must produce an output that forms the basis of a decision affecting a natural person.

High-risk AI systems

The following use cases, as outlined above, have been determined to meet the criteria for classification as high-risk AI systems:

1. AI systems used for risk assessment and pricing in the case of life and health insurance.
2. Churn prediction (if combined with other high-risk systems, e.g. emotion recognition systems)
3. AI systems intended to evaluate the creditworthiness or establish a credit score, with the exception of systems for detecting financial fraud.
4. With regard to emotion recognition, Use Case 4.1 and Use Case 4.2 can be categorised as high-risk AI systems (provided that no prohibited practices under Art. 5 AI Act are involved). In principle, this also applies to Use Case 4.3, unless an exception pursuant to Art. 6 (3) (b) AI Act (improvement of previously completed human activity) applies.

In addition, Art. 86 AI Act stipulates that the deployer must make the decision "based on" the output of the system. Recital 171 AI Act further specifies that this decision must be "mainly" based on the output of the system. This raises the question of what influence the output of the AI system must have for decisions to be based on it, and whether decisions that are only partially prepared by the system are not covered.[282] However, it is widely acknowledged that the prevailing normative text of Art. 86 AI Act takes precedence over the non-legally binding recitals.[283] Consequently, it is considered sufficient if the output of the AI system was relevant for the decision and did not merely play a subordinate role.[284] In summary, any significant influence on the decision-making procedure that has an effect on the content and outcome of

---

[282] This is the opinion of *Feiler/Forgó*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art 86 para. 4.

[283] Cf. ECJ 13 July 2023, C-376/20 P, *Commission/CK Telecoms UK Investments*, ECLI:EU:C:2023:561, para. 105: "However, the preamble to an EU act has no binding legal force and cannot be relied on as a ground either for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner that is clearly contrary to their wording [...]."

[284] Cf. the discussion in *Hornung*, Individualrechte in der KI-Verordnung. Die Rechte auf Beschwerde und auf Erläuterung der Entscheidungsfindung im Einzelfall, DuD 2024, 507 (510).

the decision can be considered to be covered by Art. 86 AI Act.[285] At this point, it should be emphasised that, in contrast to Art. 22 GDPR, Art. 86 AI Act does not require the system to make the decision itself. Consequently, Art. 86 AI Act also applies, if the system's outputs form the basis for a (fully) human decision.[286] If this requirement is met, the right to explanation can be enforced against the deployer of the AI system, i.e. those companies or organisations that use the AI system under their authority as part of their professional activities.

Example

In the event that an insurance company procures an AI system from a third party for the purpose of calculating price adjustments for its customers, the insurance company becomes the deployer against whom the right to explanation under Art. 86 AI Act is to be directed.

However, it is more challenging to assess scenarios where a company uses the AI system to generate an output (e.g. a credit reference agency calculates a credit score) and then sells the output to another company, which then makes a decision based on the output (e.g. a mobile phone company purchases a customer’s credit score and subsequently makes a decision based on that score regarding the initiation of a contractual relationship with these customers). In such cases, the roles of the deployer and the company making the decision diverge. However, since "credit scores" can also represent decisions that prepare the final main decision (e.g. issuing a mobile phone contract), the right to explanation can probably be enforced against the deployer, i.e. against the credit reference agency that "uses the AI system under its authority" (Art. 3(4) AI Act). Affected persons can ascertain the credit reference agency from which the mobile phone company procured the "credit scores" by exercising their right of access under Art. 15 GDPR.

In a subsequent step, the decision must produce legal effects or significantly affect natural persons in a similar manner, specifically in their health, safety or fundamental rights. This means that the right to explanation does not apply if the decision made on the basis of the system exhibits no substantial adverse effect on the affected person. In accordance with the wording of Art. 22 GDPR, the term “legal effect” is to be defined as the establishment, termination or adjustment of a legal status.[287] Similar to the discussion regarding Art. 22 GDPR (refer to Section 5.4.1 for further details), the question of whether the term "legal effects" should always be interpreted in a negative sense, or whether positive legal effects also fall within the

---

[285] *Anderl/Ciarnau* in *Zankl*, KI-VO. Verordnung über künstliche Intelligenz (Artificial Intelligence Act). Kurzkommentar (2025) Art 85-87 para. 7.

[286] Cf. *Hornung*, DuD 2024, 507 (510) or *Anderl/Ciarnau* in *Zankl,* Art 85-87 para. 7.

[287] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 13.

scope of application of Art. 86 AI Act, arises. An analysis of the relevant recitals indicates that the scope of application extends exclusively to negative legal effects. This assertion is supported by Recital 171 AI Act, which stipulates that the right to obtain an explanation applies as soon as the decision "produces legal effects or similarly significantly affects those persons a way that they consider it to have ***adverse*** impact on their health, safety or fundamental rights."[288] In the context of health, safety and fundamental rights, Recital 171 AI Act explicitly refers to negative effects. In contrast to the unclear situation with regard to Art. 22(1) GDPR, this also applies to the German and French language versions of the Recital. To a certain extent, these effects are equivalent in their interpretation to legal effects, which suggests that only negative legal effects should be covered in this context. This view is further substantiated by the repeated emphasis of the ECJ on the importance of recitals in the interpretation of the legally-binding provisions in question, provided that the recitals do not conflict with the provisions to be interpreted.[289] Moreover, in contrast to Art. 22 DSGVO, Art. 86 AI Act does not prohibit automated decision-making procedures, but rather serves as a legal right, which many scholars regard as an *ex post* claim.[290] In case of doubt, it is nevertheless recommended that the term "legal effects" be interpreted more broadly and therefore to include any effect, regardless of whether it is categorised as positive or negative (refer to the discussion in Section 5.4.1 for further details).

Recital 171

Affected persons should have the **right to obtain an explanation** where a **deployer's decision** is based **mainly** upon the **output from certain high-risk AI systems** that fall within the scope of this Regulation and where that decision produces legal effects or similarly significantly affects those persons in a way that they consider to have an **adverse impact on their health, safety or fundamental rights**.

That **explanation** should be **clear and meaningful** and should **provide a basis** on which the affected persons are able to **exercise their rights**. The right to obtain an explanation should not apply to the use of AI systems for which exceptions or restrictions follow from Union or national law and should apply only to the extent this right is not already provided for under Union law.

The additional requirement in Art. 86 AI Act that natural persons must be adversely affected in their health, safety or fundamental rights raises the question of when an "adverse effect" can

---

[288] Emphasis added.

[289] Cf. ECJ 21 April 2023, C-10/23, *Remia Com Impex*, ECLI:EU:C:2024:259, para. 51: "[A]ccording to settled case-law, the preamble to an EU act may explain the content of the provisions of that act and that the recitals of such an act constitute important elements for the purposes of interpretation, which may clarify the intentions of the author of that act."

[290] Cf. *Radtke,* Das Verhältnis von KI-VO und Art. 22 DS-GVO unter besonderer Berücksichtigung der Schutzzwecke, RDi 2024, para. 353 (para. 358).

be assumed. The literature provides examples such as decisions on healthcare services as an impairment of health or decisions linked to discriminatory criteria and group affiliations as an adverse effect on fundamental rights.[291] With regard to purely financial disadvantages, however, their categorisation as one of those impairments is questionable, unless they are covered as legal effects. While there are opponents to this view[292], proponents argue that specific financial disadvantages can indeed constitute an impairment of fundamental rights. Furthermore, it can be inferred from Recital 5 AI Act that economic damage can also infringe fundamental rights. The decisive factor is probably the type and extent of the financial disadvantage. It is also noteworthy that the phrase "that they consider to have an adverse impact" indicates that the perspective of the person affected is relevant to the question of impairment.[293]

Example

For example, systems unlikely to cause fundamental rights infringements include systems optimising document handling, information storage or improving indexing, searching, or text processing.[294]

Similarly, the use of emotion recognition by a prominent online fashion retailer to provide personalised advertising is not assumed to violate fundamental rights (unless the advertising is displayed across various devices and in the form of "retargeting" that is perceived as highly annoying, or occurs in a discriminatory or highly manipulative manner). This seems improbable in the context of Use Case 4.3.a in relation to emotion recognition in advertising, provided that it is solely employed for the purpose of making adjustments or improvements to products or services.

Nevertheless, such systems may potentially infringe upon fundamental rights if, for instance, an advertising campaign promoting sports betting is targeted at an individual with a gambling addiction on the basis of emotion recognition (refer to Use Case 4.1 for further details).

Furthermore, Art. 86 AI Act states that affected "persons" have the right to explanation of individual decision-making. In view of the open wording of Art. 86 AI Act, which only refers to

---

[291] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 13.

[292] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 13.

[293] Cf. *Hornung*, DuD 2024, 507 (510); *Metikos/Ausloos*, Law, Innovation, and Technology 2025, tpb, and *Anderl/Ciarnau* in *Zankl,* Art 85-87 para. 9.

[294] Cf. *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (as at 24 April 2024).

"persons", it is questionable whether the right under paragraph 1 only covers natural persons or also legal persons. There are several arguments in this regard. Firstly, the wording suggests that both natural and legal persons could be encompassed, given the AI Act's explicit address of natural persons in other provisions, e.g. Art. 26(11) and Art. 27(1)(c) and (d). In addition, certain aspects addressed by the provision, such as legal effects and interference with fundamental rights, could also be applicable to legal persons.[295] However, literature also points out that, in contrast to Art. 86, for example, Art. 85 AI Act explicitly refers to *legal* persons and natural persons alike. Moreover, it is argued that Art. 26(11) AI Act and the associated recital 93, which to a certain extent pertain to Art. 86, also exclusively refer to *natural* persons. Based on these considerations, among others, proponents of this view argue that Art. 86 AI Act likely pertains to natural persons only, in accordance with the intention of the legislator.[296]

In response to this, it can be argued that the persons addressed by Art. 27(1)(d) AI Act[297] were explicitly restricted to natural persons during the legislative process in accordance with Art. 27(1)(c) AI Act[298] , which underlines a corresponding intention to clarify or restrict in this area. Accordingly, the fact that Art. 86, compared to other provisions of the AI Act, was **not** similarly restricted and **does not** explicitly refer to natural persons only could already indicate a corresponding legislative intent for a more open formulation.

This perspective is further substantiated by the interpretation that Art. 86 AI Act is a provision that ensures protection that extends beyond the provisions of the GDPR.[299] This is due to the fact that, firstly, the GDPR, and consequently Art. 15 and 22, are not applicable to legal entities.[300] Secondly, there appears to be a corresponding necessity for protection in terms of the general objectives of the AI Act.[301] In this context, small companies could be considered, for example, that are denied a loan that is important for the continued existence of the company due to AI-based credit scoring. In particular, it seems fundamentally inappropriate in this context to distinguish between a one-person company as a legal entity and a natural person undertaking entrepreneurial activities individually. However, in contrast to Article 86 AI Act, most of the points listed in Annex III explicitly refer to natural persons, such as point (5)(b) on credit scoring. Nonetheless, it is conceivable that certain cases enumerated in Annex III may also pertain to legal persons (such as point (8)); moreover, Annex III may also be amended (Cf. Article 7 AI Act).

In view of the ECJ's potential broad interpretation of Art. 86 AI Act based on the *effet utile*, it is therefore advisable to assume the applicability of this provision to legal entities.

Art. 86(2) AI Act states that the right to explanation shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under paragraph 1 follow from Union

---

[295] Cf. *Hartmann* in *Martini/Wendehorst*, KI-VO Art 86 para. 12.

[296] Cf. overall *Hartmann* in *Martini/Wendehorst*, KI-VO Art 86 para. 12, according to whom a definition of affected persons proposed in the meantime in the legislative process would only have been only aimed at natural persons (and *groups of persons*), although this was ultimately not included in the final text.

[297] This does not pertain to the *groups of people* mentioned by this provision.

[298] Cf. *Fülöp/Poindl* in *Pehlivan/Forgó/Valcke*, AI Act Art 27 Section 3.3.4.4.

[299] Refer to Section 5.5.5 for further details.

[300] Cf. Art. 2 and 4(1) GDPR.

[301] Cf. Art. 1 AI Act, also in comparison to Art. 1 GDPR, which in turn explicitly refers only to natural persons.

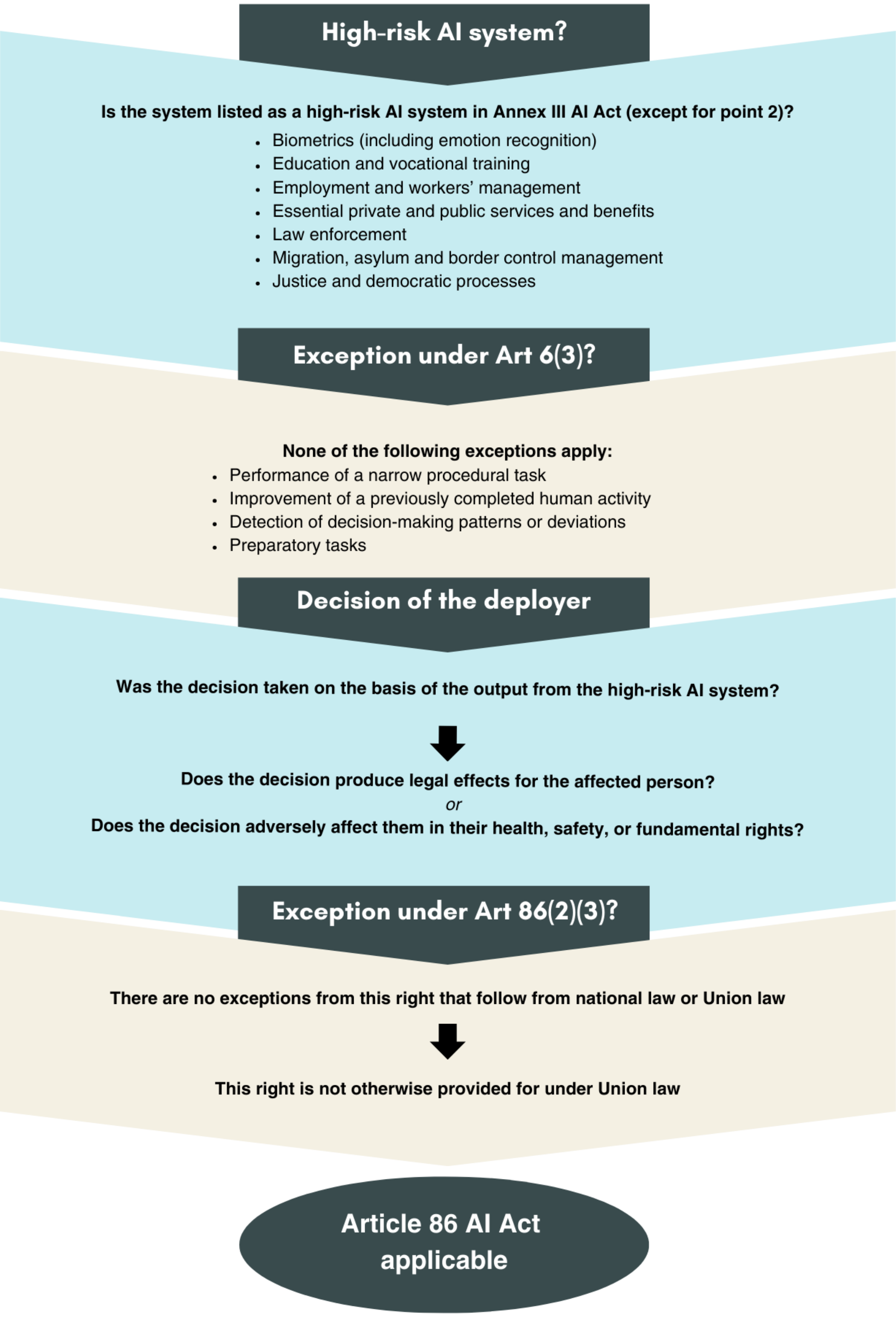
or national law in compliance with Union law. In this context, material or sectoral exceptions to the obligation to provide an explanation may be considered, provided that the limits of Union law are respected.[302]

Art. 86(3) AI Act enshrines the subsidiarity of Art. 86 AI Act and clarifies that it only applies to the extent that the right to explanation is not otherwise provided for under Union law. This can be understood as a reference to the right of access under Art. 15(1)(h) in conjunction with Art. 22 GDPR.[303] The extent to which Art. 86 AI addresses the lacunae in cases not covered by Art. 22 and Art. 15(1)(h) GDPR will be examined in more detail in Sections 5.5.4. and 5.5.5.

