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

VIENNA +30 OUR RIGHTS FUTURE

ICHROP
HUMAN RIGHTS OF OLDER PERSONS 2023

Data Protection and AI Regulation – *Examples for tackling normative gaps in the digital human rights framework of older people*

29 November - 01 December 2023, Vienna

Introduction

- Rapid Ageing of world population
- Ageing does not necessarily make individuals more vulnerable →but several physical, political, economic, and social factors contribute to challenges faced by them in enjoying their human rights (OHCHR report 2022)
- **New challenge:** "clash" of global ageing with the technological / digital developments

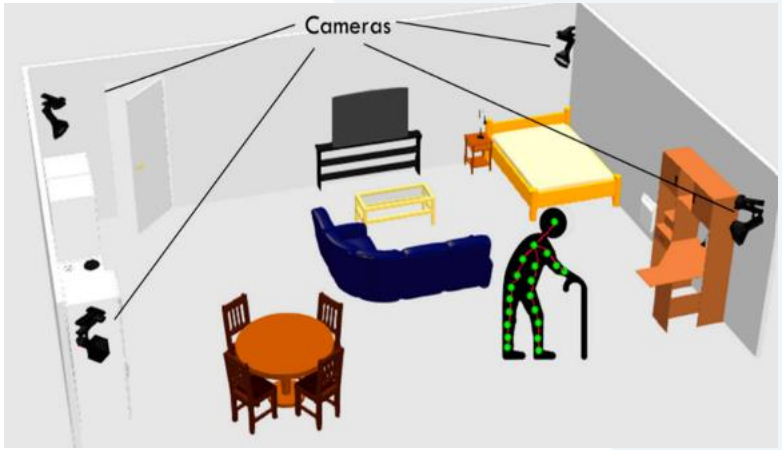
Barbara Mikolajczyk, "Universal human rights instruments and digital literacy of older persons", in: *The International Journal of Human Rights*, Vol. 27 No. 3 (2023), 403-424, https://doi.org/10.1080/13642987.2022.2131772
OHCHR report *Normative standards and obligations under international law in relation to the promotion and protection of the human rights of older persons* (A/HRC/49/70, January 2022)
https://www.bmfsfj.de/resource/blob/159708/ed236ad230d6038b9f0a439fb03ddf3cb/achter-altersbericht-kurzfassung-englisch-data.pdf

Use cases – a selection

ElliQ

Source: Intuition Robotics – ElliQ (https://elliq.com/)

Image processing based fall detection system



Source: Wang et al., „Possible Life Saver: A Review on Human Fall Detection Technology", in: *Robotics Vol. 9 No. 55* (2020), 1-19, doi:10.3390/robotics9030055

Normative Gaps?

- OHCHR report (2022): Existing norms and procedures are missing concerning older persons‘ human rights because
  - Are spread across many different documents and
  - Are narrow in idea and approach →limited effectiveness

- **Challenges:**
  - **Rights of older persons ⇔ digital rights**
  - **Legally binding ⇔ soft law**
  - **No global legally binding data protection and AI regulation**

- *UDHR, ICESCR, EU-Charter (CFR), ECHR, CEDAW, UN CRPD,…*
- *United Nations Principles for Older Persons (1991)*
- *The Madrid Plan of Action on Ageing (2002)*
- *European Council conclusions on Human Rights and Well-Being of Older Persons in the Era of Digitalisation (2020)*
- *European Declaration on Digital Rights and Principles for the Digital Decade (2023)*
- *GDPR and AI Act*
- *AUT: Data Protection Act and recommendations of monitoring bodies (e.g. NPM commissions)*

Good practice for horizontal human rights protection – The EU General Data Protection Regulation (GDPR)

- Data protection is the precondition for
  - functioning of a free and democratic society
  - enjoyment of various other fundamental rights
- Data protection as „catalyst" for human rights protection
- Legislative duty to protect (EU)
- GDPR fully applicable since 2018
- Lays down data protection rules
- Strengthens fundamental rights
- Promotes higher due diligence rules
- Stronger accountability (also includes immaterial damage)

- **Art 6**: Lawfulness of processing →*based on exemption clauses*
- **Art 9**: Processing of special categories of personal data *(e.g. health data)*
- **Chapter 3**: Rights of the data subject
- **Art 35:** Data Protection Impact Assessment – *mandatory for high risk systems*

The GDPR and older persons

- Does not explicitly refer to the rights of older persons
- However, it protects the personal data of all natural persons
- Covered by general provisions on data protection, non-discrimination, and protection of vulnerable individuals

- **Recital 1: Data Protection as a Fundamental Right**
- **Recital 2: Respect of the Fundamental Rights and Freedoms**
- **Recital 4: Data Protection in Balance with Other Fundamental Rights**
- **Recital 58: The Principle of Transparency**
- **Recital 75: Risk to the Rights and Freedoms of Natural Persons**
  - The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to **discrimination,**[…];
  - […] where personal data of **vulnerable natural persons** […] are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Foundations of data protection

