User Rights and Adaptive A/IS – From Passive Interaction to Real Empowerment

Ozlem Ulgen[1][0000-0003-0246-5736]

[1] Birmingham City University, Birmingham, UK
ozlem.ulgen@bcu.ac.uk

Abstract. Adaptive autonomous intelligent systems (A/IS) may satisfy design functionality and user experiential requirements but prior to deployment an assessment must be made of their impact on user rights. A/IS systems may assist rather than replace humans but it is unclear where the line is drawn between supplementing human endeavour and knowledge, on the one hand, and gradual erosion of human cognitive abilities on the other. This paper makes the case for development of ethical standards for user awareness of A/IS in operation, taking account of rights under the EU General Data Protection Regulation (GDPR) and the Council of Europe Modernised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+). It sets out three main user awareness stages (pre-use, during-use, and post-use) along with consideration of commensurate rights. In the pre-use stage potential users will need to be aware that an A/IS is either fully or partially in operation, and consent to such an operation or have the option to opt out. During A/IS use if there is a part of the A/IS operation which involves a "black box" scenario, that is, it is difficult for a human to discern what the system is doing and why, then appropriate risk-based parameters need to be set for the systems use. Post-use requires users to be aware of how their data and information shared with the A/IS will be used by the system and any third parties.

Keywords: User Rights; Adaptive Autonomous Intelligent Systems (A/IS); "Technology-Biased Approach" (TBA); "Human-Centric Approach" (HCA); GDPR; Convention 108+; Pre-Use, During-Use, Post-Use Awareness and Rights Stages.

1. Rationale for User Awareness and Rights Stages

As technology proceeds at a pace difficult for legislators to keep up with, a corpus of ethical principles has emerged to regulate design, development, and deployment, namely: human agency; human control; privacy and data protection; prevention of harm; fairness; transparency; auditability; accountability; and responsibility. Human agency requires that A/IS designers, developers, and deployers exercise professional and ethical practices, and respect and give effect to the autonomy of A/IS users.[1] This means that humans interacting with A/IS must be able to keep full and effective self-determination over themselves without being subordinated, deceived, manipulated, or coerced by the A/IS. Technology complements rather than replaces human capabilities. Human control requires that A/IS designers, developers, and deployers introduce mechanisms to ensure some form of human involvement in the operation of the A/IS or human control over how, when, and where it operates.[2] Privacy and data protection requires that A/IS designers, developers, and deployers have mechanisms in place to safeguard and protect personal data and its use throughout the

A/IS lifecycle, respecting users' privacy rights.[3] Prevention of harm requires that A/IS designers, developers, and deployers create and use systems which are not harmful to humans, society, and the environment, and which ensure the well-being of humanity.[4] Fairness requires that A/IS designers, developers, and deployers ensure diversity of personnel involved in assessing risks/problems associated with A/IS, and awareness of different cultural norms in order to ensure non-discrimination in A/IS use.[5] Transparency applies both to the information provided to the user regarding data processing as well as the actual processing and functionality of the A/IS.[6] Auditability requires that A/IS designers, developers, and deployers have auditable mechanisms in place to ensure explainability of A/IS actions, consequences, and responses to risks/problems.[7] Accountability requires that A/IS designers, developers, and deployers account for their actions, respond to user concerns and problems, and provide explanations and justifications for A/IS actions and consequences.[8] Responsibility requires that A/IS designers, developers, and deployers have redress mechanisms in place for errors/complaints/harmful consequences from A/IS, and accept legal responsibility under relevant laws.[9]