---

[302] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 16.

[303] Cf. *Nannini*, Habemus a Right to an Explanation. So What? A Framework on Transparency-Explainability Functionality and Tensions in the EU AI Act, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4896020 (as at 16 August 2024): "Article 86(3) specifies that the RTE applies only to the extent that it is not otherwise provided for under Union law, such as the GDPR's RTE arising from Articles 15(1)(h) and 22(1)."



High-risk AI system?

Is the system listed as a high-risk AI system in Annex III AI Act (except for point 2)?

- Biometrics (including emotion recognition)
- Education and vocational training
- Employment and workers’ management
- Essential private and public services and benefits
- Law enforcement
- Migration, asylum and border control management
- Justice and democratic processes

Exception under Art 6(3)?

None of the following exceptions apply:

- Performance of a narrow procedural task
- Improvement of a previously completed human activity
- Detection of decision-making patterns or deviations
- Preparatory tasks

Decision of the deployer

Was the decision taken on the basis of the output from the high-risk AI system?

⬇

Does the decision produce legal effects for the affected person?

or

Does the decision adversely affect them in their health, safety, or fundamental rights?

Exception under Art 86(2)(3)?

There are no exceptions from this right that follow from national law or Union law

⬇

This right is not otherwise provided for under Union law

Article 86 AI Act applicable

Figure 3: Checklist applicability of Article 86 AI Act

5.5.2 Elements of the explanation

If the decision produces **legal effects** or **similarly significantly affects** persons in a way that they consider to have an adverse impact on their health, safety or fundamental rights, these persons 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.

5.5.2.1 Role of the AI system in the decision-making procedure

Clarifying the explanation about the **role** of the AI system in the decision-making procedure is relatively unproblematic. The role in the decision-making procedure can be defined as the respective contributions to the decision by humans or machines alike.[304] Accordingly, it is necessary to explain how the decision was reached with the **involvement** of the AI system, what part of the decision was determined by the system, what scope was left for human actors to correct or adjust the decision, and how this scope was used in individual cases.[305] Specifically, this entails a process-oriented understanding, necessitating information about the stage of the decision-making procedure in which the AI system is employed, its purpose (e.g. for pre-selection, categorisation, analysis, etc.), the extent of its involvement in the decision-making procedure, and the degree to which a human adaptation of the decision was possible or actually occurred.[306]

5.5.2.2 The main elements of the decision taken

A. *General information*

The AI Act does not specify what exactly is meant by the **"main elements"** of the decision taken and therefore leaves room for interpretation. In terms of a teleological interpretation of Art. 86 AI Act, transparency regarding the decision-making procedure plays a key role.[307] To illustrate this point, as set out in Recital 171 AI Act, the explanation must provide a basis on which the affected persons are able to exercise their rights. In order to do so, the affected person must, in any case, be able to assess the central steps and influencing factors of the decision-making procedure.[308] In summary, the specific scope of Art. 86 AI Act remains vague, but the following formula could provide a point of orientation: The more serious the expected impairments, the higher the demands on the explanation.[309]

There can be two key types of explanations: On the one hand, explanations can include a

---

[304] Cf. *Merkle*, Transparenz nach der KI-Verordnung - von der Blackbox zum Open-Book? RDi 2024, 414 (419).
[305] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 15.
[306] Cf. *Anderl/Ciarnau* in *Zankl,* Art 85-87 para. 10 and *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 15.
[307] Cf. *Hornung*, DuD 2024, 507 (511).
[308] *Hornung*, DuD 2024, 507 (511).
[309] *Hornung*, DuD 2024, 507 (511).

process-based explanation, which encompasses information about the control of the AI system during its development and deployment.[310] The process-based explanation is frequently associated with the obligation to provide information under data protection law and is understood as *an ex ante approach prior* to the specific decision. Closely related to this are explanations that focus on system functionality, including the logic, envisaged consequences, significance and general functionality of the system. Examples of explanations that focus on system functionality include explanations of the underlying model, classification structures or decision trees.[311]

On the other hand, explanations may encompass an *outcome-based explanation*, which should provide information regarding the circumstances that led to a particular decision.[312] This category of explanation refers to the content of a specific decision and includes the primary reasons for the decision, the individual circumstances of a specific automated decision, the weighting of features, machine-defined case-specific decision rules, and information about reference or profile groups.[313] This category is primarily concerned with individuals impacted by an AI-based decision and thus adopts an *ex-post approach*, which is also an inherent aspect of Art. 86 AI Act as a claim to be granted retrospectively.[314] This is due to the general absence of direct coverage by Art. 86 AI Act of a prior duty of the deployer to provide information to natural persons affected by decisions supported by high-risk AI systems.[315] Despite the indications in the recitals that the deployer must inform affected persons in advance about their rights under Art. 86 AI Act, Recital 93 AI Act contains the following reference: "Deployers of high-risk AI systems listed in an annex to this Regulation also play a critical role in informing natural persons and should, when they make decisions or assist in making decisions related to natural persons, where applicable, inform the natural persons that they are subject to the use of the high-risk AI system. This information should include the intended purpose and the type of decisions it makes. The deployer should also inform the natural persons about their right to an explanation provided under this Regulation." However, it should be noted that this explicit duty to provide information regarding the rights of individuals is not directly derived from Art. 86 of the AI Act, but rather, it is **regarded as encompassed by Art. 26(11) AI Act**, which enshrines a right to be informed about the utilisation of high-risk AI systems to support decision-making processes. A broad interpretation of Art. 26(11) AI Act is recommended, which also includes the obligation to provide information in advance about the right to explanation under Art. 86 AI Act (Refer to Section 5.5.7 for more detailed explanations).[316]

---

[310] Cf. *Information Commissioner's* Office/The *Alan Turing Institute,* Explaining decisions made with AI (2022) 23 et seq., https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence-1-0.pdf.

[311] Cf. *Kim/Routledge,* Why a Right to Explanation of Algorithmic Decision-Making Should Exist. A Trust-Based Approach, Business Ethics Quarterly 2022, 75 (80) and *Wachter/Mittelstadt/Floridi,* International Data Privacy Law 2017, 78.

[312] Cf. *Information Commissioner's* Office/The *Alan Turing Institute,* Explaining decisions 23 et seq.

[313] Cf. *Kim/Routledge*, Business Ethics Quarterly 2022, 75 (78).

[314] Cf. *Radtke,* RDi 2024, para. 353 (para. 358).

[315] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 5 and *Merkle*, RDi 2024, 414 (419). Refer to Section 5.5.7 for further details about information obligations with regard to Art 86 AI Act.

[316] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 5.

B. Comparison with the predecessor provision of Art. 68c [EP version]

Prior to delving into the specifics of the content of the decision, it is worth taking a look at the original version of Art. 86 AI Act. This provision was not yet part of the AI Act in the Commission's draft and was initially included in the text as Art. 68c at the suggestion of the EP. When comparing the final content of Art. 86 AI Act with that of its predecessor, Art. 68c AI Act [EP version], it is evident that it was significantly restricted. Art. 68c (1) AI Act [EP version] read as follows:

"Any affected person subject to a decision which is taken by the deployer on the basis of the output from an high-risk AI system which produces legal effects or similarly significantly affects him or her in a way that they consider to adversely impact their health, safety, fundamental rights, **socio-economic well-being or any other of the rights deriving from the obligations laid down in this Regulation**, shall have the right to request from the deployer clear and meaningful explanation **pursuant to Article 13(1)** on the role of the AI system in the decision making procedure, the main **parameters of the decision taken and the related input data**."[317]

Firstly, the adverse effect on socio-economic well-being has been removed as a requirement. The reference to the transparency obligation under Art. 13(1) AI Act has also been dropped, as Art. 13 AI Act no longer contains a cross-reference to Art. 68c AI Act [EP version] like previously in the EP version. Nevertheless, the link between the transparency obligation enshrined in Art. 13 AI Act and the final version of Art. 86 AI Act cannot be disregarded, as it is mandatory that the former precedes the deployer's fulfilment of the right to explanation. The deployer will not be able to provide adequate information about the decision-making procedure if the system is not sufficiently transparent and they thus cannot adequately interpret its outputs. Further implications of the history of Art. 86 AI Act that are relevant to the specific components of the explanation are referred to below.

C. Specific components of the explanation

The following components can be considered the "most important elements" of an AI-based decision. These were drawn from literature, from conclusions derived from the process leading to the final version of Art. 86 AI Act, and analogies from data protection law:

- It can be assumed that the "main elements of the decision taken" are first and foremost the factors on which the decision is based, which are to be delivered in an accessible and not too technical way.[318] This includes the main reasons for the decision, which are to be understood as **central influencing factors** ("characteristics"), i.e. the criteria that led to the decision; in summary, all the information about the data on the basis of which a decision was made.[319] This also includes, for example, **preliminary decisions** that determine the final "main decision" (e.g. segmentation of target groups).[320]

---

[317] Emphasis added.

[318] Cf. *Information Commissioner's* Office/The *Alan Turing Institute,* Explaining decisions, 21.

[319] Cf. *Information Commissioner's* Office/The *Alan Turing Institute,* Explaining decisions, 21.

[320] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 15.

Whether this also includes so-called **input data** must be analysed by looking at the predecessor provision, Art. 68c AI Act [EP version]. In addition to the role of the system in the decision-making procedure, Art. 68c AI Act [EP version] contained the mandatory disclosure of the main "parameters" and the "related input data" in contrast to the main "elements" pursuant to Art. 86 AI Act. The terminological shift from "parameters" to "elements" suggests an expansion of the required content, as the term "parameters" refers to algorithmic or technical parameters, while "elements" allows for a broader interpretation that goes beyond technical aspects.[321] However, this opening of the scope of application is somewhat relativised, at least as far as the factors preceding the decision are concerned. This is because the "relevant input data", still contained in Art. 68c AI Act [EP version] no longer appears in the final text as a further component of the explanation. It can therefore be concluded that this information is no longer to be provided, which in turn would drastically contradict the *télos* of Art. 86 AI Act. This is because information about the input data in particular is likely to be essential for affected persons, who might want to know on what data concerning them a decision was based. This is also emphasised in the literature on the ethical use of AI, where, for example, *Brey* and *Dainow* (2024) point out that there must always be mechanisms in place to explain the decision itself and the data used for it to the persons affected.[322] However, from a legal perspective, such a requirement can also be found in the final version of the AI Act. Recital 171 AI Act states that the explanation should provide a basis on which affected persons can exercise their rights. This is particularly true for explanations about the input data, as affected persons are unlikely to be able to exercise any subsequent rights if they do not have any information about the data on which the decision was based in the first place. The counter-argument that reference can be made to the right of access under Art. 15 GDPR for information about the data processed is not tenable, as the input data does not always have to be personal data, which would render the GDPR inapplicable.[323]

- Likewise, it is mandatory to provide detailed information about how this data or influencing factors contributed to the decision-making procedure.[324] This is particularly salient in the context of the **weighting of features/parameters** and the influence of specific data on the decision-making procedure. However, it is not entirely undisputed whether it is necessary to include this information. For instance, *Hacker* (2024) does not consider the so-called "feature salience" (identifying which features of the input data were most influential in the decision-making process) to be covered by the right

---

[321] Cf. the definitions of "parameter" and "element" in the Duden online dictionary: https://www.duden.de/rechtschreibung/Parameter and https://www.duden.de/rechtschreibung/Element (Last access: 14 February 2025).

[322] Cf. *Brey/Dainow,* Ethics by design for artificial intelligence, AI and Ethics 2024, 1265 (1269).

[323] The fact that input data must in any case be provided with information in accordance with Art. 15 GDPR can be substantiated by the right to a copy laid down in Art. 15(3) GDPR. This right encompasses the provision of extracts from databases, copies of all personal data that are the subject of processing, and, in certain instances, entire documents that (at least partially) allow conclusions to be drawn about the input data. The right to a copy and its implications for the data to be transferred are addressed and further strengthened in the Opinion in the case Dun & Bradstreet, among others (Cf. *Advocate General de la Tour* 12 September 2024, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2024:745, paras 40 et seq.).

[324] Cf. *Information Commissioner's* Office/The *Alan Turing Institute,* Explaining decisions, 21.

to explanation under Art. 86 AI Act; yet, he partially relativises this general exclusion assuming that these features and their influence must be explained if they can be considered to be part of the main elements of the decision.[325] Because the weighting of parameters or an explanation of which characteristics essentially influenced the decision can provide information about potential discrimination or bias in the specific decision-making procedure, it can definitely be assumed that they belong to the "main elements". This is also in line with the objective of the protection of fundamental rights by the AI Act, as enshrined in Art. 1(1) AI Act.[326]

- Another category pertains to the **impact** of the use of an AI system and its decisions on individuals and society. Despite the fact that the impact of the decision on affected persons is not explicitly referenced as part of the explanation under Art. 86 AI Act, it is mentioned in Art. 15(1)(h) GDPR. Consequently, when we look at these provisions together, it is recommended that the statement on the impact of the decision be considered a part of the "main elements" of the decision. This recommendation is further substantiated by the protective purpose of the provision, and the fact that the ECJ in its case law follows the principle of interpreting the wording of a provision so as to ensure that it has the most optimal impact (*effet utile*). It could be argued that the deployer of an AI system cannot always foresee the effects of a decision, since these effects always also have a subjective component from the perspective of the person affected, as previously discussed. However, this is countered by the fact that deployers must implement effective human oversight mechanisms in accordance with Art. 14 AI Act and must therefore understand the risks associated with the use of the system. Furthermore, in some cases, a fundamental rights impact assessment according to Art. 27 AI Act, or a data protection impact assessment as outlined in Art. 35 GDPR may be required, thereby compelling the deployer to address the impact of the AI system's utilisation. Furthermore, the aforementioned efficiency requirement (or *effet utile)* speaks against such an interpretation. In addition, Recital 171 AI Act expressly points out that affected persons must be able to exercise their rights based on the explanation, for which the information on the effects of a decision is a decisive premise.
- A further component of the explanation pertains to information about the algorithmic code underlying the system, provided that this does not necessitate the disclosure of trade and business secrets. However, given that explanations of the algorithmic code are often associated with such a disclosure, it is generally assumed that it is not the entire algorithm and its mode of operation that must be disclosed, but rather the algorithmic weighting of the most important parameters[327] and a description of the system processes or how the algorithm roughly operates (e.g. whether it is a machine learning system, etc.). This is because it is imperative to ensure that the existence of trade secrets does not lead to a full refusal of the information request or to the failure to provide information at all in this regard. In the event of the code being disclosed, the

---

[325] Cf. *Hacker*, Comments on the Final Trilogue Version of the AI Act 11, https://ssrn.com/abstract=4757603 (as at 23 January 2024).
[326] Following this argumentation: *Anderl/Ciarnau* in *Zankl,* Art 85-87 para. 10.
[327] Cf. *Anderl/Ciarnau* in *Zankl,* Art 85-87 para. 10.

> respective explanation should therefore be one that provides information about the actual terms of the interface between the inputs and outputs of algorithms and the underlying assumptions, as well as how datasets were trained and implemented.[328] In addition, the right of data subjects to receive proper information about the storage and destruction procedures, as well as about the terms of any process to obtain informed consent as required is being raised at this point.[329]

Whilst not directly derivable from Art. 86 AI Act, an explanation on the responsibility chain is recommended. This should indicate who is involved in the development, management and implementation of the system, and who to contact for a human review of a decision.[330]

It is important to note, however, that different contexts and situations give rise to different explanation needs.[331] While system developers, for example, need to be familiar with precise technical details about how an AI system works, affected persons may be more interested in the factors that led to a decision. Affected persons, in particular, are interested in information about the origin of the data, why their data was processed, how the underlying model operates, which factors influence the decision, and why a certain output was achieved.[332]

5.5.3 Formal aspects of Art. 86 AI Act

The formal aspects related to Art. 86 AI Act, e.g. the deadline for responding to requests for information, the form of the explanation or the question of the associated costs, are not mentioned at all in Art. 86 AI Act. It is therefore necessary to await supreme court rulings on these issues. Consequently, the following elaborations have to be understood as recommendations only, until these open questions have been fully clarified. The right to explanation pursuant to Art. 86 AI Act must in any case be asserted by means of a request from the affected person.

5.5.3.1 Deadline

The AI Act does not specify a deadline until which the deployer must respond to a request for information under Art. 86 AI Act. It is therefore recommended to use the corresponding provisions of the GDPR by analogy, given that, in practice, affected persons can exercise both the right of access under Art. 15 GDPR and the right to explanation under Art. 86 AI Act concurrently and a different deadline would not be appropriate. Art. 12 GDPR is the relevant provision under data protection law, which states that the data subject must be provided with

---

[328] Cf. *European Parliamentary Research Service (EPRS)* Artificial Intelligence ante portas. Legal & Ethical Reflections 2, https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf (as at 19 March 2019).

[329] Cf. *European Parliamentary Research Service,* Artificial Intelligence ante portas 2.

[330] Cf. *Information Commissioner's* Office/The *Alan Turing Institute,* Explaining decisions, 21.

[331] Cf. *The Royal Society,* Explainable AI. The basics. Policy briefing (2019) 19, https://ec.europa.eu/futurium/en/system/files/ged/ai-and-interpretability-policy-briefing_creative_commons.pdf.

[332] Cf. *The Royal Society,* Explainable AI 19.

the relevant information without undue delay and in any event **within one month of receipt of the request**. In case of complex requests, it is permissible to extend this period **by two further months**, about which the data subject must be informed together with the reasons for the delay within one month of receipt of the request.

Of course, there can be instances, where the collection of relevant information within the stipulated timeframe is not feasible due to the complexity of the AI system. In such cases, an extended deadline may be necessary. This will likely require a case-by-case evaluation.

5.5.3.2 Form and costs of the explanation

The AI Act does not contain any requirements in this regard. Consequently, reference must again be made to Art. 12 GDPR. Accordingly, affected persons must be provided with the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The response to the request for information can be provided in **any appropriate form**, for example orally, in writing or by electronic means. If the affected person submits the request electronically, it must also be answered electronically wherever possible. Furthermore, the information must be provided **free of charge**, except in circumstances where the requests are excessive or manifestly unfounded (Cf. Art. 12(5) GDPR).

5.5.3.3 Negative information

It is conceivable that individuals may claim the right to explanation under Art. 86 AI Act even though they are not entitled to it. This may be because they are not affected by a decision, or because a decision concerning them was not made with the support of a high-risk AI system within the meaning of Art. 86 AI Act. Even though not explicitly laid down in law, based on a broad interpretation of Art. 26 (11) AI Act, negative information should be provided to the requesting person in these cases, i.e. a reference to the fact that no decisions are currently being made on the basis of the AI system's output, along with an explanation of why Art. 86 AI Act does not apply. This is recommended for documentation purposes and in the interest of customer satisfaction (refer to Section 5.5.7 for further details).

5.5.4 The value of Art. 86 AI Act

It is striking that while the GDPR contains a comprehensive catalogue of data subject rights in Articles 15 et seq., the AI Act, through Art. 86, merely provides for a single comparable (“ex-post”) right for affected persons (refer to Section 5.5.7 for more details on other rights, in particular information obligations).[333] Although Art. 85 AI Act enshrines a right to lodge a

---

[333] *Schwartmann/Köhler*, Rechtsbehelfe, in *Schwartmann/Keber/Zenner* (eds.), KI-VO. Leitfaden für die Praxis (2024) para. 56 (para. 58).

complaint with a market surveillance authority and Art. 87 AI Act regulates the reporting of infringements and the protection of whistleblowers, the legal remedies granted under the AI Act are limited to these provisions and Art. 86 AI Act remains the only one that can be directly enforced against the deployer. It is therefore all the more welcome that the right to explanation, which was not yet provided for in the European Commission's original draft regulation, was finally included in the text at the request of the European Parliament.[334]

However, given the exceptions mentioned in Art. 86(1) and (2) AI Act and the subsidiarity clause of Art. 86(3) AI Act, only a narrow scope of application of this provision remains.[335] For this reason, the value of Art. 86 AI Act is contested in some places, arguing that the original draft regulation specifically had excluded the right to explanation.[336] Proponents of this view argue that the *explanatory memorandum* of the EU Commission asserts that the right to explanation is already established in other provisions of the AI Act, such as the transparency requirement of Art. 13 and the human oversight enshrined in Art. 14. This is said to be the reason why the scope of application of Art. 86 AI Act remains limited.[337] However, the aforementioned provisions do not impose a direct obligation on the deployer to explain AI decisions to affected persons, which underscores the value of an explicitly enshrined right to explanation. It can facilitate exercising follow-on rights by affected persons because in analogy to the right of access enshrined in Art. 15 GDPR, the right to explanation can serve as a prerequisite for the assertion of other legal claims.[338] This could include, for example, product liability claims[339] or legal remedies against the decision itself, which essentially depend on whether the affected persons can provide information about the reasons for the decision and the decision-making procedure. Further considerations on the value of Art. 86 AI Act arise in particular in relation to the right of access under the GDPR (see below).

5.5.5 Demarcation issues and filling the gaps

The initial question is whether the subsidiarity of Art. 86 AI Act means that it does not apply in instances where Art. 22 in conjunction with Art. 15(1)(h) GDPR are applicable, or whether the

---

[334] *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner* para. 56 (para. 58).

[335] *Schwartmann/Köhler* in *Schwartmann/Keber/Zenner* para. 56 (para. 58).

[336] Cf. e.g. *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (as at 24 April 2024).

[337] Cf. e.g. *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (as at 24 April 2024). or *Panigutti/Hamon/Hupont/Fernandez Llorca/Fano Yela/Junklewitz/Scalz/Mazzini/Sanchez/Soler Garrido/Gomez,* The role of explainable AI in the context of the AI Act, in ACM (ed.), FAccT '23. Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency 2023, 1139.

[338] Cf. *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (as at 24 April 2024).

[339] Cf. *Radtke,* RDi 2024, para. 353 (para. 358).

right to explanation under Art. 86 AI Act exists in addition to the corresponding rights laid down in the GDPR. This is based on the premise that the right of access under the GDPR does not encompass certain aspects that are encompassed by Art. 86 AI Act, thus creating a “gap-filler position” of the latter. Art. 86(3) AI Act, which states that this provision applies only to the extent that the "right referred to in paragraph 1" is not otherwise provided for under Union law, lends support to the latter interpretation. The wording of Art. 86(3) AI Act appears to comprise a complete identity of both facts and legal consequences.[340] Furthermore, it is argued that the subsidiarity of Art. 86 AI Act can be assumed if another valid provision applicable to the individual case brings about a comparable legal consequence for the person affected. The characteristics of the seemingly competing provisions would not be congruent in this instance.[341] *Metikos* and *Ausloos* are also of the opinion that Art. 86 AI Act “does not amend the right to an explanation under the GDPR but rather provides an additional right that individual decision-subjects can exercise besides the right to an explanation under the GDPR."[342]

The right under paragraph 1 does not contain the same elements as the right of access under Art. 15 GDPR, as the phrase "the logic involved, as well as the significance and the envisaged consequences of such processing" from Art. 15(1)(h) GDPR does not necessarily coincide with the explanation of the "role of the AI system in the decision-making procedure and the main elements of the decision taken" in accordance with Art. 86(1) AI Act. For example, the role of the system in the decision-making procedure does not have to be explicitly explained in accordance with Art. 15(1)(h) GDPR. In addition, Art. 22 GDPR refers to a decision based solely on automated processing, whereas the right under Art. 86 AI Act only requires that the system's outputs form the basis of the decision.[343] Moreover, the right to explanation refers to high-risk AI systems, whereas this is irrelevant for the applicability of Art. 22 GDPR.[344] This is also emphasised by Recital 10 AI Act, which clarifies that "[...] data subjects continue to enjoy all the rights and guarantees awarded to them by such Union law, including the rights related to solely automated individual decision-making, including profiling." Thus, both the content as well as the prerequisites and legal consequences are regulated completely differently by Art. 86 AI Act and Art. 15(1)(h) in conjunction with Art. 22 GDPR.[345] Therefore, this report and the manuals follow the interpretation that both legal remedies can exist in parallel.[346]

An argument against this reading is that Art. 68c AI Act [EP version] still contained an explicit reference in paragraph 3 that the right to explanation applies independently of the Articles 13, 14, 15 and 22 GDPR. By contrast, the final version of paragraph 3 no longer contains this reference and has instead been replaced by the subsidiarity clause. This indicates a preference of the EU legislator to not allow for the coexistence of both rights. However, the draft version of this provision should not be given too much legal relevance in the sense that it

---

[340] Cf. *Hornung*, DuD 2024, 507 (511).
[341] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 paras 17 et seq.
[342] *Metikos/Ausloos,* Law, Innovation, and Technology 2025, tpb.
[343] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 18.
[344] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art 86 para. 18.
[345] Cf. *Ebers*, Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU's AI Act, European Journal of Risk Regulation 2024, 1 (13).
[346] Cf. *Anderl/Ciarnau* in *Zankl,* Art 85-87 para. 12.

would be a clear indication in favour of or against a particular interpretation. It is therefore necessary to await clarification of this controversial issue by the ECJ. For the time being, it is recommended to assume the applicability of Art. 86 AI Act in case of doubt.

Notwithstanding these questions of demarcation raised at the beginning, there are certain cases in which the applicability of Art. 22 in conjunction with Art. 15(1)(h) GDPR is excluded and thus Art. 86 AI Act applies, provided that the other requirements set forth by this provision are met. On the one hand, this is the case when a decision is made based on the output of an AI system without processing personal data. In these cases, the GDPR generally does not apply. This may be the case, for example, if the data processing is based on aggregated data that no longer include personal data.[347] Moreover, Art. 22(1) GDPR does not apply in situations where personal data is processed but the decision-making procedure is only partially automated, as Art. 22 GDPR requires "a decision based solely on automated processing". The case of the utilisation of fraud detection algorithms by public bodies that filter out a subset of individuals “suspected” of fraud, who will then be further investigated by human officials, serves as an example.[348] As explained above, in its recent “SCHUFA” judgment, the ECJ examined the distinction between solely automated and partially automated decisions in more detail and found that the decision-making procedure must be "significantly" influenced by the system in order to fall within the scope of Art. 22 GDPR. The ECJ in its ruling on the relevance of credit reference agencies:

"Article 22(1) [GDPR] [...] must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes ‘automated individual decision-making’ within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person."[349]

The output of the system must therefore significantly influence the decision, but not completely replace it. Even if this can lead to a combination of human and automated decision-making falling within the scope of Art. 22 (1) GDPR, there will still be some combinations that are not covered by Art. 22(1) GDPR and to which Art. 86 AI Act applies.

There are therefore constellations in which the right of access under the GDPR does not apply, but data subjects still need access to information about AI systems with which they come into contact. At this point, the relevance of Art. 86 AI Act comes to the fore again, as deployers must inform about the role of the AI system in the decision-making procedure in the explanation, which indicates that the right to explanation laid down in the AI Act applies to decisions in which AI systems are involved in different phases and functions, from supporting

---

[347] Cf. *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (as at 24 April 2024).

[348] Cf. *Kelder,* On the relative importance of the AI Act right to explanation, https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (as at 24 April 2024).

[349] ECJ 7. 12. 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, para. 75.

to fully determining. Consequently, Art. 86 AI Act may fill a considerable gap left by the GDPR.[350]

5.5.6 Challenges during implementation

Whilst the right to explanation is widely regarded as a right of affected persons, it also comprises an economic component, which should not be disregarded. It can happen for example that the right to explanation comes into conflict with the interests in protection of information holders, by jeopardising their trade secrets, particularly in the context of algorithms. This dynamic can, in turn, influence competition among companies that benefit from the secrecy of their algorithms. Consequently, the right to explanation might indirectly function as an instrument of competition law, as the disclosure of algorithms could reduce market imbalance.[351] This "trade-off" between the interests of the affected person and the organisation receiving the request for information has been interpreted, at least in relation to Art. 15 GDPR, in such a way that a refusal to provide all information on the grounds of trade or business secrets is contrary to Union law.[352] This can probably also be applied to the right to explanation under Art. 86 AI Act. Closely related to this is the competition between Art. 86 of the AI Act and copyright and patent law, to which computer programmes and software may be subject.[353]

The technical aspects associated with the right to explanation are no less challenging. When implementing this right, it is imperative to address the question of how specific machine learning processes and outcomes can be explained at all or how the decision-making procedure itself can be rendered more transparent.[354] Hence, it is almost impossible to obtain a comprehensive explanation of all parameters and processes. This may not be necessary, however, as affected persons are entitled to a clear and meaningful explanation that enables them to exercise their rights (Cf. Recital 171 AI Act). Consequently, the question of completeness does not arise, and overly complex explanations of numerous parameters and processes could even compromise comprehensibility. Therefore, the lack of a comprehensive XAI does not preclude affected persons from exercising their right to explanation.[355]

5.5.7 Information obligations under the AI Act

The AI Act contains more information obligations and transparency provisions that benefit affected persons. Firstly, the provisions in Art. 50 and Art. 26(7) and (11) should be mentioned

---

[350] Cf. *Kelder,* On the relative importance of the AI Act right to explanation (2024), https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/#:~:text=Following%20the%20trilateral%20negotiations%2C%20the,elements%20of%20the%20decision%20taken%E2%80%9D (as at 24 April 2024).

[351] Cf. *Hoffmann/Kevekordes,* The Right to Explanation, DuD 2021, 609 (613).

[352] ECJ 27 February 2025, C-203/22, *Dun & Bradstreet Austria*, ECLI:EU:C:2025:117, para. 70.

[353] Cf. *Hoffmann/Kevekordes,* DuD 2021, 609 (612).

[354] Cf. *Hoffmann/Kevekordes,* DuD 2021, 609 (614).

[355] Cf. *Hoffmann/Kevekordes,* DuD 2021, 609 (615).

particularly in this regard.

Article 50 stipulates transparency requirements in connection with certain AI systems (**not necessarily high-risk systems**). For example, providers must in principle "ensure that AI systems intended 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" (paragraph 1). Furthermore, e.g. systems that generate deep fakes and emotion recognition systems (see already Section 5.3.4) are addressed. In this context, also Art. 50 (6) AI Act is to be mentioned, according to which the obligations set out in Chapter III (which also includes Art. 86) and other transparency obligations under national or Union law (such as under the GDPR) remain unaffected by Art. 50 (1)-(4), from which it can be deduced that the transparency obligations under Art. 50 clearly apply alongside other Union acts and not subsidiarily.[356] This presumably is a difference between on the one hand Art. 50 AI Act in conjunction with Arts 13 and 14 GDPR and on the other hand Art. 86 AI Act in conjunction with Arts 15 and 22 GDPR, as the question of subsidiarity seems clearer in this regard than with Art. 86.

By contrast, Art. 26 AI Act principally regulates the obligations of **deployers of high-risk AI systems**.[357] In this regard, paragraph 7 refers to employers as deployers of such systems. These are obliged to "inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system" before putting into service (see Art. 3(11) AI Act) or using the system at the workplace. Art. 26(11), on the other hand, refers to deployers of high-risk AI systems listed in Annex III "that make decisions or assist in making decisions related to natural persons" and obliges them (without prejudice to Art. 50) to inform these persons "that they are subject to the use of the high-risk AI system". In principle, information on automated decision-making, including profiling, must also be provided in accordance with the information obligations under Arts 13 and 14 GDPR[358], meaning that in such cases pursuant to Art. 22(1) and (4) GDPR "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" must be provided (Art. 13(2)(f) and 14(2)(g); see also Sections 5.4.2 and 5.4.3). In addition, Art. 26(11) AI Act refers to the information obligations pursuant to Art. 13 LED. The right to explanation pursuant to Art. 86 AI Act is not explicitly mentioned in Art. 26(11) AI Act but is addressed in Rec. 93. Accordingly, the "information should include the intended purpose and the type of decisions it makes. The deployer should also inform the natural persons about their right to an explanation provided under this Regulation". Therefore, a broad interpretation of Art. 26(11) AI Act is recommendable, which also includes the obligation of deployers to inform in advance about the right to explanation pursuant to Art. 86 AI Act.[359] However, it remains unclear in what form or at what point and in particular at what time data

---

[356] Cf. *Martini* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art. 50 paras 123, 124.

[357] Cf. *Eisenberger* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art. 26 para. 1.

[358] See in this regard fundamentally *Illibauer* in *Knyrim*, DatKomm Art. 13 DSGVO paras 54 et seq. with further references, in particular also the ECJ case law on the *Schufa* case; *Illibauer* in *Knyrim*, DatKomm Art. 14 DSGVO para. 33.

[359] Cf. *Hartmann* in *Martini/Wendehorst,* KI-VO Art. 86 para. 5.

subjects are to be informed of the right under Art. 86 AI Act. Regarding the placement of the information, it is firstly advisable to inform affected persons of their rights directly in the notice concerning the decision, but also to use other channels - preferably in parallel - to ensure the greatest possible transparency, such as the company website, the privacy policy or printed brochures. With regard to the timing of the information, it will probably have to be assumed based on the purpose of the provisions that the information must be provided before, respectively at the time of the corresponding use of the AI system. On the one hand, this can be inferred from the principle of efficiency (*effet utile*), as the right to explanation under Art. 86 AI Act is more likely to have an optimal effect if information about its existence is provided as early as possible. Furthermore, this arises from fundamental rights considerations and the right of self-determination of the affected persons not to be subject to a high-risk AI-based decision and therefore to be able to take respective measures in good time. In any case, information about the possibility of asserting the right to explanation must be provided in the notice concerning the decision itself at the latest.

In addition, it is conceivable that the processing of the data, respectively the use of the high-risk AI system, which serves as the basis for the decision, and the decision itself could be significantly separated in time. An illustration of this phenomenon can be observed in customer interactions with a company's service hotline, wherein subsequent utilisation of emotion recognition systems classified as high-risk AI systems occurs for the general analysis of customer satisfaction. This might occur without concrete decisions about the future course of action with regard to the respective customers being planned at this stage. If, consequently, considerably later, the decision is made that the contracts of those customers who have been classified as "very dissatisfied" by the AI-supported system are to be terminated, the question arises as to when these customers are to be informed about the right under Art 86 AI Act, as the AI Act does not address this issue. It can be assumed that the use of the high-risk AI system, respectively the processing of customer data, already represents "preliminary decisions" on the basis of which the "main decision" is ultimately made. For example, in the ECJ’s SCHUFA ruling, the calculation of a "credit score", on which the decision on a person's creditworthiness is largely based, was categorised as a preliminary decision, which already significantly prepares the main decision with regard to creditworthiness.[360] Furthermore, it can be assumed that companies use this form of AI applications precisely for the purpose of making a decision subsequently based on the data generated in this way, which in any case has an impact on the persons concerned – be it the placement of personalised advertising, price adjustments for life and health insurance or credit checks. It is therefore advisable to **inform customers at the time of data collection or the use of the AI** that high-risk AI systems are being used and that decisions are being made with their support that may affect customers.

Of course, it can be argued that at the time of AI deployment, there is no intention at all to use its output as the basis for a specific decision. However, this case is somewhat unrealistic, as such systems are presumably used for the main purpose of supporting decisions. Furthermore, it will presumably prove extremely difficult in practice to determine when a company specifically intends to make a decision based on an AI output. It is therefore recommendable, in case of

---

[360] ECJ 7 December 2023, C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957, paras 44 et seq.

doubt, to provide information about the existence of the right to explanation under Art. 86 AI Act as early and comprehensively as possible. This also results from the fact that, in accordance with Art. 26(11) AI Act, information must already be provided at the time of the basic usage of a corresponding high-risk AI system. Thus, information on the right to explanation under Art. 86 AI Act, which would be applicable in the event of a future AI-based decision, should also be transmitted here.

This information should be disclosed as transparently as possible and, if possible, through various channels. In the case of AI-supported analysis of customer conversations with a company's service hotline, affected persons could be informed of this right at the beginning of the conversation or via an automated audio tape before connecting with the customer service representative. It is also conceivable to inform customers about individual aspects of the AI-supported decision in various stages. First, the use of the high-risk AI system itself could be disclosed and it could be pointed out that there is a possibility that the output generated by the system will be used as a basis for a certain category of decisions in the future (including the intended purpose and type of the decisions within the meaning of Rec. 93 AI Act) and the extent to which affected persons are entitled to the right to explanation under Art. 86 AI Act in such cases. Even though not explicitly stipulated by law, this should include negative information, i.e. the reference that no decisions are made based on the AI system's output. If a concrete decision is ultimately made, the entitlements under Art. 86 AI Act could be explained separately again and the required information be set out in detail.

Example

If, for example, a decision is made on a premium adjustment for life insurance using a high-risk AI system, the deployer should inform the affected person already at the time the AI system is used that a high-risk AI system is supporting the calculation of the premium and that a decision on a premium adjustment can be made on the basis of this calculation. It is also advisable to make affected persons aware of the right under Art. 86 AI Act again in the actual communication about the contract adjustment.

If the decision is made digitally, for example on online portals through personalised advertising, the information could be displayed immediately after the notice concerning the decision in the form of a hyperlink.

It is generally advisable to provide information about the right under Article 86 of the AI Act well in advance of the actual decision, for example by referring to high-risk AI-based decisions in the respective data protection policy, in any transparency reports, in the FAQ section on the company website or in information brochures in the company’s outlets.

Apart from the obligations mentioned above, other provisions of the AI Act can also benefit transparency towards affected persons, which is why it is advisable to include this information in the explanation. In this context, e.g. the registration obligations pursuant to Art. 49 AI Act are to be mentioned, which oblige certain actors to register various aspects in connection with high-risk AI systems in the EU database pursuant to Art. 71. This e.g. concerns summaries with regard to impact assessments in connection with certain systems that must be registered by certain deployers.[361] The correspondingly registered information contained in the database shall in principle be "accessible and publicly available in a user-friendly manner" (see in detail, in particular on exceptions, Art. 71(4) AI Act). Furthermore, according to Art. 85, in principle "any natural or legal person having grounds to consider that there has been an infringement of the provisions of this Regulation may submit complaints to the relevant market surveillance authority". As of February 2025, no specific Austrian authority has been designated as the competent market surveillance authority and the designation must be made by 2 August 2025. However, as of 2 November 2024, public authorities and bodies in the area of fundamental rights have been given more powers in relation to AI (cf. 77(2) AI Act). These are responsible for supervising and enforcing compliance with obligations under Union law protecting fundamental rights in relation to the high-risk AI systems listed in Annex III (Art. 77(1) AI Act). In this regard, the competent market surveillance authority has comprehensive cooperation obligations with the public authorities and bodies mentioned.[362] Accordingly, the competent market surveillance authority must inform the above-mentioned institutions of serious fundamental rights incidents in connection with high-risk AI systems and also in case it has identified that an AI system poses a risk to fundamental rights (Art. 73(7) and Art. 79(2) AI Act). If, in the course of an evaluation, the market surveillance authority finds that a high-risk AI system, despite its compliance with the AI Act, presents a risk to the health or safety of persons, to fundamental rights, or to other aspects of public interest protection, it has to request the relevant operator to take all appropriate measures to eliminate this risk without undue delay. The competent market surveillance authority must consult the above-mentioned institutions in connection with this evaluation (Art. 82(1) AI Act).

---

[361] See in detail Art. 49(3) and Annex VIII Section C AI Act as well as e.g. *Fülöp/Poindl* in *Pehlivan/Forgó/Valcke*, AI Act Art 27 section 3.3.2 and 3.3.5.

[362] More details at: https://www.digitalaustria.gv.at/Themen/KI/Artikel-77-AI-Act.html.

5.6 Sanctions and compensation

The AI Act contains penalty provisions in Articles 99 et seq. under the title "Penalties" (Chapter XII), which in principle also address deployers of AI (Art. 99(4)(e) e.g. addresses the obligations pursuant to Art. 26). However, Art. 99 in principle lists certain obligations and does not generally penalise every violation of the Regulation. No reference is made to Article 86 there, also not by way of the deployers' obligations pursuant to Art. 26 AI Act. However, penalties would accordingly at least cover the aspect of the obligation to provide information pursuant to Art. 26(11) AI Act described in Section 5.5.7 that refers to the right pursuant to Art. 86. Moreover, the transparency obligations for deployers pursuant to Art. 50 AI Act are also subject to penalties (Art. 99(4)(g)). This only appears to be fundamentally different in relation to Union institutions, bodies, offices and agencies, where, apart from the violation of the prohibition of certain practices pursuant to Art. 5 AI Act, "non-compliance of the AI system with any requirements or obligations under this Regulation" other than that can also be sanctioned (Art. 100(2) and (3) AI Act).[363] In addition, each Member State shall adopt specific rules "on to what extent administrative fines may be imposed on public authorities and bodies established in that Member State" (Art. 99(8) AI Act).

It should furthermore be noted that pursuant to Art. 83(5) GDPR the national supervisory authority can also impose sanctions in the event of an infringement of the obligation to provide information regarding automated decisions pursuant to Art. 15(1)(h) in conjunction with Art. 22 GDPR.[364]

At present, it is still questionable to a certain degree to what extent at least some provisions of the AI Act, such as Art. 86, constitute protective laws [Schutzgesetze] within the meaning of Article 1311 Austrian Civil Code [§ 1311 ABGB] (i.e. specific legal provisions prohibiting a certain behaviour already because of its abstract dangerousness) and thus enable those affected to claim compensation for damages on this basis against persons who infringe them – of course, albeit taking into account all (other) requirements.[365] In the context of AI, infringements of protective laws [Schutzgesetze] are generally of particular importance as a basis for **tortious** [deliktische] **compensation claims for damages**, because the damages to be expected will often not concern absolutely protected legal interests [absolut geschützte Rechtsgüter] (which would also be a possibility as a basis for tortious [deliktische] compensation claims for damages). Yet, in connection with infringements of protective laws [Schutzgesetze], such other damages may under certain circumstances also be eligible for compensation.[366]

In this context it should be emphasised that under Austrian law compensation claims for

---

[363] Cf. *Anderl/Ciarnau* in *Zankl*, KI-VO (2025) Art. 100 para. 3.

[364] The following paragraphs refer to the Austrian legal situation and are to be considered correspondingly.

[365] Cf. *Karner* in *Bydlinski/Perner/Spitzer*, KBB. ABGB. Kommentar zum ABGB^7 (2023) § 1294 ABGB paras 1, 4, § 1311 ABGB para. 3 with further references; see fundamentally furthermore RIS-Justiz RS0027415 and, on Union law in this context, cf. e.g. OGH [Austrian Supreme Court] 2 August 2012, 4 Ob 46/12m; furthermore, it should e.g. be considered, whether there is a damage eligible for compensation, cf. concerning this, in particular in connection with *protective laws* (*Schutzgesetze*), for example: *Karner* in *Bydlinski/Perner/Spitzer,* KBB^7 § 1295 ABGB para. 2 with further references.