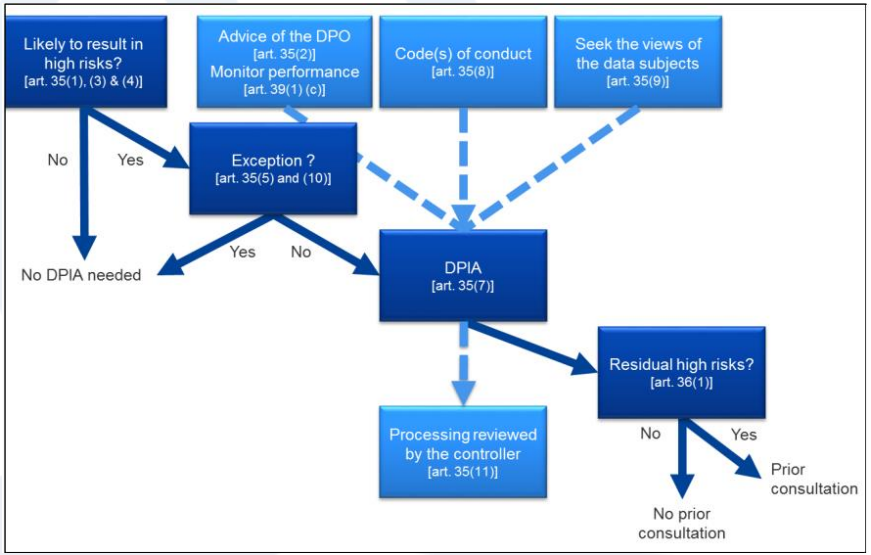
- **Personal data needs to be processed lawfully in any case! (Art 6 GDPR)**
  - **Challenges:** Sometimes, several legal justifications are possible; numerous legal systems outside the EU are more liberal providing less detailed regulation on the national level
  - **Principles** relating to processing of personal data (Art 5 GDPR)
  - **Data protection impact assessment** (Art 35 GDPR)
    - processing of personal data likely resulting in a high risk

Data Protection Impact Assessment - Overview

- Art 35 GDPR →implementation of privacy by design and privacy by default (Art 25 GDPR)
- „Processing operations that may result in a high risk to the rights and freedoms of natural persons" *→risk-based approach*
- Required in case of e.g.:
  - Art 35 (3) b: processing on a large scale of special categories of data referred to in Art 9 (1)
- If Art 35 not applicable → still risk analysis to adequately implement Art 25 and 32 GDPR

Source: https://www.lboro.ac.uk/data-privacy/resources/dpia/dpia-process

Article 29 Data Protection Working Party – Guidelines on high risk data processing



High risk exists if at least two of the following nine criteria are met:

- Evaluation or scoring (profiling/predicting) of natural persons
- Automated-decision making with legal or similar significant effect
- Systemic monitoring
- **Sensitive data or data of highly personal nature (Art 9,10) – *linked to household, private activities or impact on exercise of fundamental right***
- Data processed on a large scale (Recital 91)
- Matching or combining datasets
- **Data concerning vulnerable data subjects (Recital 75) →*special reference to „the elderly*"**
- **Innovative use of applying new technological or organisational solutions (e.g. AI)**
- When the processing itself prevents data subjects from exercising a right or using a service or a contract (Art 22, Recital 91)

Possible solutions – *not exhaustive*

- **Anonymisation**
  - all identifiable elements are removed from a set of personal data so that the data subject is no longer identifiable. If successful →principles of data protection do not apply
  - Different procedures
  - ! Possibility of Re-identification is increasing with available technology (anonymisation is difficult!)

- **Pseudonymisation (Art 25, Recital 28)**
  - Part of data protection by design and by default
  - „appropriate technical and organisational measures"
  - Can reduce the risks to the data subjects, but does not preclude other measures of data protection
  - Principles of data protection do apply!

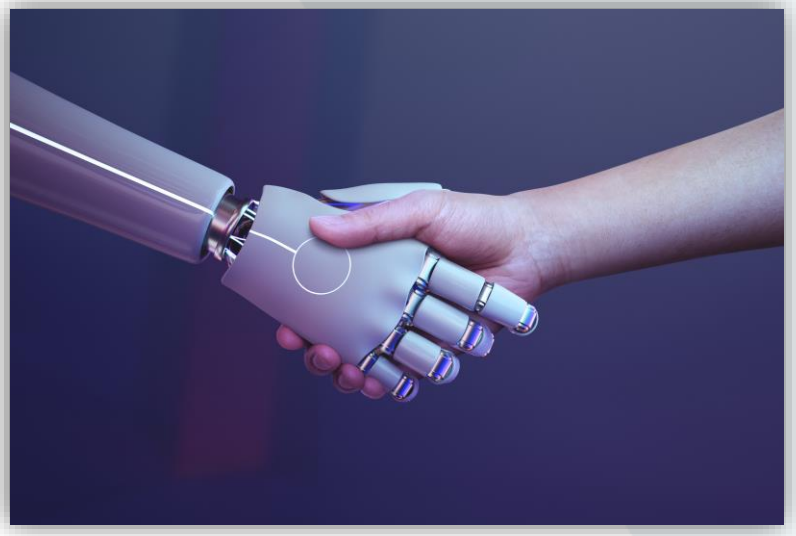
- **Use of less invasive technology** (e.g. deployment of ambient sensing fall detection system instead of image processing based fall detection system; edge computing)

- Privacy by Design (Art 25) and DPIA (Art 35) are to be observed by the **threat of punishment** with 10 million Euros or 2% of the annual turnover, even if nothing concretely happened with the data **(Art 83 (4) GDPR)**

Artificial Intelligence (AI)

Areas of tension

- Accountability ⇔ Trust
- Safety ⇔ Innovation
- Liberty ⇔ Dependency
- Impact of AI on rights of older persons:
  - Amplification of age-related biases and inequities
  - Digital divide and social exclusion
  - Question of Human Dignity?



Source: https://www.freepik.com/

Artificial Intelligence Act (AI Act)

- Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM(2021) 206 final
- first Europe-wide, horizontal and sector-independent AI regulation

- **EP definition:** "[An] 'artificial intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments."

April 2021: proposal EC → June 2023: start trilogue negotiations → