Unboxing Artificial Intelligence: 10 steps to protect Human Rights

Recommendation

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Unboxing Artificial Intelligence: 10 steps to protect Human Rights

By the Council of Europe
Commissioner for Human Rights

2019

Council of Europe

Acknowledgements:

The Commissioner would like to express her gratitude to Nani Jansen Reventlow, human rights lawyer and Director of the Digital Freedom Fund, and Jonathan McCully, independent consultant and Legal Adviser to the Digital Freedom Fund, for their invaluable assistance and expertise in preparing this Recommendation.

Cover photo:
© Shutterstock.com

Printed at the Council of Europe

Contents

Introduction

The impact of Artificial Intelligence (AI) on human rights is one of the most crucial factors that will define the period in which we live. AI-driven technology is entering more aspects of every individual's life, from smart home appliances to social media applications, and it is increasingly being utilised by public authorities to evaluate people's personality or skills, allocate resources, and otherwise make decisions that can have real and serious consequences for the human rights of individuals. As stressed by the Commissioner for Human Rights in a Human Rights Comment, finding the right balance between technological development and human rights protection is therefore an urgent matter.

In accordance with the mandate of the Commissioner for Human Rights to promote the awareness of and effective observance and full enjoyment of human rights in Council of Europe member states as well as to provide advice and information on the protection of human rights (Articles 3 and 8 of Resolution (99) 50 of the Committee of Ministers), the Commissioner issues this 10-point Recommendation on AI and human rights.

There is currently no agreed definition of "Artificial Intelligence". However, for the purposes of this Recommendation, AI is used as an umbrella term to refer generally to a set of sciences, theories and techniques dedicated to improving the ability of machines to do things requiring intelligence. An AI system is a machine-based system that makes recommendations, predictions or decisions for a given set of objectives. It does so by: (i) utilising machine and/or human-based inputs to perceive real and/or virtual environments; (ii) abstracting such perceptions into models manually or automatically; and (iii) deriving outcomes from these models, whether by human or automated means, in the form of recommendations, predictions or decisions.

A list of further relevant terminology used in this Recommendation can be found in the Glossary in the Annex.

AI involves opportunities as well as risks; human rights should be strengthened by AI, not undermined. This Recommendation on AI and human rights provides guidance on the way in which the negative impact of AI systems on human rights can be prevented or mitigated, focusing on 10 key areas of action.

The Recommendation builds on work done in this area by the Council of Europe, in particular the European Ethical Charter on the use of artificial intelligence in judicial systems, the Guidelines on Artificial Intelligence and Data Protection, the Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes and the Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, as well as the report of the United Nations Special Rapporteur on the promotion and protection of the freedom of opinion and expression, addressing the implications of artificial intelligence technologies for human rights in the information environment. It is rooted in the existing universal, binding and actionable framework provided by the international human rights system, including the human rights instruments of the Council of Europe.

The Recommendation is addressed at member states, but the principles concern anyone who significantly influences – directly or indirectly – the development, implementation or effects of an AI system. AI developed in the private sector should be held to the same standards as that developed in the public sector if and when there is any intention to work with public bodies and public services.

The annexed checklist identifies actionable points for each key area, providing general guidance on operationalising the recommendations.

Recommendations

1 - Human rights impact assessment

Member states should establish a legal framework that sets out a procedure for public authorities to carry out human rights impact assessments (HRIAs) on AI systems acquired, developed and/or deployed by those authorities. HRIAs should be implemented and operationalised in a similar vein as other forms of impact assessment conducted by public authorities, such as Regulatory Impact Assessments and Data Protection Impact Assessments.

Member states may delineate the types of AI system that are subject to HRIAs under the law, but such delineations must be comprehensive enough to cover all AI systems that have the potential to interfere with an individual's human rights at any stage of the AI system lifecycle.

As part of the HRIA legal framework, public authorities should be required to conduct a self-assessment of existing and proposed AI systems. This self-assessment should evaluate the potential impact of the AI system on human rights taking into account the nature, context, scope, and purpose of the system. Where a public authority has not yet procured or developed a proposed AI system, this assessment must be carried out prior to the acquisition and/or development of that system.

The HRIAs must also include a meaningful external review of AI systems, either by an independent oversight body or an external researcher/auditor with relevant expertise, in order to help discover, measure and/or map human rights impacts and risks over time. Public bodies should consider involving National Human Rights Structures (NHRSs) in carrying out this meaningful external review.

Self-assessments and external reviews should not be limited to an evaluation of the models or algorithms behind the AI system, but should include an evaluation of how decision-makers might collect or influence the inputs and interpret the outputs of such a system. It should also include an assessment of whether an AI system remains under meaningful human control throughout the AI system's lifecycle.

In circumstances where the self-assessment or external review discloses that the AI system poses a real risk of violating human rights, the HRIA must set out the measures, safeguards, and mechanisms envisaged for preventing or mitigating that risk. In circumstances where such a risk has been identified in relation to an AI system that has already been deployed by a public authority, its use should be immediately suspended until the abovementioned measures, safeguards and mechanisms have been adopted. Where it is not possible to meaningfully mitigate the identified risks, the AI system should not be deployed or otherwise used by any public authority. Where the self-assessment or external review discloses a violation of human rights, the public authority must act immediately to address and remedy the violation and adopt measures to prevent or mitigate the risk of such a violation occurring again.

The HRIAs, including research findings or conclusions from the external review process, must be made available to the public in an easily accessible and machine-readable format.

Public authorities should not acquire AI systems from third parties in circumstances where the third party is unwilling to waive restrictions on information (e.g. confidentiality or trade secrets) where such restrictions impede or frustrate the process of (i) carrying out HRIAs (including carrying out external research/review), and (ii) making HRIAs available to the public.

Public authorities should be required to conduct HRIAs on a regular basis, and not only at the point where public authorities acquire and/or develop AI systems. HRIAs should, at the very least, be undertaken at each new phase of the AI system lifecycle and at similarly significant milestones.

2 - Public consultations

State use of AI systems should be governed by open procurement standards, applied in a transparently run process, in which all relevant stakeholders are invited to provide input. Member states should consider updating their access to information, open government, and public procurement laws and policies to reflect AI-specific requirements.

Member states should allow for public consultations at various stages of engaging with an AI system, and at a minimum at the procurement and HRIA stages. A meaningful public consultation process entails timely and prior publication of all relevant information on the AI system that facilitates a proper understanding of its operation, function, and potential or measured impacts. Consultations should provide an opportunity for all stakeholders, including state actors, private sector representatives, academia, the non-profit sector, the media and representatives from marginalised and affected

groups or communities, to provide input. NHRSs act as a bridge between civil society and state authorities and can help conduct meaningful consultations.

3 - Obligation of member states to facilitate the implementation of human rights standards in the private sector

Member states should effectively implement the UN Guiding Principles on Business and Human Rights and the Recommendation CM/Rec(2016)3 of the Committee of Ministers to member states on human rights and business. They should do so in a non-discriminatory manner with due regard to gender-related risks. In addition, they should set out clearly the expectation that all AI actors (e.g. AI creators, owners, manufacturers, managers, service providers and other AI enterprises) who are domiciled or operate within their jurisdiction, should likewise implement these principles throughout their operations.

In order to comply with their positive and procedural obligations under the European Convention on Human Rights, member states should apply such measures as may be necessary to protect the human rights of individuals against violations by AI actors throughout AI systems' entire lifecycle. Member states should specifically ensure that their legislation creates conditions that are conducive to the respect for human rights by AI actors and do not create barriers to effective accountability and remedy for AI-related human rights violations.

Member states should apply additional measures to require AI actors to respect human rights, including, where appropriate, by carrying out human rights due diligence. Member states should require AI actors to take effective action to prevent and/or mitigate the harms posed by their AI systems, and AI actors should be transparent about efforts to identify, prevent, and mitigate the harms posed by their AI systems. Member states should provide for adequate consequences if identified risks of adverse human rights impacts are not duly mitigated and addressed.

4 - Information and transparency

The use of an AI system in any decision-making process that has a meaningful impact on a person's human rights needs to be identifiable. The use of an AI system must not only be made public in clear and accessible terms, individuals must also be able to understand how decisions are reached and how those decisions have been verified.

If an AI system is used for interaction with individuals in the context of public services, especially justice, welfare, and healthcare, the user needs to be notified and the possibility of recourse to a professional upon request and without delay must be communicated. Those who have had a decision made about them by a public authority that is solely or significantly informed by the output of an AI system should be notified and be promptly provided with the aforementioned information.

Oversight over an entire AI system must also be enabled by transparency requirements. This can be either in the form of public disclosure of information on the system in question, its processes, direct and indirect effects on human rights, and measures taken to identify and mitigate against adverse human rights impacts of the system, or in the form of an independent, comprehensive, and effective audit. In all cases, the information made available should allow for meaningful assessment of the AI system. No AI system should be complex to the degree it does not allow for human review and scrutiny. Systems that cannot be subjected to appropriate standards of transparency and accountability should not be used.

5- Independent oversight

Member states should establish a legislative framework for independent and effective oversight over the human rights compliance of the development, deployment and use of AI systems by public authorities and private entities. This legislative framework may include mechanisms that consist of a combination of administrative, judicial, quasi-judicial and/or parliamentary oversight bodies effectively cooperating with each other. Member States should consider empowering, where appropriate, existing NHRSs so they can perform a role in providing independent and effective oversight over the human rights compliance of AI systems.

Oversight bodies should be independent of the public authorities and private entities developing, deploying or otherwise using the AI systems, and they must be equipped with appropriate and adequate inter-disciplinary expertise, competencies and resources to carry out their oversight function.

Independent oversight bodies should proactively investigate and monitor the human rights compliance of AI systems, receive and handle complaints from affected individuals, carry out periodic reviews of AI system capabilities and technological developments more generally. They should have the power to intervene in circumstances where they identify (a risk of) human rights violations occurring. They should also regularly report to parliament and publish reports about their activities.

Public authorities and private parties should be required to provide all the information necessary for effective oversight of AI systems upon request and regularly report to the oversight bodies. They should implement oversight bodies' recommendations regarding human rights impacts of AI systems. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review.

6 - Non-discrimination and equality

In all circumstances, discrimination risks must be prevented and mitigated with special attention for groups that have an increased risk of their rights being disproportionately impacted by AI. This includes women, children, older people, economically disadvantaged persons, members of the LGBTI community, persons with disabilities, and "racial", ethnic or religious groups. Member states must refrain from using AI systems that discriminate or lead to discriminatory outcomes and, within their jurisdiction, protect individuals from the consequences of use of such AI systems by third parties.

The active participation of and meaningful consultation with a diverse community that includes effective representation from these groups in all stages of the AI lifecycle is an important component of prevention and mitigation of adverse human rights impacts. In addition, special attention needs to be paid to transparency and accessibility of information on the training data used for the development of an AI system. HRIAs and other forms of human rights due diligence should be repeated at regular intervals and appropriate and accessible avenues for accountability and redress made available.

Member states should apply the highest level of scrutiny when using AI systems in the context of law enforcement, especially when engaging in methods such as predictive or preventive policing. Such systems need to be independently audited prior to deployment for any discriminatory effect that could indicate de facto profiling of specific groups. If any such effects are detected, the system cannot be used.

7 - Data protection and privacy

The development, training, testing and use of AI systems that rely on the processing of personal data must fully secure a person's right to respect for private and family life under Article 8 of the European Convention on Human Rights, including the "right to a form of informational self-determination" in relation to their data.

Data processing in the context of AI systems shall be proportionate in relation to the legitimate purpose pursued through such processing, and should at all stages of the processing reflect a fair balance between the interests pursued through the development and deployment of the AI system and the rights and freedoms at stake.

Member states should effectively implement the modernised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+") as well as any other international instrument on data protection and privacy that is binding on the member state. The processing of personal data at any stage of an AI system lifecycle must be based on the principles set out under the Convention 108+, in particular (i) there must be a legitimate basis laid down by law for the processing of the personal data at the relevant stages of the AI system lifecycle; (ii) the personal data must be processed lawfully, fairly and in a transparent manner; (iii) the personal data must be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; (iv) the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; (v) the personal data must be accurate and, where necessary, kept up to date; (vi) the personal data should be preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

Member states should introduce a legislative framework that provides appropriate safeguards where AI systems rely on the processing of genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data; personal data relating to "racial" or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life. Such safeguards must also provide protection against this data being processed in a discriminatory or biased way.

8 - Freedom of expression, freedom of assembly and association, and the right to work

In the context of their responsibility to respect, protect and fulfil every person's human rights and fundamental freedoms, member states should take into account the full spectrum of international human rights standards that may be engaged by the use of AI.