A/IS technologies may be introduced at various lifecycle stages of a product, service, or system and consideration of lifecycle stages makes it clearer to understand how the technology operates, its intended function, and effects. This can be referred to as the "technology-biased approach" (TBA) which seeks to better understand the capabilities and limitations of the A/IS in order to improve performance, optimise operational efficiency, and identify and rectify any errors or failures. However, given the plethora of ethical principles mentioned above and their focus on the human user, on its own, the TBA creates ethical dissonance by not aligning design, development, and deployment with values protecting the human user. For human-machine interaction, the TBA limits its focus on the system rather than considerations of human wants, needs, and values that can be incorporated into the system lifecycle stages. A "human-centric approach" (HCA) would have such considerations at the forefront of design, development, and deployment. Ultimately, the mergence and integration of TBA and HCA will lead to not only improved functionality and reliance of A/IS, but also to ethically aligned design, development, and deployment to take account of user awareness and rights. The HCA that espouses user awareness and rights is evident in the plethora of international, regional, and national regulatory standards emerging in relation to artificial intelligence, robotics, and emerging technologies more generally.[10] The EU General Data Protection Regulation (GDPR),[11] and the Council of Europe Modernised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+)[12] contain

provisions respecting and safeguarding user rights related to A/IS particularly as they relate to data processing and personal data. Lifecycle stages exist as a matter of logical application and purposive interpretation of rights contained in these provisions, even though these are not explicitly mentioned.[13] We can identify and analyse user awareness and rights in three stages: (i) pre-use stage; (ii) during-use stage; and (iii) post-use stage.

2. Pre-Use Stage

In the pre-use stage potential A/IS users will need to be aware that an A/IS will be either fully or partially in operation, and consent to such an operation or have the option to opt out. With potential A/IS users being made aware of the existence of an A/IS element in the context of use, they will be empowered to decide for themselves whether they want to interact or engage with such a system or not. Ethically, human agency is exercised through free will and active informed consent in the choice that needs to be made. A number of mechanisms and procedures would need to be in place to enable the user to: (a) have pre-use awareness of the type of A/IS product, service, or system they are interacting with, including whether there is an AI element; (b) opt out of using the product, service, or system; (c) challenge an A/IS decision effectively and efficiently; (d) understand the full terms and conditions that apply to any A/IS interactions; and (e) review at a later date to understand previous A/IS interactions.

2.1. Pre-Use Awareness

Potential A/IS users must be able to understand the type of A/IS product, service, or system they are interacting with, including whether there is an AI element and whether the A/IS will be fully or partially in operation. Such information should be conveyed in a manner that is clear, accessible, and provides a real opportunity to exercise human agency prior to any use. This also means making the information easily understandable and accessible without causing undue inconvenience to the user (e.g. avoiding multiple click throughs to get to the relevant information; avoiding non-transparent or hidden locations to display information). The pre-use awareness issues outlined above fall under several provisions of the GDPR, and Convention 108+ (see Table 1).

Table 1. Pre-Use Stage Rights

Right	GDPR Provision	Convention 108+ Provision
Not to be subject to automated decision-making	Article 22(1)	Article 9(1)(a)

Table 1. Pre-Use Stage Rights

Right	GDPR Provision	Convention 108+ Provision
To prior consent	Article 7(1)	Article 5(2)
To be notified of right to withdraw consent prior to giving consent	Article 7(3)	
To be notified of automated decision-making	Articles 13(2)(f), 14(2)(g), 15(1)(h)	Article 9(1)(b)
To access to personal data	Article 15(1)(h)	Articles 8(1), 9(1)(b)
To information on logic in automated decision-making	Articles 13(2)(f), 14(2)(g), 15(1)(h)	Article 9(1)(c)
To information on the significance and envisaged consequences of automated decision-making processing	Articles 13(2)(f), 14(2)(g), 15(1)(h)	
To object to processing of data	Article 21	Article 9(1)(d)

Right not to be subject to automated decision-making

Article 22 of the GDPR states:

> *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.

Paragraph 1 makes it clear that a person has the right not to be subject to a decision based solely on automated processing, including profiling,[14] which produces legal effects concerning him or her or similarly significantly affects him or her. This represents a general prohibition on such automated decision-making. The negative right formulation also gives rise to exercising human agency prior to any A/IS use (e.g. by requesting confirmation or assurance that such decision-making is not taking place; a person being able to object even if such decision-making is deemed not to have legal effects or similarly significant effects). "Legal effects" refers to affecting a person's legal rights, obligations, or status (e.g. freedom to associate with others; voting in elections; taking legal action; termination or cancellation of a contract; residency or citizenship rights).[15] "Similarly significant" effects refers to adverse impacts that are similar to legal effects such as affecting the circumstances, behaviour or choices of the individual concerned; having a prolonged or permanent impact on the data subject; or leading to the exclusion or discrimination of individuals.[16] Examples include automatic refusal of online credit applications, e-recruitment without human intervention, automated systems determining access to health and education services.