[366] Cf. *Wendehorst* in *Martini/Wendehorst,* KI-VO Art. 1 paras 78 et seq.

damages generally require a certain connection between the protective purpose of the violated norm and the claimed damage. Such liability for damages is only applicable if the violated norm was intended to prevent this very damage (which is of practical relevance in connection with infringements of protective laws [Schutzgesetze]).[367] This purpose of the relevant norms must be determined through teleological interpretation.[368] On the other hand, it is also essential in the given context, that the AI Act does not contain an individual liability provision, such as e.g. Art. 82 GDPR.[369] By contrast, Art. 82 GDPR establishes an independent direct tortious [deliktische] liability for the processing of personal data violating the GDPR.[370] In this context, *Wendehorst* states that other product safety regulations are often generally qualified as *protective* laws [Schutzgesetze] and that this will presumably apply to at least some provisions of the AI Act.[371] With regard to this, firstly it should be noted that a general purpose of the AI Act pursuant to Art. 1(1) is "ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, [...] against the harmful effects of AI systems", which suggests a corresponding notion of protection with regard to affected persons. However, it might be necessary to differentiate in detail with regard to the exact objective of individual provisions. This also follows e.g. from the AI Liability Directive (AILD), which was originally proposed as a kind of package together with the proposal for the AI Act.[372] This Directive was intended to provide for certain alleviations of the burden of proof quasi supplementing the non-contractual, fault-based, civil liability regulated by national or (other) EU legislation, which would nevertheless continue to apply.[373] In this proposal, the EU Commission appears to interpret (at least in part) only some obligations of the (proposed) AI Act as a "duty of care [...] directly intended to protect against the damage that occurred"[374], which results from a synopsis of the following:

According to the proposed text, in principle only non-compliance with duties of care "directly intended to protect against the damage that occurred" were to be considered relevant for triggering the presumption of causality proposed therein (of course besides other requirements).[375] Furthermore, concerning high-risk AI systems subject to certain requirements laid down in the (proposed) AI Act, at least with regard to their providers or persons subject to provider's obligations, only certain, exhaustively (argumento: "only") listed

---

[367] Cf. *Karner* in *Bydlinski/Perner/Spitzer,* KBB^7 § 1295 ABGB para. 9, § 1311 ABGB para. 5 with further references.

[368] Cf. *Karner* in *Bydlinski/Perner/Spitzer,* KBB^7 § 1295 ABGB para. 9.

[369] Cf. also *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art. 1 para. 61; on the lack of specific individual liability provisions in the proposal for the AI Act and on corresponding liability considerations from a German perspective, cf. also *Dötsch*, Außervertragliche Haftung für Künstliche Intelligenz am Beispiel von autonomen Systemen (2022) 400, 401.

[370] Cf. *Schweiger* in *Knyrim*, Der DatKomm. Praxiskommentar zum Datenschutzrecht Art. 82 DSGVO paras 1, 38 (as at 1 December 2021, rdb.at).

[371] Cf. *Wendehorst* in *Martini/Wendehorst,* KI-VO Art. 1 paras 84, 85.

[372] However, the AILD proposal has not yet been adopted (as at February 2025) and has apparently even been withdrawn by the EU Commission (for more information, cf.: https://commission.europa.eu/document/download/7617998c-86e6-4a74-b33c-249e8a7938cd_en?filename=COM_2025_45_1_annexes_EN.pdf).

[373] Cf. Proposal for a Directive of the European Parliament and of the Council adapting the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive [AILD]), COM(2022) 496 final; on liability in connection with artificial intelligence, see also the explanatory memorandum in the margin: Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.

[374] Cf. Art. 4(1)(a) AILD proposal.

[375] Cf. Rec. 22 and Art. 4(1)(a) AILD proposal.

requirements under the (proposed) AI Act () were considered to be relevant.[376] Rec. 22 of the proposed AILD also explicitly mentioned regulatory requirements that were not supposed to protect against corresponding damage (which was presumably particularly intended for the proposed AI Act[377]), by stating that "[n]on-compliance with duties of care that were not directly intended to protect against the damage that occurred do not lead to the application of the presumption, for example a provider's failure to file required documentation with competent authorities would not lead to the application of the presumption in claims for damages due to physical injury"[378].[379]

However, in this regard, also liability scenarios based on Art. 82 GDPR should be emphasised again, as it is argued here that although it would be required that the processing of personal data gives rise to the damage (and not e.g. merely a breach of information obligations under Chapter III GDPR), it would not be necessary that quasi the specific provision violated would per se be intended to protect the injured parties, because the GDPR as a whole would aim to protect the rights and freedoms of data subjects.[380] In principle, this could accordingly also be argued in a similar way with regard to the AI Act[381], although it is to be noted that Art. 82 GDPR in a way simply constitutes an independent regime (see already above).

However, Article 86 AI Act in particular appears to be aimed at protecting those affected, namely especially regarding their information,[382] and could therefore to some extent also be aimed at preventing corresponding damage. Furthermore, this provision was not included in the Commission's original proposal for the AI Act, which after all was significant in connection with the proposal for the AILD, and therefore it is likely that it had not been taken into account therein.[383] Apart from that, the information obligation pursuant to Art. 26(11) AI Act is

---

[376] Cf. Rec. 26 and Art. 4(2) AILD proposal; with regard to users (now principally: deployers) of corresponding high-risk AI, on the other hand, the respective provision (Art. 4(3) AILD Proposal) was not so clear as to the extent to which the corresponding list of requirements under the proposed AI Act, of which a breach would be relevant for the presumption of causality, was supposed to be exhaustive, in particular because no "only" (or a similar clarification) was used therein; however, if the Recitals (in particular 24 and 26) of the AILD proposal are used for interpretation, this legislative proposal was probably to be understood to mean that, besides the listed requirements under the proposed AI Act , "other duties of care laid down in Union or national law" would in principle also have been relevant for such users. Conversely, with regard to the proposed AI Act only those listed apply (cf. Rec. 26 AILD Proposal, which, inter alia, states that the Directive was supposed to cover the fault of such users if "this fault consists in non-compliance with **certain specific requirements**" under the AI Act (proposal); emphasis added).

[377] This is because immediately prior to this, non-compliance with instructions of use (cf. concerning this particularly Arts 13 and 29(1) of the AI Act proposal; now in principle Arts 13 and 26 (1) AI Act) was considered potentially relevant: "Thus, this presumption can apply, for example, in a claim for damages for physical injury when the court establishes the fault of the defendant for non-complying with the instructions of use which are meant to prevent harm to natural persons."; This finally was also reflected in Art 4(3)(a) AILD proposal.

[378] Cf. concerning this e.g. the obligations to provide documentation already in Art. 23 AI Act Proposal (now in principle Art. 21 AI Act); cf. in this context, however, also Rec. 25 AILD proposal, which stated that a breach of requirements to submit documents or to register with authorities "could not be considered as reasonably likely to have influenced the output produced by the AI system or the failure of the AI system to produce an output", which was presumably additionally aimed at the requirement pursuant to Art. 4(1)(b) AILD proposal.

[379] Cf., similarly with regard to the nature of AI Act provisions as protective laws [Schutzgesetze], again: *Wendehorst* in *Martini/Wendehorst,* KI-VO Art. 1 para. 84, 85.

[380] Cf. *Schweiger* in *Knyrim*, DatKomm Art. 82 DSGVO para. 38.

[381] See for the general objective of the AI Act, in particular pursuant to Art. 1(1), already above.

[382] Cf. in this context, besides the text of Art. 86 AI Act, in particular Rec. 171 AI Act and concerning this also *Hartmann* in *Martini/Wendehorst,* KI-VO Art. 86 paras 1, 2; cf. also Rec. 93 AI Act, especially in connection with the corresponding information of affected persons.

[383] Cf. the comments above and also the fundamental explanations in the explanatory memorandum to the AILD

presumably also related to the (fundamental rights) protection of affected persons (cf. Rec. 93 AI Act).

In connection with AI of course also contractual compensation claims for damages can be relevant, besides tortious [deliktische] compensation claims for damages, respectively in particular regarding infringements of protective laws [Schutzgesetze]. .[384]

Finally, it should also be mentioned that the AI Act has been included in Annex I of the Representative Actions Directive[385] (Art. 110 AI Act). This directive refers to "representative actions brought against infringements by traders of the provisions of Union law referred to in Annex I, including such provisions as transposed into national law, that harm or may harm the collective interests of consumers" (Art. 2(1) Representative Actions Directive). In this context, it is noted on the one hand that the right pursuant to Art. 86 of the AI Act would have a special suitability for collective redress and, on the other hand, that compensation actions for damages based on infringements of protective laws [Schutzgesetze] would have presumably the highest economic relevance.[386]

---

proposal.

[384] See in this regard in detail *Wendehorst* in *Martini/Wendehorst,* KI-VO Art. 1 paras 90 et seq.

[385] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ L 2020/409, 1.

[386] See in total in detail *Wendehorst* in *Martini/Wendehorst*, KI-VO. Verordnung über Künstliche Intelligenz. Kommentar (2024) Art. 110 paras 1 et seq.

5.7 Comparison and subsumption of the practical examples under the legal provisions

The previous explanations have shown that a joint consideration of the aspects of data protection law and Art. 86 AI Act is necessary in order to approach a clarification of the partially unresolved issues surrounding the right to explanation in connection with AI-supported decision-making procedures. Even if the lack of practice with the AI Act means that it will be necessary to await supreme court rulings with regard to some unresolved aspects of Art. 86 AI Act, valuable conclusions can already be drawn by analysing the data protection literature and case law, and many questions can thereby be answered. However, it should be emphasised that the practical examples used only represent a part of the possible applications of Art. 86 AI Act and that their legal analysis may also differ depending on their specific variation. Furthermore, the publication of in-depth literature and the interpretation of Art. 86 AI Act by jurisprudence will also contribute to sharpening the legal subsumption and clarify some partially (still) contentious issues. The analysis should therefore by no means be regarded as conclusive or even legally binding but represents a first approximation of the practical implications of the right to explanation under Art. 86 AI Act, whereby partially other conclusions are conceivable as well depending on the chosen line of argumentation or interpretation. With regard to the selected use cases, therefore the picture summarised below emerges. The following use cases were considered in this regard:

- **Use Case 1:** Pricing of life and health insurance
- **Use Case 2:** Churn Prediction
- **Use Case 3:** Credit Scoring
- **Use Case 4:** Emotion recognition in marketing and sales promotion
    - **Use Case 4.1:** Use of gesture recognition to determine reactions in sports betting advertising to increase efficiency
    - **Use Case 4.2:** Use of emotion recognition based on images of the facial area as part of identity verification (e.g. for flight bookings), whereby identified emotions are reacted to accordingly (e.g. by lowering prices) in order to increase the probability of a purchase
    - **Use Case 4.3:** Use of emotion recognition in marketing for goods or services to recognise in how far these could be adapted (for example to increase customer satisfaction), e.g. in the form of adapting travel offers based on emotional reactions to corresponding advertising videos in order to better match potential individual preferences (**Use Case 4.3.a**) or inferring emotions on the basis of texts or audio files with voice recordings in order to analyse and react to the satisfaction of existing customers (**Use Case 4.3.b**)

5.7.1 Relevant provisions of the GDPR

The GDPR is applicable if personal data within the meaning of Art. 4(1) GDPR (e.g. name, address, gender, etc.) is processed, which essentially applies to all use cases, except where e.g. anonymous data are processed. With regard to the processing of special categories of personal data ("sensitive data") pursuant to Art. 9(1) GDPR, the situation is somewhat more differentiated depending on the use case, as it hinges on whether certain categories of data such as data concerning a person's origin, sex life, health or religion are processed. While this can easily be answered on a case-by-case basis with regard to use cases 1-3 and depends on exactly what data is being processed, this criterion is more difficult to assess for Use Case 4 on emotion recognition:

- Use Case 1: Sensitive data is processed if the decision on the health risk factors and subsequently on pricing is made on the basis of the processing of health data, which is very likely in this case.
- Use Case 2: Here it depends on the specific case, but there is a possibility of processing sensitive data if the probability of customer churn is derived from this data. However, this seems highly unlikely.
- Use Case 3: Here, too, it depends on the specific case constellation, but there is a possibility of processing sensitive data if the creditworthiness or credit score is derived from this data.
- Use Case 4: Emotion recognition regularly goes hand in hand with the processing of biometric data, whereby, with reference to the discussion in Section 5.3.4, it is important to consider how the term "biometric data" is to be interpreted and whether emotion recognition involves biometric data as understood by the GDPR - in contrast to the AI Act - that allow or confirm the unique identification of data subjects. In this case sensitive data within the meaning of the GDPR would be involved.
    - Use Case 4.1: If biometric data is processed that allows or confirms the unique identification of the data subject, this must be affirmed from a GDPR perspective. In this sub-case, however, the processing of biometric data within the meaning of the GDPR is rather to be negated.
    - Use Case 4.2: If biometric data is processed that allows or confirms the unique identification of the data subject, this must be affirmed from a GDPR perspective. In this sub-case, biometric data within the meaning of the GDPR will presumably be involved.
    - Use Cases 4.3.a and 4.3.b: If biometric data is processed that allows or confirms the unique identification of the data subject, this must be affirmed from a GDPR perspective. In these Use Cases, however, the processing of biometric data within the meaning of the GDPR is not mandatory.

The next step is to analyse the extent to which the individual use cases fall within the scope of Art. 22 GDPR, which subsequently determines whether the right to access pursuant to Art. 15

(1)(h) GDPR applies. Art. 22 GDPR requires that a decision based on automated processing - including profiling - is made which produces legal effects concerning the data subject or similarly significantly affects the data subject. In most cases, this also applies to all use cases, whereby it depends on the fulfilment of the specific criteria in the different constellations whether Art. 22 GDPR applies.

- Use Case 1: Art. 22 GDPR is applicable, as automated profiling is conducted here, on the basis of which a decision on pricing is made. Furthermore, the decision to adjust the price based on profiling has an effect on the data subject, namely on the one hand on their financial situation and on the other hand in the broadest sense on their access to healthcare services. In case the decision to adjust the price is furthermore accompanied by the establishment, termination or adaptation of a contractual relationship, a legal effect is to be assumed anyway.
- Use Case 2: Here it depends on the specific case. It applies if profiling of individual persons is conducted, on the basis of which profiles are created which serve for selecting customers at risk of churning and consequently for taking targeted preventive measures for them.
- Use case 3: Art. 22 GDPR also applies here, as the term "decision" is to be interpreted broadly including preliminary decisions, such as the calculation of a score value, if these have a significant influence on the decision-making process. The effect then lies in the decision to grant a loan or to conclude a contract with the data subject.
- Use case 4: In the case of emotion recognition, it principally can be assumed that a decision is made based on automated data processing. Regarding the criterion of the effect of the respective decision, the question is to what extent the decision has a legal effect or significantly affects the data subject in a similar way.
    - Use case 4.1: Particularly personalised advertising for sports betting that addresses and exploits the vulnerabilities of affected persons, such as targeted advertising for sports betting to persons with gambling addiction, must in any case be considered as a corresponding impairment.
    - Use case 4.2: Here, it will have to be examined on a case-by-case basis whether financial health or private life are affected sufficiently.
    - Use cases 4.3.a and 4.3.b: The use of emotion recognition in advertising to adapt products and services can presumably not yet be considered to affect persons significantly (Use case 4.3.a). However, if emotion recognition is used to analyse customer satisfaction, provided that a decision e.g. on the termination of a contractual relationship is linked toit, a legal effect can be assumed (Use case 4.3.b).