Freedom of expression: Member states should be mindful of the obligation to create a diverse and pluralistic information environment and the adverse impact AI-driven content moderation and curation can have on the

exercise of the right to freedom of expression, access to information, and freedom of opinion. Member states are also encouraged to consider taking appropriate measures to regulate technology monopolies to prevent the adverse effects of concentration of AI expertise and power on the free flow of information.

Freedom of assembly and association: Special attention should be paid to the impact the use of AI systems in content moderation can have on the freedom of assembly and association, especially in contexts where these freedoms are difficult to exercise offline. The use of facial recognition technology should be strictly regulated by member states, including through legislation setting out clear limitations for its use, and public transparency to protect the effective exercise of the right to freedom of assembly.

Right to work: The potential of AI to accelerate automation and thereby negatively impact the availability of work should be carefully monitored. Regular assessments should be made to track the number and types of jobs created and lost due to AI developments. Adequate plans should be developed for reschooling and reassigning jobs to those workers clearly affected by a decrease in the demand for human labour. Member states should also adapt education curricula to ensure access to jobs requiring competences related to AI systems.

9 - Remedies

AI systems must always remain under human control, even in circumstances where machine learning or similar techniques allow for the AI system to make decisions independently of specific human intervention. Member states must establish clear lines of responsibility for human rights violations that may arise at various phases of an AI system lifecycle. Responsibility and accountability for human rights violations that occur in the development, deployment or use of AI Systems must always lie with a natural or legal person, even in cases where the measure violating human rights was not directly ordered by a responsible human commander or operator.

Anyone who claims to be a victim of a human rights violation arising from the development, deployment or use by a public or private entity of an AI system should be provided with an effective remedy before a national authority. Moreover, member states should provide access to an effective remedy to those who suspect that they have been subjected to a measure that has been solely or significantly informed by the output of an AI system in a non-transparent manner and without their knowledge.

Effective remedies should involve prompt and adequate reparation and

redress for any harm suffered by the development, deployment or use of AI systems, and may include measures under civil, administrative, or, where appropriate, criminal law. NHRSs can be such a source of redress, through rendering their own decisions in accordance with their respective mandates.

Member states should provide individuals with the right not to be subject to a decision significantly affecting them that is based on automated decision-making without meaningful human intervention. At the very least, an individual should be able to obtain human intervention in such automated decision-making and have their views taken into consideration before such a decision is implemented.

Member states must ensure that individuals have access to information in the possession of a defendant or a third party that is relevant to substantiating their claim that they are the victim of a human rights violation caused by an AI system, including, where relevant, training and testing data, information on how the AI system was used, meaningful and understandable information on how the AI system reached a recommendation, decision or prediction, and details of how the AI system's outputs were interpreted and acted on.

When national authorities consider challenges to human rights violations caused by the development, deployment or use of AI systems, they must show appropriate scepticism towards the "allure of objectivity" presented by AI systems and ensure that individuals challenging human rights abuses are not held to a higher standard of evidence compared to those responsible for the measure being challenged.

10 - Promotion of "AI literacy"

The knowledge and understanding of AI should be promoted in government institutions, independent oversight bodies, national human rights structures, the judiciary and law enforcement, and with the general public. Member states should consider establishing a consultative body within government to advise on all AI-related matters.

Those involved directly or indirectly in the development or application of AI systems need to have the necessary knowledge and understanding of how it functions and be informed about its impact on human rights. In order for such actors to be informed about the impact of their systems on human rights, they must also be made aware of the spectrum of human rights standards that might be engaged by their work.

Member states should invest in the level of literacy on AI with the general public through robust awareness raising, training, and education efforts,

including (in particular) in schools. This should not be limited to education on the workings of AI, but also its potential impact – positive and negative – on human rights. Particular efforts should be made to reach out to marginalised groups, and those that are disadvantaged as regards IT literacy in general.

Checklists

Human rights impact assessment

Do's
DO take steps to introduce laws and regulations requiring HRIAs to be conducted in relation to AI systems that have been or may be acquired, developed and/or deployed by public authorities. **DO** promptly carry out HRIAs in relation to all AI systems that have already been deployed/are already being used by any public authority at the time the relevant legal framework on HRIAs has been adopted. Otherwise, HRIAs must first be conducted prior to the acquisition and/or development of an AI system by a public authority. **DO** continuously monitor the implications of AI systems on human rights throughout their lifecycle, and carry out regular HRIAs at each new phase of the lifecycle and when there are changes in context, scope, nature and purpose of the systems.

Don'ts
DO NOT fail to meaningfully consult with and get input from relevant stakeholders, including civil society organisations and those with relevant expertise in AI and human rights, when introducing a legal framework on HRIAs. **DO NOT** conduct HRIAs in a non-transparent manner, and do not use or facilitate the use of laws on confidentiality, privacy, trade secrets, state secrecy, or intellectual property to frustrate the carrying out or publication of HRIAs. **DO NOT** acquire, develop, deploy or use an AI system that has the potential of interfering with human rights in circumstances where (i) it has not been subject to an HRIA, or (ii) an HRIA has disclosed that the AI system poses a real risk of violating human rights, and no measures, safeguards, or mechanisms have been adopted for preventing or mitigating the identified risks.

Public consultations

Do's
DO apply open procurement standards and a transparent process to the use of AI systems. **DO** include all stakeholders in public consultations, including the affected groups or communities, at a minimum during the procurement and HRIA stages.

Don'ts
DO NOT provide for public consultations without taking adequate measures to make them meaningful, including timely prior publication of all relevant information related to the AI system, and actively seeking the engagement of all relevant stakeholders.

Obligation of member states to facilitate the implementation of human rights standards in the private sector

Do's
DO carry out an audit of existing criminal and civil laws, as well as other equivalent liability regimes, to identify gaps or obstacles for holding AI actors to account for AI-related human rights violations. **DO** enforce existing laws where necessary to meet the state duty to protect the human rights of individuals against violations by AI actors. **DO** take steps to ensure AI actors "know and show" that they are meeting their responsibility to respect human rights, including through transparent human rights due diligence processes that involve the identification of the human rights risks associated with their AI systems, and taking effective action to prevent and/or mitigate the harms posed by such systems.

Don'ts
DO NOT treat laws, policies and regulations that are applicable to the AI sector as being isolated from, or uninformed by, the human rights obligations on member states. **DO NOT** facilitate the implementation and enforcement of human rights standards in the AI sector in a discriminatory manner.

Information and transparency	Do's
	DO provide all necessary information for individuals to understand when and how AI systems are being used, especially in the context of public services.

Don'ts
DO NOT use AI systems that are complex to a degree that they cannot be subjected to human review and scrutiny by appropriate standards of transparency and accountability.

Independent oversight

Do's
DO legislate for the establishment of a framework for independent and effective oversight over the human rights compliance of AI systems, drawing on existing oversight bodies including NHRSs where possible. **DO** take steps to ensure all relevant oversight bodies have access to sufficient expertise, have received appropriate training on AI systems and their implications for human rights, and have received adequate funding and other resources in order to carry out their functions effectively. **DO** ensure that the functions of the relevant oversight bodies are adequate for the purpose of investigating and monitoring all actors, whether public or private, that may be responsible for AI system human rights violations (including those that occur during their development, testing and use).

Don'ts
DO NOT limit the functions and powers of oversight bodies to such an extent that they are unable to meaningfully intervene in circumstances where they identify (a risk of) human rights violations occurring. **DO NOT** compromise the institutional, operational, financial and personal independence of the oversight bodies responsible for investigating and monitoring the human rights compliance of AI systems. **DO NOT** deprive, or allow others to deprive, oversight bodies of the information necessary for them to carry out their functions effectively, including by depriving them of access to (training and testing) datasets, AI inputs/outputs, models/algorithms, operational guidance and human rights due diligence.

Non-discrimination and equality

Do's
DO prevent and mitigate discrimination risks of the use of AI systems for groups that have an increased risk of their rights being disproportionately impacted by it. **DO** apply the highest level of scrutiny when using AI systems in the context of law enforcement, especially to avoid profiling of individuals belonging to specific groups.

Don'ts
DO NOT use AI systems or allow third parties to use AI systems that discriminate or lead to discriminatory outcomes

Data protection and privacy

Do's
DO carry out a review and assessment of existing data protection laws to determine whether they sufficiently protect the right to respect for private life and the right to data protection in the context of AI systems, and institute legal reform where they do not. **DO** proactively take steps to ensure that private and public entities involved in developing, deploying and using AI systems respect data subjects' rights and meet their obligations under applicable data protection laws.