Paragraph 2 sets out exceptions to the right not to be subject to automated decision-making which include: a) necessity of automated decision-making for entering into or performance of a contract between the data subject and a data controller (contract exception); b) authorisation by EU law or EU Member State law to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or c) data subject's explicit consent (consent exception). If contract or consent exceptions apply, Paragraph 3 requires the data controller to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, and 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. These latter user safeguards are relevant to the opt out mentioned below.

Even if an exception applies, under Paragraph 4, the automated decision cannot be based on "special categories of personal data" (i.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation).[17] The only exceptions to automated decisions based on "special categories of personal data" is where the data

subject has given explicit consent to the processing of such personal data for one or more specified purposes, except where EU law or EU Member State law prevent such consent from overriding the prohibition;[18] or processing of such personal data is necessary for reasons of substantial public interest, on the basis of EU law or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[19]

In contrast to the GDPR, Article 9(1)(a) of Convention 108+ provides a somewhat weaker right not to be subject to solely automated decisions:

> *Every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration.*

If an individual objects to automated decision-making this does not necessarily mean it will not take place. An organisation may show it has "taken into consideration" the individual's objection and justify proceeding with automated decision-making under Article 11 on the grounds that it is provided for by law and constitutes a necessary and proportionate measure in a democratic society for quite wide-ranging purposes including: national defence, national security, public safety, important economic and financial interests of the state, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest, protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression, archiving in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.

In any case, Article 5(2) of Convention 108+ contains an implicit right to prior consent to data processing by requiring States Parties to demonstrate that data processing is carried out on the basis of the "free, specific, informed and unambiguous consent of the data subject" or of some other legitimate basis laid down by law. Consent here means the free expression of an intentional choice, given either by statement (in written, electronic, or oral form) or by a clear affirmative action which clearly indicates acceptance of the proposed processing of personal data. Mere silence, inactivity or pre-validated forms or boxes will not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. Where there are multiple purposes, consent should be given for each different purpose.[20] Under Article 7(1) of the

GDPR there is a general consent provision whereby the data controller must be able to demonstrate that the data subject has consented to the processing of their data. In addition, under Article 7(3) the data controller is required to notify the data subject prior to them giving consent that they have the right to withdraw consent at any time.

Right to be notified of automated decision-making

Article 13(2)(f) of the GDPR provides that the data controller shall, at the time when personal data are obtained, provide the data subject with information on 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. Article 14(2)(g) provides that where personal data have not been obtained from the data subject, the data controller is obliged to provide the data subject with information on 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. Article 15(1)(h) provides users with the right of access to personal data along with notification on 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.

In contrast to the GDPR, Article 9(1)(b) of Convention 108+ provides a right to:

> *obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1.*

Although this is not expressed in terms of a pre-use right, the reference to "at reasonable intervals" would cover pre, during, and post use stages. This may seem onerous on the organisation using automated decision-making, but the right is exercising by the user requesting such information rather than the organisation being required to disclose prior to use. Under Article 8(1) the organisation has a duty to be transparent in data processing by providing the data subject with information on the legal basis and the purposes of the intended processing, the categories of personal data processed, the recipients or categories of recipients

of the personal data, if any, and the means of exercising the rights under Article 9.

Right to meaningful information about the logic involved in automated decision-making

The reference in Articles 13(2)(f), 14(2)(g), 15(1)(h) of the GDPR to users having the right to "meaningful information about the logic involved" in automated decision-making is intended to enable users to contest, challenge, or dispute the decision. Necessarily the information should be of a type and nature that is comprehensible to the user and that can be used subsequently to challenge any decision. Recital 58 of the GDPR states that the principle of transparency requires that any information addressed to the public or to the data subject should be "concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used." A range of information may fall under this provision including: algorithmic models; datasets; personal data disclosed by the user; previous data about the user held by the organisation; official data sources (e.g. electoral roll; anti-money laundering and fraud detection lists; land registry; births, deaths, and marriages registry); and regulated-industry data sources (e.g. banking; credit reference agencies; insurance; healthcare). Including the algorithmic model upon which the automatic decision-making is based would allow users to challenge the rules that are being applied to assess and reach a decision. Whether or not it is appropriate and necessary to disclose the algorithmic model, their complexity should not be used as an excuse to avoid providing meaningful information. Recital 58 of the GDPR states that the principle of transparency is of "particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising." All other types of information would allow the user to contest the accuracy of the data being used.[21]

Article 9(1)(c) of Convention 108+ is similar in providing for a right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to the data subject. This includes knowing the reasoning underlying the processing of data, and the consequences of such a reasoning, which led to any resulting conclusions (e.g. logic of an algorithmic credit scoring system that leads to acceptance or rejection of an application). This right is especially relevant in the context of exercising the right to object and the right to complain under Articles 9(1)(d) and (f). Article 9(1)(d) contains the right to object at any time to the processing of personal data, unless the data controller demonstrates legitimate grounds for such processing which

override the data subject's interests or rights and fundamental freedoms. The right to complain is of relevance at the post-use stage. Although Article 21 of the GDPR provides for a right to object to processing of personal data at any time, some consider this separate and inapplicable to automated decision-making under Article 22 due to the contract and consent exceptions.[22] But such an interpretation would defeat the essence of human agency by not recognising personal autonomy in the decision as to whether to engage with an A/IS. It is also an unrealistic representation of pre-use stage user experience and reactions, and fails to take account of Article 21(5) allowing users to exercise their right to object by automated means.

Right to meaningful information about the significance and the envisaged consequences of automated decision-making processing

The reference in Articles 13(2)(f), 14(2)(g), 15(1)(h) of the GDPR to users having the right to "meaningful information about … the significance and the envisaged consequences of such processing" is a much broader right of explanation which has been interpreted to mean "information must be provided about intended or future processing, and how the automated decision-making might affect the data subject. In order to make this information meaningful and understandable, real, tangible examples of the type of possible effects should be given."[23] Automated decision-making processing that produces legal effects or similarly significantly affects on the data subject falls under this category of A/IS user right to information and disclosure. Overall, this right may require information on the processing system itself, the processing that led to the decision, and the possible consequences to the user. An example of how this right could be operationalised at the pre-use stage is an illustrative, interactive web-based comparator model allowing the user to input varying data to produce different results (e.g. car, home, health insurance premiums based on certain risk factors such as age, dangerous driving habits, year property built, underlying health issues).

Opt Out

Potential A/IS users, who at the pre-use stage identify that the A/IS will be in full or partial operation and do not want to interact with the A/IS, must have the option to opt out of use and for an alternative method of use to be made available. An example where this may be necessary is eligibility assessments and approval decisions for financial products such as mortgages and medical insurance, where the user's particular circumstances and personal details require careful human consideration and evaluation rather than being subjected to algorithmic decision-making. The A/IS must be able to demonstrate the availability of an opt out and alternative methods of use. The opt out may also

need to be extended to during-use stage. If through use of the A/IS there is user profiling, this must be clear at the pre-use stage and an opt out for profiling provided. Opting out and using an alternative method should not place the user at a disadvantage in terms of service and user experience. For example, a medical centre deploying an A/IS appointments booking system should ensure that patients who are unable to access the A/IS or do not wish to do so are not placed at a disadvantage in terms of accessing and booking appointments. This may require setting periods of time for human operator availability to deal with telephone or face-to-face bookings, and advertising these times of availability to patients. Another area of concern is potential loss of business for businesses that opt out of using an A/IS appointments booking system, although this may be considered a choice and risk assumed by the business.

3. During-Use Stage

During A/IS use if there is a part of the A/IS operation which involves a "black box" scenario, that is, it is difficult for a human to discern what the system is doing and why, then appropriate risk-based parameters need to be set for the systems use (see Table 2).

Table 2. During-Use Stage Rights

Right	GDPR Provision	Convention 108+ Provision
To object to processing of data	Article 21	Article 9(1)(d)
To lawful, fair, and transparent processing of data	Articles 5(1)(a) and 6	Article 5(2), (3), (4)
To rectification of inaccurate data	Article 16	Article 9(1)(e)
To withdraw consent	Article 7(3)	Article 5(2)

As already mentioned under pre-use stage, Article 9(1)(d) of Convention 108+ allows the data subject to object at any time to the processing of personal data, including during-use stage. A similar provision exists under Article 21 of the GDPR. However, if consent has already been given for data processing then withdrawal of consent rather than objection to data processing would be most appropriate at the during-use stage.[24] There is a right to lawful, fair, and transparent processing of personal data under Articles 5(1)(a) of the GDPR and Articles 5(2)-(4) of Convention 108+. Article 6(1)(a)-(f) of the GDPR sets out conditions which will make the processing lawful (e.g. data subject's consent; necessary for performance of a contract;

compliance with legal obligations; necessary to protect data subject's or another natural person's vital interests; necessary for performance of a public interest task; necessary for pursuing legitimate interests of data controller or third party). During A/IS operation the user may become aware of inaccuracy in the data held or used in relation to them, in which case they must be able to seek rectification of the inaccuracy or error. Article 16 of the GDPR provides the data subject with the right to obtain from the data controller, without undue delay, the rectification of inaccurate personal data, including having incomplete personal data completed. Article 9(1)(e) of Convention 108+ provides for the data subject's right to obtain, on request, free of charge and without excessive delay, rectification or erasure of such data if these *are being* processed contrary to the Convention.

Withdrawal of consent can occur at any time including during-use stage, and Article 7(3) of the GDPR provides a specific right to the data subject to withdraw consent at any time. Although Convention 108+ does not refer to a specific right to withdraw consent, under Article 5(2) it establishes two prerequisites in order to make data processing lawful: either there is consent by the data subject, or there is provision in law for such data processing. As a result, if the data subject consents to data processing they may also withdraw such consent at any time.[25] Whether withdrawing consent under the GDPR or Convention 108+, the lawfulness of data processed prior to the withdrawal will not be affected but continuation of data processing will not be allowed, unless justifiable for some other purpose provided under EU law or EU Member State law, or national law. The key difference between the two instruments is that the GDPR requires a pre-use stage notification to the data subject of their right to withdraw consent.

4. Post-Use Stage

Post-use requires users to be aware of how their data and information shared with the A/IS will be used by the system and any third parties, as well as providing redress mechanisms for errors and harm caused. (see Table 3).

Table 3. Post-Use Stage Rights

Right	GDPR Provision	Convention 108+ Provision
To rectification of inaccurate data	Article 16	Article 9(1)(e)
To an explanation of automated decision	Recital 71	
To obtain human intervention	Article 22(3)	

Table 3. Post-Use Stage Rights

Right	GDPR Provision	Convention 108+ Provision
To express a point of view	Article 22(3)	Article 9(1)(a)
To contest the automated decision	Article 22(3)	Article 9(1)(f)

As with during-use stage, an A/IS user may become aware post-use that there are inaccuracies or errors in the data used in relation to them perhaps leading to an unfair, unlawful, or unreasonable decision. Article 16 of the GDPR provides the data subject with the right to obtain from the data controller, without undue delay, the rectification of inaccurate personal data, including having incomplete personal data completed. Article 9(1)(e) of Convention 108+ provides for the data subject's right to obtain, on request, free of charge and without excessive delay, rectification or erasure of such data if these *have been* processed contrary to the Convention.