Where Art. 22 GDPR applies, data subjects have the right to obtain from the controller meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing. Irrespective of this, the data controller is obliged in all cases to provide information in advance in accordance with Art. 13, respectively 14 GDPR, address transparency towards data subjects. Accordingly, the controller must provide certain information (contact details of the controller, the purposes of processing, the legal basis for the data processing, etc.) at the time of data collection.

5.7.2 Art. 86 AI Act and related provisions

The AI Act is applicable if an AI system pursuant to Art. 3(1) AI Act is involved. It will have to be examined on a case-by-case basis whether the specific system used by a company fulfils these requirements, but it can be assumed that this will regularly have to be affirmed in the case in the selected use cases.

In Use Case 4, the question must also be asked whether respective systems constitute an emotion recognition system pursuant to Art. 3(39) AI Act, which inter alia depends on whether the system processes biometric data within the meaning of Art. 3(34) AI Act (in particular data obtained by directly measuring biological signals relating to corresponding personal characteristics using special technical means and aimed at an emotion recognition purpose). This must be clarified in each individual use case, in particular based on the specific technical approach, but will often apply for Use Cases 4.1, 4.2 and 4.3.a. The fulfilment of this requirement is generally questionable only regarding Use Case 4.3.b, because in so far as only texts are used to infer emotions, no direct measurement of biological signals is usually involved. However, if, for example, keystrokes or gestures are analysed and emotions are inferred from them, this could again constitute emotion recognition pursuant to the AI Act. Particularly regarding Use Case 4.1, it is also necessary to check whether the system actually recognises emotional reactions based on gestures or whether merely other states or conditions (such as fatigue) are inferred. The first case would be an emotion recognition system within the meaning of the AI Act, but not the latter.

In principle, the use cases in question do not constitute prohibited practices within the meaning of Art 5 AI Act. However, depending on the specific structure of the cases, there is a possibility of an overlap with the prohibitions listed in Art 5 AI Act.

The next step is to check whether the AI systems used in the use cases constitute high-risk AI systems in accordance with Art. 6(2) in conjunction with Annex III AI Act, as Art. 86 AI Act only applies to these:

- Use Case 1: Yes, as the pricing of life and health insurance is explicitly categorised as high-risk in Annex III point (5)(c) AI Act.
- Use Case 2: In principle, this does not constitute a high-risk AI system, as it is not to be assigned to any of the areas listed in Annex III. However, if churn predictions are performed using other high-risk AI systems listed in Annex III, for example using emotion recognition systems, this would be a high-risk AI system.
- Use Case 3: Systems that are used to assess the creditworthiness or credit scoring of natural persons are considered high-risk within the meaning of Annex III point (5)(b) AI Act, with the exception of AI systems for the detection of financial fraud.
- Use Case 4: Here, where emotion recognition systems within the meaning of the AI Act

are used, in particular Use Case 4.1 and Use Case 4.2 can be categorised as high-risk in accordance with Annex III point (1)(c) AI Act, unless already prohibited pursuant to Art. 5(1)(a) or (b) AI Act. In principle, this also applies to Use Case 4.3, unless an exception under Art. 6(3)(b) AI Act applies (in the sense of the improvement of completed services). In Use case 4.3.a, however, the classification as high-risk AI system will have to be negated in general because corresponding offers are already adapted/improved in advance. This would be similar in Use case 4.3.b, if e.g. offers would be directly adapted as a reaction to any dissatisfaction.

In order for Art. 86 AI Act to apply, the deployer must also make a decision based on the output of the high-risk AI system. The deployer is the organisation or company that uses the AI system under its own authority in the course of its professional activities. In Use Case 1, for example, this would be the insurance company or, in Use Case 4.3.b, the company that uses emotion recognition AI to analyse audio recordings of customer conversations in order to assess customer satisfaction and then takes corresponding measures concerning customers who are classified as dissatisfied, such as the termination of respective contracts. The actual decision is to be interpreted broadly here and ranges from "preliminary decisions" (e.g. calculation of a score value) to price adjustments and general measures (e.g. advertising campaigns, the submission of service offers, etc.). In this regard, it is crucial that the output of the AI system was relevant for the decision and did not play a merely subordinate role. All these requirements principally regularly apply to the use cases.

In a next step, the decision must produce legal effects on the affected person or significantly affect them in a similar way, namely in their health, safety or fundamental rights. This means that the right to explanation does not apply if the decision taken on the basis of the system does not significantly affect the persons concerned.

- Use Case 1: This requirement is controversial in this use case, as the decision regarding the pricing of life and health insurance represents a financial disadvantage that is not considered a legal effect and it is questionable whether it constitutes an impairment of fundamental rights. However, it is reasonable to argue that certain financial disadvantages (e.g. significantly excessive insurance premiums) also constitute an impairment of fundamental rights. In addition, the amount of the insurance premium affects health in the broadest sense, as it affects access to healthcare services, which is why a relevant impairment can also be assumed here. Insofar as the establishment, cancellation or adjustment of a contractual relationship is concerned, this represents an effect on the legal position of the affected person and therefore a legal effect in any event.
- Use Case 3: The decision to grant a loan or conclude a contract (e.g. mobile phone or energy supply contract) concerns the establishment of a legal position in any case and therefore represents a legal effect. Furthermore, in most cases it will be a relevant impairment, as this decision affects the financial position and the general life situation of the affected person.
- Use Case 4: The general principle here is that it depends on the intensity of the advertising campaigns and whether the advertising is displayed across multiple devices

and leads to unreasonable harassment of the affected person in the form of "retargeting". This will e.g. not be the case if only generic advertising from a well-known online fashion retailer based on a simple demographic profile is displayed on a website, or if emotion recognition is used for future adjustments of products and services (Use Case 4.3). However, discriminatory advertisements, personalised price offers or advertisements that specifically address and exploit the vulnerabilities of affected persons, such as advertisements for sports betting aimed at gambling addicted persons (Use Case 4.1), can be seen as relevant impairments. It would be equally pertinent for Art. 86 AI Act if emotion recognition is used to analyse customer satisfaction linked to a decision to terminate the contractual relationship as this would represent a legal effect (Use Case 4.3.b). As already discussed, it is disputed whether purely financial disadvantages are considered a relevant impairment if they are not already covered in the form of legal effects. In these cases, the extent of the disadvantage will be decisive. For example, if in Use Case 4.2 price adjustment based on emotion recognition is performed, it will have to be examined on a case-by-case basis taking into account the perspective of the affected person regarding a sufficient degree of impairment of financial health or private life.

Insofar as Art. 86 AI Act is applicable, affected persons have the right to obtain a clear and meaningful explanation of the role of the AI system in the decision-making procedure and the most important elements of the decision taken. Information on this right must be provided in advance. Also, in case high-risk AI is used for decision-making or in case an emotion recognition system is used, corresponding information must be provided.

5.7.3 Table summarising the classification of the use cases

		Use Case 1	Use Case 2	Use Case 3	Use Case 4		
					Use Case 4.1	**Use Case 4.2**	**Use Case 4.3.a and 4.3.b**
GDPR	**Personal data**	In principle yes (this is assumed subsequently)					
	"Sensitive" data pursuant to Art. 9(1) GDPR	Yes	Rather no	Depends on the individual case	Rather no	Regularly yes	Rather no
	Scope of Art. 22 GDPR	Yes	Yes (if profiling of individual persons takes place)	Yes	Rather yes, in case of automated decision-making	Disputable (to be examined on a case-by-case basis)	Use Case 4.3.a rather no (no relevant impairment); Use Case 4.3.b rather yes
	Art. 15(1)(h) GDPR	Yes	Yes, in the case of profiling and thus fulfilment of Art. 22	Yes	Yes, if Art. 22 GDPR is fulfilled	Depending on whether Art. 22 GDPR is fulfilled	Yes, if Art. 22 GDPR is fulfilled (Use Case 4.3.a rather no; Use Case 4.3.b rather yes)
	Information obligations according to Arts 13/14	Yes					

		Use Case 1	Use Case 2	Use Case 3	Use Case 4		
					Use Case 4.1	Use Case 4.2	Use Cases 4.3.a and 4.3.b
AI Act	**AI system**	Regularly yes					
	Emotion recognition system (ERS)				Must be examined on a case-by-case basis, regularly representing an ERS as defined by the AI Act if emotional reactions are inferred from gestures.	Must be examined on a case-by-case basis, regularly representing an ERS as defined by the AI Act	Must be examined on a case-by-case basis, ERS as defined by the AI Act questionable in 4.3.b, presumably clearer in 4.3.a
	Prohibited system under Art. 5 AI Act	No	No	Principally no	Particularly possibly prohibited practice under Art. 5(1)(b) AI Act	Principally no	Principally no
	High-risk AI system	Yes	No (except in combination with ERS or other high-risk AI)	Yes	Yes	Yes	Tendentially yes; possibly exception pursuant to Art. 6(3)(b) AI Act relevant
	Legal effect or similarly significantly affecting persons	Yes	-	Yes	Particularly in case of advertisements for sports betting aimed at gambling addicted persons, yes	To be examined on a case-by-case basis if relevant impairment is constituted	Rather no in relation to 4.3.a; e.g. in case of termination of contracts, yes in relation to 4.3.b
	Further pre-information obligations	Information on the use of high-risk AI for decision-making and the existence of the right under Art. 86 AI Act					
					Providing information on the use of an ERS to affected persons at the latest at the time of the first interaction or exposure		

6 Social science aspects

Adopting a social science perspective on the right to access and the associated AI-specific challenges allows us to look beyond the purely legal requirements presented so far. This is essential as it provides insights into why the right to access is sometimes not complied with in practice, which in turn facilitates drawing conclusions regarding Art. 86 AI Act and its practical enforceability. Closely related to this is the aforementioned problem of the so-called “automation bias”, which describes the tendency of persons involved in AI-supported decisions to rely excessively on automated decision-making systems without subjecting them to rigorous scrutiny. This too provides valuable insights for the practical application of the right to explanation and measures to be taken.

6.1 Access

Our research shows that the right to access under data protection law has recently been the subject of several empirical studies. A meta-analysis conducted by *Habu & Henderson* (2023), for instance, demonstrates a substantial increase in research activities concerning this subject since 2013. In fact, the right to access appears to be the most extensively researched right of the persons affected.[387]

The right to access is generally regarded as a "central right of data subjects".[388] From a legal standpoint, its distinctive status is predicated on the fact that it is explicitly guaranteed at a constitutional level via Art. 8(2) CFR.[389] From a teleological point of view, the significance (or purpose) of the right is primarily that in many cases it is the only factor that facilitates the enforcement of other data subject rights (such as the right to rectification pursuant to Art. 16 GDPR, the right to erasure pursuant to Art. 17 GDPR or the right to object pursuant to Art. 21 GDPR). In this way, the right of access also serves to disclose or identify automated decision-making processes or unlawful data processing practices in the first place.

As part of the European research project IRISS (Increasing Resilience in Surveillance Societies)[390], a systematic investigation into the practical exercise and enforcement of the right to access was carried out between 2012 and 2015 under the direction of British criminologist *Clive Norris*.[391] The study covers a total of ten European countries,[392] whereby over 300 public and private organisations and 184 responses to requests for information were examined in detail. With regard to information on automated decision-making processes, it is reported that

---

[387] *Habu/Tristan*, Data subject rights as a research methodology, Journal of Responsible Technology 2023, 100070.

[388] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung/BDSG^2 Art 15 DSGVO 419.

[389] *Bäcker* in *Kühling/Buchner,* Datenschutz-Grundverordnung^2 Art 15 DSGVO 419.

[390] *European Commission*, Increasing Resilience in Surveillance Societies, https://cordis.europa.eu/project/id/290492/reporting (last access: 14 February 2025).

[391] *Norris/L'Hoiry/Galetta/Hert/Szekely/Raab*, Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform, https://www.statewatch.org/media/documents/news/2015/feb/iriss-policy-brief.pdf (as at 31 January 2015).

[392] This study was conducted in the following countries: Austria, Belgium, Germany, Hungary, Italy, Luxembourg, Norway, Slovakia, Spain and the UK.

in more than two thirds of cases (71%) this was either not provided at all or not provided in a legally compliant manner. Furthermore, more than a fifth (21%) of all cases in the sample had to be forwarded to the respective national data protection authorities due to the behaviour of the data controllers.[393]

In the context of Austria, reference may also be made to a qualitative study conducted by *Rothmann* (2017) on the processing of data via video surveillance.[394] A total of 29 requests for information were sent to various operators of such systems in 2013 and 2014, and their reactions and response behaviour were analysed. The study reveals various strategies used by those responsible, to reject the requests and refuse the right to access. These include missing contact details or contact persons, which make it difficult to make a request at all, as well as forms of rejection and denial of the legal claim. In some cases, references were made to controversial interpretations of data protection law, according to which for example the data subjects would have to provide a certificate of good conduct in order to receive information, or the information itself would in turn violate the rights of third parties and therefore could not be provided.[395] In only six cases did the controllers include the video footage in the provided information as required by law, and in just two cases was the data transmitted in full. Furthermore, the associated legal information (e.g. purpose, legal basis, recipients of the data) was only provided in 14 out of 29 requests. In only three cases was the information provided to the extent stipulated by law.[396] While empirical evidence in this area is described as highly situation-specific, an overall tendency of controllers to comply with the legal requirements only to a limited extent and to frequently attempt to evade accountability can be observed.[397]

In this context, reference can also be made to the study by *Wulf* and *Seizov* (2024), who also analysed the effectiveness of the right to access referring to Art. 15 and Art. 22 GDPR.[398] The researchers first conducted an online survey (n=835) of UK consumers in order to learn about the data subjects' expectations regarding the information about automated data processing and AI-based individual decisions.[399] The findings indicate that approximately half of the respondents neither know whether they have ever used an AI-based service (51%) nor whether they have ever been subject to an automated individual decision (56%). The survey also found that around 44% of respondents want to be informed about the actual use of an AI-based algorithm, as well as about the underlying logic and the personal data being processed. Another 15% go one step further and would like the "computer code" behind the algorithm to

---

[393] *Norris/L'Hoiry*, Exercising Citizen Rights Under Surveillance Regimes in Europe. Meta-analysis of a Ten Country Study, in *Norris/Hert/L'Hoiry/Galetta* (eds), The Unaccountable State of Surveillance. Law, Governance and Technology Series (2017) 405.

[394] *Rothmann,* Video Surveillance and the Right of Access. The empirical proof of panoptical asymmetries, Surveillance & Society 2017, 222; see also *Rothmann*, Videoüberwachung und Auskunftsrecht. An empirical analysis of visual claims, DuD 2014, 405.

[395] Cf. DSB 12. 5. 2008, K121.385/0007-DSK/2008; 30. 7. 2010, K121.605/0014-DSK/2010; 7. 9. 2013, K121.698/0004-DSB/2013; 9. 6. 2013, K121.605/0003-DSK/2013.

[396] The British study *Spiller,* Experiences of accessing CCTV data. The urban topologies of subject access requests, Urban Studies 2016, 2885.

[397] *Habu/Tristan*, Journal of Responsible Technology 2023, 100070.