Don'ts
DO NOT provide broad and disproportionate data processing exemptions or immunities to those who develop, deploy or use AI systems. **DO NOT** permit the development or use of AI systems that rely on training or testing datasets that have been collected or otherwise processed in violation of the right to respect for private life and the right to data protection. **DO NOT** permit the development or use of AI systems that process personal data, either as input or output data, in violation of the right to respect for private life and the right to data protection.

Freedom of expression, freedom of assembly and association, right to work

Do's
DO take into account the full range of international human rights standards potentially engaged by the use of AI.
DO be mindful of the impact AI-driven content moderation and curation can have on the exercise of the right to freedom of expression, access to information, and freedom of opinion.
DO strictly regulate the use of facial recognition technology to allow effective exercise of the right to freedom of assembly.
DO monitor the potential negative impact of AI on the right to work and plan for mitigation, including through schooling.

Don'ts
DO NOT permit or facilitate the development, deployment or use of AI systems that violate any of the human rights protected under international human rights standards.

Remedies

Do's
DO carry out an assessment of existing laws, including civil, criminal and administrative laws, and institute reform where those laws do not provide an effective remedy to those claiming to be a victim of a human rights violation arising from the development, deployment or use of an AI system. **DO** ensure that liability regimes clearly establish who is legally responsible for the whole spectrum of human rights violations that may occur at each phase of an AI system's lifecycle. **DO** ensure that the judiciary and other relevant national authorities do not place inappropriate weight on the assumed/perceived accuracy or objectivity of an AI system, and that they provide an equality of arms between the victim and the defendant in cases challenging human rights violations caused by AI systems.

Don'ts
DO NOT permit the development, deployment or use of AI systems that operate wholly outside of any human control. **DO NOT** allow for individuals to be subject to an automated decision that significantly affects them in circumstances where they have not been provided with an opportunity to obtain meaningful human intervention and have not had their views taken into consideration before the decision has been implemented.

Promotion of AI literacy

Do's
DO establish a consultative government body to advise on AI-related matters. **DO** promote knowledge and understanding of AI and human rights for all, ranging from those involved in the development of AI systems, to the general public.

Don'ts
DO NOT limit AI literacy efforts to technological aspects without including its potential impact on human rights.

Annex
Definitions

For the purpose of this Recommendation, the following terms should be understood as follows:

Algorithm: A finite suite of formal rules/commands, usually in the form of a mathematical logic, that allows for a result to be obtained from input elements.

Artificial Intelligence (AI): An umbrella term that is used to refer to a set of sciences, theories and techniques dedicated to improving the ability of machines to do things requiring intelligence.

AI system: A machine-based system that can make recommendations, predictions or decisions for a given set of objectives. It does so by utilising machine and/or human-based inputs to: (i) perceive real and/or virtual environments; (ii) abstract such perceptions into models manually or automatically; and (iii) use model interpretations to formulate options for outcomes.

AI system lifecycle: A set of phases concerning an AI system that involve: (i) planning and design, data collection and processing, and model building; (ii) verification and validation; (iii) deployment; (iv) operation and monitoring; and (v) end of life.

Automated decision-making: A process of making a decision by automated means. It usually involves the use of automated reasoning to aid or replace a decision-making process that would otherwise be performed by humans. It does not necessarily involve the use of AI but will generally involve the collection and processing of data.

Machine learning: A field of AI made up of a set of techniques and algorithms that can be used to "train" a machine to automatically recognise patterns in a set of data. By recognising patterns in data, these machines can derive models that explain the data and/or predict future data. In summary, it is a machine that can learn without being explicitly programmed to perform the task.

Model: An actionable representation of all or part of the external environment of an AI system that describes the environment's structure and/or dynamics. The model represents the core of an AI system. A model can be based on data and/or expert knowledge, by humans and/or by automated tools like machine learning algorithms.

Personal data: Information relating to an identified or identifiable natural person, directly or indirectly, by reference to one or more elements specific

to that person. S*ensitive personal data* concern personal data relating to "racial" or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data, data concerning health or concerning sex life or sexual orientation.

Personal data processing: Any operation or set of operations performed or not using automated processes and applied to personal data or sets of data, such as collection, recording, organisation, structuring, storage, adaptation or modification, retrieval, consultation, use, communication by transmission, dissemination or any other form of making available, linking or interconnection, limitation, erasure or destruction.