A/IS users must have means to contest, challenge, or dispute an A/IS decision or any aspect of interaction with the A/IS. The means of contestation, challenge, or dispute should be readily available and provide a clear complaints procedure that provides all relevant information to a human complaint handler. Recital 71 of the GDPR refers to the right to obtain an explanation of the decision reached after an automated decision-making assessment, and the right to challenge the decision. In the case of contract or consent exceptions to the right not to be subject to automated decision-making, Article 22(3) of the GDPR recognises as minimum safeguards the data subject's rights to obtain human intervention, to express their point of view, and to contest the automated decision. In the context of A/IS users, the right to obtain human intervention can be interpreted as applying at the pre-use and during-use stages (e.g. provision of alternative method of interaction; access to human agent to query or rectify an operational issue). Similar provisions exist under Convention 108+. Article 9(1)(a) contains the right of the data subject to express their view in relation automated decision-making. Article 9(1)(f) provides the right to a remedy where the data subject's rights under the Convention have been violated.

5. Conclusion

It is clear from the GDPR and Convention 108+ provisions that emphasis is on a HCA closely aligned with a TBA that promotes ethical A/IS design, development, and deployment within definable and enforceable rights. Viewed from the perspective of user-system lifecycle stages, these rights can be

operationalised and protected. Some differences exist between the GDPR and Convention 108+. At the pre-use stage, only the GDPR contains a user right to be notified prior to their consent that they have the right to withdraw consent at any time; only the GDPR contains a right to information on the significance and envisaged consequences of automated decision-making processing. Regarding the right to object to processing of data, both the GDPR and Convention 108+ contain provisions, although there is some debate as to whether Article 21 of the GDPR applies to automated decision-making. At the during-use stage, the same issue regarding the right to object exists. At the post-use stage, only the GDPR provides for a right to explanation, and a right to obtain human intervention. These differences require further analysis to determine whether they result in material impact on the existence or effect of rights.

References

1. Respect for human autonomy is one of four ethical principles established under the EU AI Guidelines - *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence (EU AI HLEG), European Commission, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/2, last accessed 2020/02/03, p. 12; cf. Articles 32 (which implicitly predicates the security framework for data processing on guaranteeing the human dignity of natural persons), and 88(2) (which refers to safeguarding the data subject's human dignity in the processing of data for employment purposes) of the European Parliament and Council of the European Union, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), (OJ L 119, 4.5.2016), 27 April 2016; Preamble of the Council of Europe Modernised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108+), Amending Protocol to the Convention, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018 (Convention 108+) (which refers to securing human dignity and personal autonomy, and predicates the legal framework on safeguarding these).
2. Human agency and oversight represents a key requirement to implement the ethical principle of human autonomy under the EU AI HLEG, pp. 15-16; cf. Principle (d) of the 2019 Guiding Principles on Lethal Autonomous Weapons Systems by the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems (UNGGE Principles), https://undocs.org/en/CCW/GGE.1/2019/3, last accessed 2020/02/03, which refers to "the operation of such systems within a responsible chain of human command and control"; Preamble of Convention 108+ (which refers to a person's right to control their personal data and the processing of it).
3. Privacy and data governance represents a key requirement to implement the ethical principle of prevention of harm under the EU AI HLEG, pp. 17; cf. Recital 116, Articles 1(2), 12-18, 20, 21, and 22 GDPR; Preamble and Article 1 of Convention 108+; Principles 1 and 3 of 2019 IEEE Ethically Aligned Design for Autonomous and Intelligent Systems - *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (Final version, 4 April 2019) (IEEE EAD), pp. 19-20, 23-24, https://ethicsinaction.ieee.org, last

accessed 2020/02/03; IEEE P7002, IEEE Standards Project for Data Privacy Process, https://standards.ieee.org/project/7002.html, last accessed 2020/02/03.