[398] *Wulf/Seizov*, "Please understand we cannot provide further information". Evaluating content and transparency of GDPR-mandated AI disclosures, AI & Society 2024, 235 (235 et seq.).

[399] According to the authors, the sample refers to British respondents and is described as exploratory (i.e. not representative); cf. *Wulf/Seizov*, AI & Society 2024, 235 (238).

be disclosed. In addition, similar to the studies mentioned above, the researchers sent a total of 100 requests for information to various companies and organisations and systematically analysed their responses. In contrast to the online survey, the requests for information relate to German companies, with a heterogeneous selection of sectors ranging from airlines and car-sharing to insurance and utilities.[400]

The ensuing table illustrates the evaluation of the formal criteria. It demonstrates that in just over half of the cases, the companies had a designated and clearly labelled communication channel for data protection requests, through which it was easy to submit the requests. The average response time for requests was approximately three weeks and the text-based information ranged from a minimum of 29 words to a maximum of over 19,000 words. Moreover, the analysis shows that around 32% of companies merely referred to the privacy policy in their information.

In addition to the evaluation of the formal criteria, a linguistic analysis of the text-based responses was conducted. This analysis revealed that only half of the responses could be described as linguistically transparent, i.e. largely free of convoluted sentences, excessive legal or technical jargon or modal phrases that obscure the scope, type and frequency of automated data processing carried out by the organisation.

According to the information provided, around 66% of companies use some form of AI-based data processing. Most companies employ AI to enhance the customer experience and to optimise their product and service offerings. Forms of profiling and automated decision-making are the least common AI applications, at 30% and 26% respectively. However, the authors also assume that the companies surveyed repeatedly provide false information or simply do not disclose their utilisation of AI-based data processing methods.

---

[400] *Wulf/Seizov*, AI & Society 2024, 235 (241).

Table: Formal criteria in the response to requests for information (explorative samples of n=100 companies and organisations)

Means of First Contact	**Email**	**Contact Form**	**Other**		
	81%	18%	1%		
Ease of First Contact	**Easy**	**Neutral**	**Difficult**		
	54%	43%	3%		
Reply Time (Days)	**Min**	**Median**	**Mean**	**Max**	**S.D.**
	1	12	23	112	28.56
Length of Personalised Reply (Words)	20	272	654.80	11,977	1,470.37
Length of Disclosure (Response + Add-ons, Words)	29	1,260	2,379.48	19,116	3,046.39
Medium of AI Response	**Plain Email**	**Secure Email**	**Account Area**	**Webpage**	**Regular Mail**
	60%	3%	9%	4%	24%
Number of Messages Exchanged	**1**	**2 - 3**	**4 - 5**	**6 - 7**	**8**
	64%	21%	9%	5%	1%
Additional Authentication Requested	**None**	**Picture ID**	**Account Data**	**Multiple**	
	88%	7%	4%	1%	
Contact Person's Role	**Customer Service**	**Privacy Officer**	**Legal Counsel**	**Unknown / Other**	
	37%	31%	8%	24%	
Degree of Response Personalization	**Privacy Policy Reference**	**Generic GDPR Response**	**Personalized Response**		
	32%	22%	46%		
Personal Data Enclosed	**None**	**General GDPR Data**	**AI-Processed Data**		
	65%	11%	24%		

In summary, the authors found that in 51% of cases, the information on AI-based applications and automated data processing is either opaque or does not fully address the topic. Instead of disclosing which algorithms are employed, how they work and for what purpose, many companies obscure this information with misleading or overloaded wording. Only 18% of the information is described as sufficiently specific and transparent.

6.2 Automation Bias

Digital systems generally operate on the basis of binary codes (0/1). The process of developing the code to process data and analyse different scenarios is embedded in a specific socio-cultural context.[401] AI-based decision-making systems never function in an entirely objective manner. The criteria and thresholds employed to determine the classification of data as correct or incorrect, suspicious or unsuspicious, relevant or irrelevant are subject to different (methodological) approaches, perspectives and values, which are, to a certain extent, inscribed in the software and manifest themselves in the code.[402]

Furthermore, it is important to note that algorithmic decision-making systems are based on premises of statistical probability. Consequently, it can be argued that certain decisions are inherently subject to a certain level of significance or error (such as $\alpha = \leq 5\%$ or $\leq 1\%$). This ultimately means that no evaluation or classification of the system can be considered definitive. Rather, it is a human-defined threshold value of probabilistic tuning.[403] If this threshold value is set too high, there is a risk that the system fails to recognise a critical scenario (false rejection); if the system is set sensitively, this in turn implies an increased number of false alarms (false acceptance).[404]

The reference to such methodological inadequacies and potential biases is relevant as it is assumed that people tend to equate the information and decisions of a computer-based system with those of human beings, or even prefer them.[405] Early studies on this phenomenon can be found in particular in the field of aviation and cockpit research under the term "complacency".[406] The US National Aeronautics and Space Administration Center defines the term as "self-satisfaction that may result in non-vigilance based on an unjustified assumption of satisfactory

---

[401] Cf. the explanations in Rec. 44 AI Act.

[402] *Bowker/Star*, Sorting Things Out. Classification and Its Consequences (2000); *Graham/Wood*, Digitising Surveillance. Categorization, Space, Inequality, Critical Social Policy 2003, 227 (231 et seq.); *Rothmann/Vogtenhuber,* Abweichendes Verhalten und automationsunterstützte soziale Kontrolle, Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (288 ff).

[403] *Rothmann/Vogtenhuber,* Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (288 et seq.).

[404] *Introna/Wood*, Picturing Algorithmic Surveillance. The Politics of Facial Recognition Systems, Surveillance & Society 2004, 188; *Kammerer*, Bilder der Überwachung (2008) 202 et seq.

[405] *Reeves/Nass*, The media equation. How people treat computers, television, and new media like real people and places (2002); *Rothmann/Vogtenhuber,* Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (288 et seq.).

[406] *Parasuraman/Manzey*, Complacency and Bias in Human Use of Automation, Human Factors 2010, 381; *Wiener* describes this as a "psychological state characterised by a low index of suspicion", *Wiener,* Complacency. Is the term useful for air safety? in Flight Safety Foundation (ed.), Proceedings of the 26th Corporate Aviation Safety Seminar. Denver, CO 1981 (1981) 116.

system state".[407] The first empirical evidence of this effect was already provided in the early 1990s through various experimental test set-ups.[408]

Recently, this socio-technical problem has also been discussed under the term “automation bias”.[409] This is generally understood as the tendency to rely excessively on automated decision-making systems in certain situations without critically questioning their output.[410] Accordingly, decisions or recommendations based on automation are more likely to be regarded as valid and justified in practice, despite the possibility that they may provide incorrect or incomplete information.[411]

In the medical field in particular, the phenomenon of automation bias has been receiving increasing attention.[412] In the context of AI-assisted mammography, for example the bias can lead to false breast cancer diagnoses as well as unnecessary biopsies on persons with no abnormalities.[413] A study by *Khera et al.* (2023), for instance, reported that even in controlled environments without time pressure, medical staff preferred the automated decision system and relied on the AI-based tool despite the presence of contradictory or clinically unreasonable information.[414]

Another relevant study entitled “Automation bias: a systematic review of frequency, effect mediators, and mitigators“ was conducted by *Goddard et al.* (2012), who undertook a meta-analysis of 74 international (medical) articles.[415] In the course of this study, a range of factors that can influence or encourage automation bias are described. As influencing factors on the user side, the authors identify cognitive characteristics as well as task-specific previous experience, attitudes (e.g. trust or confidence) and convictions. Environmental factors mentioned include workload, task complexity and time pressure, which in turn can have cognitive effects.[416] Research also indicates that users with less experience tend to be averse to AI systems, whereas preconception towards automation decreases with a higher level of knowledge.[417]

As a strategy for mitigating automation bias, the possibility of offering training courses or

---

[407] *Billings/Lauber/Funkhouser/Lyman/Huff*, Aviation Safety Reporting System (1976) 23.

[408] *Parasuraman/Manzey*, Human Factors 2010, 381 (383 et seq.).

[409] *Alon-Barkat/Busuioc*, Human-AI Interactions in Public Sector Decision Making. "Automation Bias" and "Selective Adherence" to Algorithmic Advice, Journal of Public Administration Research and Theory 2023, 153; *Logg*, Algorithm Appreciation. People Prefer Algorithmic to Human Judgment, Organizational Behavior and Human Decision Processes 2019, 90.

[410] *Wickens/Clegg/Vieane/Sebok*, Complacency and Automation Bias in the Use of Imperfect Automation, Human Factors 2015, 729.

[411] This also implies that AI-based decisions tend to become less negotiable. In Lessig's sense, the code thus becomes the law (code is law) and the algorithm becomes the norm-setting force in the social sphere. *Lessig,* Code - Version 2.0 (2006); cf. also *Kammerer*, Bilder der Überwachung 205; *Rothmann/Vogtenhuber*, Zeitschrift für soziale Probleme und soziale Kontrolle 2013, 271 (289).

[412] *Goddard/Roudsari/Wyatt*, Automation bias. A systematic review of frequency, effect mediators, and mitigators, J AmMed Inform Assoc 2012, 121.

[413] *Baltzer*, Automation Bias in Breast AI, Radiology 2023, e230770.

[414] *Khera/Simon/Ross*, Automation Bias and Assistive AI, Risk of Harm From AI-Driven Clinical Decision Support, jama 2023, 2255.

[415] *Goddard/Roudsari/Wyatt*, J AmMed Inform Assoc 2012, 121 (121 et seq.).

[416] *Goddard/Roudsari/Wyatt*, J AmMed Inform Assoc 2012, 121 (121 et seq.).

[417] *Horowitz/Kahn*, Bending the Automation Bias Curve. A Study of Human and AI-Based Decision Making in National Security Contexts, International Studies Quarterly 2024, sqae020.

various forms of supporting information is repeatedly discussed in the literature. Consequently, such information, together with design factors like the position of the advice on the screen and the nature of the advice (e.g. information vs. recommendation), can improve decision-making.[418] In this regard, a German study by *Bahner et al.* (2008) analysed the effect of specific training courses on the handling of automated decisions and a possible associated automation bias.[419] This was found to reduce user inattention or indifference to potentially biased results, thereby encouraging them to question the automated decisions.

Training courses can therefore be considered a suitable means of reducing the risk of being deceived by a supposed bias, even if this ultimately cannot completely avoid it.

The Australian study by *Vereda et al.* (2023), in turn, demonstrates how the provision of general explanations regarding the functionality of "intelligent agents" influences the automation bias. According to the study, this does not necessarily reduce the bias, but at times even increase it.[420] However, information or explanations can shorten the time taken for human decision-making and enhance the accuracy of users' decisions. The authors posit that, in general, the approach is effective, yet the advantages are considered to be highly contextdependent. Eventually, the authors also address the trade-off between the degree of user bias and the accuracy of the system. They conclude that a balance should be sought, whereby users should be helped to accept decisions made by particularly accurate and robust systems, i.e. to reduce “algorithmic aversion”, but at the same time remain sceptical in certain situations.[421]

Based on *Baltzer* (2023), the following strategies can be recommended to mitigate the effects of automation bias for organisational implementation:[422]

- **Training and** on-going **awareness-raising** for users of automated systems to raise awareness of the problem of automation bias and promote the ability to make more informed decisions, avoid automation-related negligence and critically question automated decisions.
- **Design** and **development of** a **transparent system** that displays and communicates its own uncertainties and thus helps users to better assess the reliability of the automated recommendations. This implies regular technical validation and ensuring the accuracy and robustness of the system.
- More generally, there is a need to **ensure accountability** for decisions and the identification or designation of appropriate points of contact.

---

[418] *Goddard/Roudsari/Wyatt*, J AmMed Inform Assoc 2012, 121 (125).
[419] *Bahner/Hüper/Manzey*, Misuse of automated decision aids. Complacency, automation bias and the impact of training experience, Int. J. Human-Computer Studies 2008, 688.
[420] *Vereda/Livnia/Douglas/Howeb/Millerc/Sonenberg*, The effects of explanations on automation bias, Artificial Intelligence 2023, 103952.
[421] *Vereda et al.*, Artificial Intelligence 2023, 103952.
[422] *Baltzer*, Radiology 2023, e230770.

7 Ethical aspects

In addition to legal and sociological aspects, the right to explanation and the general handling of AI-based systems also have a strong ethical component. Ethics is generally defined as philosophical reflection on moral concepts, such as "good" and "evil" or "right" and "wrong".[423] As a philosophical discipline ethics is concerned with the critical examination of normative assumptions, values and judgements that are subject to decision-making and action.[424] An understanding of ethics that reflects the reality of life and its specific problems is often associated with the ethical sub-discipline of applied ethics, which aims to analyse questions that arise in specific areas, such as bioethics, technology ethics, business ethics, legal ethics or political ethics.[425] One field of applied ethics and a sub-discipline of technology ethics is so-called "AI ethics", which deals with normative questions raised by the conception, development, implementation and use of AI.[426]

The development of AI ethics highlights the significant ethical implications of artificial intelligence for humans and society at large, which now extend to almost all areas of our lives.[427] These implications encompass the changing relationship between humans and machines and raise significant questions about human autonomy, dignity, fairness, transparency and the wider societal and environmental impacts of AI.[428] In summary, this so-called "ethical impact" of artificial intelligence manifests itself in both ethical risks and ethical benefits that can arise from the use of either certain AI systems themselves, of AI in certain sectors, towards certain individuals or groups of individuals, or in specific contexts.[429] However, the aforementioned effects, which encompass issues such as societal well-being, social inclusion and democratic discourse, are not sufficiently taken into account in the existing legal framework.[430]

In response to the challenges associated with the increasing technological progress in the field of AI research, numerous organisations have developed ethical guidelines that are intended to serve as a standard or orientation for the development and deployment of AI. Examples include the Ethics Guidelines for Trustworthy AI of the Independent High-Level Expert Group on Artificial Intelligence[431] on which the "ALTAI" assessment list is based[432] , the OECD AI Principles[433], and the UNESCO Recommendations on the Ethics of Artificial Intelligence[434].

---

[423] Cf. *Singer,* Ethics. philosophy, https://www.britannica.com/topic/ethics-philosophy (as at 13 February 2025).

[424] *Rubeis,* Ethics of Medical AI (2024) 56.

[425] Cf. *Pauer-Studer*, Einführung in die Ethik^3 (2020) 14.

[426] Cf. *Stahl,* From computer ethics and the ethics of AI towards an ethics of digital ecosystems, AI and Ethics 2022, 65 and *AI HLEG,* Ethics Guidelines 37.

[427] Cf. *Mantelero,* Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI (2022) 93.

[428] Cf. *Mantelero,* Beyond Data 93.

[429] Cf. *Poindl/Scheichenbauer/Müller*, Folgenabschätzungs-Methodologie. Datenschutz, Grundrechte, Ethik, in *Eisenberger/Klaushofer* (eds.), KI-VO. Exekutive Rechtsetzung, Standardisierung, Zertifizierung und Grundrechte-Folgenabschätzung (2025) tpb.

[430] Cf. *Poindl/Scheichenbauer/Müller* in *Eisenberger/Klaushofer* tpb.

[431] *AI HLEG,* Ethics Guidelines 2019.

[432] *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment (2020), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342.

[433] *OECD,* AI principles, https://oecd.ai/en/ai-principles (last access: 14 February 2025).

[434] *UNESCO,* Recommendation on the Ethics of Artificial Intelligence (2022),

These documents advocate for the utilisation of trustworthy AI and are founded on the safeguarding of human dignity and autonomy.

The principles of transparency and explainability of AI-based processes are given particularly high priority in all of the aforementioned guidelines. However, other principles cited in these documents, such as accountability, human oversight, non-discrimination, efficiency or trustworthiness, are also equally important for the right to explanation. At this point, reference should be made in particular to the meta-study by Jobin et al. (2019) on the "Global landscape of AI ethics guidelines", which provides an overview of the existing corpus of documents containing soft law standards or ethical guidelines issued by organisations on the use of AI. Furthermore, the study examines which statements can be deduced from the aforementioned principles for the right to explanation, and which information regarding AI systems should be disclosed as a consequence. The majority of sources cited general explanations of the use of the system, the source code, the use of data, potential effects and explanations in non-technical language as important requirements.[435]

With reference to ethical guidelines and publications, these requirements and the following additional elements (see points 1-10 below) can be identified as essential elements of the right to explanation from an ethical perspective. It should be noted that these elements do not relate exclusively to individual *ex post* explanations. Some also aim to provide general *ex ante* explanations, with the objective of enabling affected persons to comprehend the system's operation in advance. This is because explanations can generally be distinguished between those that relate to the general functionality of the AI system (model explainability or global explainability), which are possible both in advance and retrospectively, and those that relate to individual decisions (local explainability or data explainability).[436] The elements listed below include both explanatory approaches:

1. **Explanation of the decision-making process:** An explanation of whether and how algorithms have made a decision, and the reasons for using particular models and methods. This includes an explanation of why the particular decision was chosen from a range of possible alternatives.[437]
2. **Transparency of the data used:** This includes a detailed list of the input data, its origin and information on how the data is processed.[438]
3. **Transparency of the models and algorithms used:** Information about the functioning of the models used (e.g. decision trees or deep neural networks) and their potential

---

https://unesdoc.unesco.org/ark:/48223/pf0000381137.

[435] *Jobin/Ienca/Vayena,* The global landscape of AI ethics guidelines, nature machine intelligence 2019, 389 (391).

[436] Cf. *Deutsches Bundesministerium für Arbeit und Soziales (BMAS*), Selbstverpflichtende Leitlinien für den KI-Einsatz in der behördlichen Praxis der Arbeit und Sozialverwaltung (2022) 56, https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/a862-01-leitlinien-ki-einsatz-behoerdliche-praxis-arbeits-sozialverwaltung.pdf?__blob=publicationFile&v=2 and the more detailed explanations in Section 5.4.2.

[437] Cf. *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 14; *AI HLEG,* Ethics Guidelines for Trustworthy AI 18; *OECD,* AI principles; *Deutsches Bundesministerium für Arbeit und Soziales*, Selbstverpflichtende Leitlinien für den KI-Einsatz 55.

[438] Cf. *OECD,* AI principles; *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22; *Deutsches Bundesministerium für Arbeit und Soziales*, Selbstverpflichtende Leitlinien für den KI-Einsatz 55; *Brey/Dainow*, AI and Ethics 2024, 1265 (1269).

sources of error.[439]

4. **Influence of relevant characteristics** on the decision and analysis of the weighting of these characteristics. This should also contribute to fairness and reveal any discrimination or bias.[440]
5. **Understandability and comprehensibility of the explanation:** Explanations must be written in clear, non-technical and understandable language. They must be adapted to the expertise of the persons affected in such a way that they can understand the explanation.[441]
6. **Involvement of human oversight:** The explanation should encompass information on the extent to which human decision-makers are involved in decision-making.[442]
7. **Legal basis of the decision:** The legal basis of the decision should be made transparent. This includes disclosing the possibility of contesting the decision and informing those affected about their rights.[443]
8. **Impact of the decision:** It is advisable to set out the potential impact of the decision on the affected person, including the social and economic context.[444]
9. **Responsibility and liability:** Responsible persons should be clearly named in general and to the affected persons to enable clear attribution in the event of incorrect decisions and to inform those affected who they can contact.[445]
10. **Ethics in decision-making:** Ethical considerations should be incorporated into the development and design of AI systems from the outset ("ethics by design").[446] The ethical considerations underlying the decision should be made transparent to strengthen trust in the moral integrity of the system.[447]

---

[439] Cf. *AI HLEG,* Ethics Guidelines for a Trustworthy 18; *OECD,* AI principles.

[440] Cf. *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 16; *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22.

[441] Cf. *AI HLEG,* Ethics Guidelines for Trustworthy AI 18; *OECD,* AI principles; *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22.

[442] Cf. *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 8.

[443] Cf. *UNESCO,* Recommendation on the Ethics of Artificial Intelligence 22.

[444] Cf. *OECD,* AI principles.

[445] Cf. *AI HLEG,* The Assessment List for Trustworthy Artificial Intelligence 21.

[446] Cf. *AI HLEG,* Ethics Guidelines for Trustworthy AI 21.

[447] Cf. *Brey/Dainow*, AI and Ethics 2024, 1265 (1267 et seq.).

8 Conclusion

It is evident that the right to explanation is facing new challenges in the age of increasing AI-based decision-making. Nevertheless, the associated uncertainties and unresolved legal issues require clarification, because the right to explanation constitutes an essential right of the affected persons that serves to make decisions verifiable and provides those affected with a tool to enforce related rights. The present report has demonstrated that both a joint and yet separate consideration of data protection aspects and the new regime of Art. 86 AI Act is needed. Simultaneously, it shows that several issues can already be addressed by referring to existing case law on data protection, despite the lack of experience with the practical implementation of the AI Act.

The central components of an explanation in accordance with Art. 86 AI Act could thus be determined by comparing the AI Act with existing data protection rules, combined with derivations from case law and literature, as well as by examining the process of the AI Act's creation. On the one hand, this encompasses central factors (criteria, characteristics) that were utilised in the decision-making procedure, including, in particular, the input data. Furthermore, it is essential to provide detailed information regarding the weighting of these factors, and, to the greatest extent possible, the impact of the decision on the affected person. While the explanation does not require the disclosure of the complete algorithmic code on which the system is based, it must contain information on the algorithmic weighting of the most significant parameters, a description of the system processes and an explanation of the basic functionality of the algorithm in question. In addition, the report could already address formal aspects concerning the right to explanation under Art. 86 AI Act, and deal with other related information duties.

Possible demarcation issues were illustrated by the selected use cases at a practical level in order to make the sometimes abstract legal explanations more tangible. The selected case studies covered pricing in life and health insurance, churn prediction, credit scoring and emotion recognition in marketing and sales promotion (including four sub-cases). It could be demonstrated that the majority of the use cases under consideration employed high-risk AI systems for decision-making purposes according to Art. 6(2) in conjunction with Annex III AI Act. Furthermore, it was established that these use cases fulfil the requirements for falling within the scope of Art. 86 AI Act. However, it should be emphasised that, in view of the sparse existing literature and lack of case law on Art. 86 AI Act, the purpose of this report is not to provide a general classification of certain types of cases. Thus it is necessary to examine each case on its individual merits to determine whether it falls within the scope of the AI Act and subsequently Art. 86 AI Act, which in turn determines whether an affected person is entitled to the right of explanation. It is also important to note that Art. 86 AI Act was not yet applicable at the time of the publication of this report (February 2025). Consequently, future literature and Supreme Court rulings will continue to address specific unresolved issues. Therefore, this report is not intended to be a definitive analysis and also incorporates perspectives from other disciplines to provide a more comprehensive understanding of the right to explanation.

The presentation of relevant social science aspects enabled an exploration of the right to explanation beyond the legal perspective. This revealed the reasons why the right to access established under Art. 15 GDPR, is not always complied with in practice, and consequently allowed to draw conclusions for a better practical enforceability of Art. 86 AI Act. Furthermore, reference was made to the concept of "automation bias", which describes the tendency of persons to over-rely on automated decisions. This underscores the need for training in this area, especially regarding AI-based decisions that invoke the right to access under Art. 86 AI Act. In addition, this phenomenon highlights the urgent need for human review of AI-based decisions, even in instances where it is not legally or otherwise mandated, while this information should also be included in an explanation according to Art. 86 AI Act.

Finally, relevant ethical aspects of the right to explanation were presented. While they partly coincide with the legal requirements, they represent a valuable addition. For example, it may be ethically useful for a controller to inform the affected persons about the existence of certain human lines of responsibility so that they can better understand how the decision was made and have more trust in the company using AI. It is therefore advisable to also include this aspect in an explanation pursuant to Art. 86 AI Act, even if this is not legally required. Furthermore, businesses should provide information about the legal basis of the decision-making process and make the ethical considerations underlying the decision-making process transparent. Finally, ethical considerations provide information about the general barriers that we as a society wish to impose on ourselves and which are particularly relevant when an area is still (legally) unregulated in the face of constant technological progress.

9 Annex

9.1 High-risk AI systems pursuant to Annex III AI Act

1. Biometrics

Biometrics*, in so far as their use is permitted under relevant Union or national law:*

a) ***remote biometric identification systems.*** *This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;*

b) ***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;*

c) ***AI systems*** *intended to be used for* ***emotion recognition****.*

2. Critical infrastructure

AI systems *intended to be used as* ***safety components*** *in the* ***management*** *and operation of* ***critical*** *digital* ***infrastructure****, road traffic, or in the supply of water, gas, heating or electricity.*

3. Education and vocational training

a) ***AI systems*** *intended to be used to determine* ***access*** *or* ***admission*** *or to assign natural persons to* ***educational*** *and* ***vocational training*** *institutions at all levels;*

b) ***AI systems*** *intended to be used to* ***evaluate learning outcomes****, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels;*

c) ***AI systems*** *intended to be used for the purpose of* ***assessing the appropriate level of education*** *that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels;*

d) ***AI systems*** *intended to be used for* ***monitoring and detecting prohibited behaviour*** *of students* ***during tests*** *in the context of or within educational and vocational training institutions at all levels.*

4. Employment, workers‘ management and access to self-employment

a) ***AI systems*** *intended to be used for the* ***recruitment or selection of natural persons****, in particular to place* ***targeted job advertisements****, to* ***analyse and filter job applications****, and to* ***evaluate candidates****;*

b) ***AI systems*** *intended to be used to make* ***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.*

5. Access to and enjoyment of essential private services and essential public services and benefits:

a) ***AI systems*** *intended to be used by* ***public authorities*** *or on behalf of public authorities to* ***evaluate*** *the* ***eligibility*** *of natural persons for* ***essential public assistance benefits and services****, including* ***healthcare services****, as well as to grant, reduce, revoke, or reclaim such benefits and services;*

b) ***AI systems*** *intended to be used to* ***evaluate the creditworthiness*** *of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud;*

c) ***AI systems*** *intended to be used for* ***risk assessment and pricing*** *in relation to natural persons in the case of* ***life and health insurance****;*

d) ***AI systems*** *intended to evaluate and* ***classify emergency calls*** *by natural persons or to be used to dispatch, or to* ***establish priority*** *in the dispatching of,* ***emergency first response services****, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems.*

6. Law enforcement

***Law enforcement, in so far** as their use is **permitted** under relevant Union or national law:*

- ***a)*** ***AI systems** intended to be used by or on behalf of **law enforcement authorities**, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to **assess the risk** of a natural person **becoming the victim of criminal offences**;*
- ***b)*** ***AI systems** intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools;*
- ***c)*** ***AI systems** intended to be used by or on behalf of **law enforcement authorities**, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to **evaluate the reliability of evidence** in the course of the investigation or prosecution of criminal offences;*
- ***d)*** ***AI systems** intended to be used by **law enforcement authorities** or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for **assessing the risk of a natural person offending** or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;*
- ***e)*** ***AI systems** intended to be used by or on behalf of **law enforcement authorities** or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the **profiling of natural persons** as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the **detection, investigation or prosecution of criminal offences**.*

7. Migration, asylum and border control management

***Migration, asylum and border control management, in so far as** their use is **permitted** under relevant Union or national law:*

- ***a)*** ***AI systems** intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies as **polygraphs** or similar tools;*
- ***b)*** ***AI systems** intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to **assess a risk**, including a **security risk**, a risk of **irregular migration**, or a **health risk**, **posed by a natural person** who **intends to enter or who has entered** into the territory of a Member State;*
- ***c)*** ***AI systems** intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assist competent public authorities for the **examination of applications for asylum, visa or residence permits** and for*

associated complaints with regard to the eligibility of the natural persons applying for a status, including related ***assessments of the reliability of evidence****;*

d) ***AI systems*** *intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, in the context of* ***migration, asylum or border control management,*** *for the purpose of* ***detecting, recognising or identifying natural persons****, with the exception of the verification of travel documents.*

8. Administration of justice and democratic processes

a) ***AI systems*** *intended to be used by a* ***judicial authority*** *or on their behalf to assist a judicial authority in* ***researching and interpreting facts and the law*** *and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution;*

b) ***AI systems*** *intended to be used for* ***influencing the outcome of an election or referendum or the voting behaviour*** *of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view.*

9.2 List of abbreviations

A29WP	Article 29 Data Protection Working Party
AI	Artificial Intelligence
AI Act	Artificial Intelligence Act (EU AI Regulation)
AI HLEG	High-Level Expert Group on Artificial Intelligence ("Independent Expert Group on Artificial Intelligence")
Art	Article
BDSG	Federal Data Protection Act (German abbreviation)
BVwG	Federal Administrative Court (Austria)
cf	confer
CFR	Charter of Fundamental Rights of the European Union
DPA	Data Protection Act (Austria)
DPD	Data Protection Directive (Directive 95/46/EC)
DSB	Data Protection Authority (Austria)
DSG	Data Protection Act (Austria) (German abbreviation)
DSGVO	General Data Protection Regulation (German abbreviation)
ECJ	European Court of Justice
Ed.	Publisher
EDPB	European Data Protection Board
eds.	editors
e.g.	for example
EP	European Parliament
ERS	Emotion recognition system
esp.	in particular
et al.	et alii, et aliae, et alia (and others)

etc.	et cetera
et seq.	and the following
EU	European Union
GDPR	General Data Protection Regulation
GRC	Charter of Fundamental Rights of the European Union (German abbreviation)
i.e.	that means
LED	Data Protection Law Enforcement (Directive (EU) 2016/680)
lit	litera (letter)
OJ	Official Journal (of the EU)
para./paras	Margin figure(s)
Rec.	Recital
RTE	Right to Explanation
tbp	to be published
TFEU	Treaty on the Functioning of the European Union
VO	(EU) Regulation
XAI	eXplainable AI ("Explainable AI")

Research Institute – Digital Human Rights Center

https://researchinstitute.at

kontakt@researchinstitute.at