4. Prevention of harm is the second ethical principle established under the EU AI HLEG, p. 12; generally expressed as violations of privacy and data protection rules under the GDPR; generally expressed as interference with the fundamental rights and freedoms of the individual under Convention 108+.
5. Fairness is the third ethical principle established under the EU AI HLEG, p. 12; cf. Recitals 39, 60, and 71, Articles 5(1)(a), 13(2), and 14(2) GDPR; Articles 5(4)(a) and 8(1) of the Council of Europe Modernised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108+), Amending Protocol to the Convention, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018 (Convention 108+).
6. Recitals 39, 58, 60, and 71, Articles 5(1)(a) and 12(1) GDPR; cf. Articles 5(4)(a), 8, and 9(b) Convention 108+; Principle 5 IEEE EAD, pp. 27-28; IEEE P7001, IEEE Standards Project for Transparency of Autonomous Systems, https://standards.ieee.org/project/7001.html, last accessed 2020/02/03.
7. Explicability, as the fourth ethical principle established under the EU AI HLEG, p. 13, is closely associated with auditability particularly where it concerns "black box" scenarios; cf. GDPR transparency provisions, and safeguarding measures under Article 22; Article 9(1)(c) Convention 108+; generally considered under Principle 5 IEEE EAD.
8. Accountability represents a key requirement to implement the ethical principle of fairness under the EU AI HLEG, pp. 19-20; cf Article 5(2) GDPR; Principle 6 IEEE EAD, pp. 29-30.
9. Legal responsibility is subsumed in the accountability requirement under the EU AI HLEG, pp. 19-20; Recitals 74 and 79, Article 24 GDPR; Article 15(1) Convention 108+; Principle 6 IEEE EAD.
10. 2018 UK House of Lords Select Committee AI Report - *AI in the UK: ready, willing and able?* (16 April 2018), https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf, last accessed 2020/02/03; 2018 China's AI Standardisation White Paper - *China's White Paper on Artificial Intelligence Standardisation* (January 2018, Standards Administration of China) - 人工智能标准化白皮书（白皮书）（2018年1月，中国标准管理局; 2018 Canada's White Paper on Responsible AI in Government - *Responsible Artificial Intelligence in the Government of Canada* (Digital Disruption White Paper Series, Version 2.0, 2018-04-10); 2019 EU AI Guidelines - *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence (AI HLEG), European Commission, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/2, last accessed 2020/02/03; 2016 EU Study on Civil Law Rules in Robotics - *European Civil Law Rules in Robotics* (October 2016), PE 571.379, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf, last accessed 2020/02/03; 2017 EU Parliament Resolution for further study on the implications of creating legal status for robots - *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)); 2019 IEEE Ethically Aligned Design for Autonomous and Intelligent Systems - *The IEEE Global Initiative on Ethics ofAutonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (Final version, 4 April 2019), https://ethicsinaction.ieee.org, last accessed 2020/02/03; 2019 Guiding Principles on Lethal Autonomous Weapons Systems by the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems, https://undocs.org/en/CCW/GGE.1/2019/3, last accessed 2020/02/03.

11. European Parliament and Council of the European Union, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), (OJ L 119, 4.5.2016), 27 April 2016.
12. Council of Europe Modernised Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108+), Amending Protocol to the Convention, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018 (Convention 108+).
13. Cf. Wachter, S., Mittelstadt, B., Floridi, L.: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law 7(2), 78 (2017); Malgieri, G., Comandé, G.: Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. International Data Privacy Law 7(4), 265 (2017).
14. Under GDPR Article 4(4) "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."
15. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* ("WP Guidelines"). The WP Guidelines were endorsed by the European Data Protection Board in May 2018, p. 21, https://edpb.europa.eu/node/71, last accessed 2020/01/31.
16. WP Guidelines, p. 21.
17. GDPR Article 9(1).
18. GDPR Article 9(2)(a).
19. GDPR Article 9(2)(g).
20. Convention 108+ Convention for the protection of individuals with regard to the processing of personal data (Council of Europe, June 2018), Explanatory Report (Convention 108+ Explanatory Report), pp. 19-20, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1, last accessed 2020/01/31.
21. See examples of practical application of these different interpretations to the information needed: *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (European Commission Final Report, Directorate-General for Justice and Consumers, October 2018), pp. 45-47.
22. WP Guidelines, pp. 34-35.
23. WP Guidelines, p. 26.
24. Convention 108+ Explanatory Report, p. 24.
25. Convention 108+ Explanatory Report, p. 20.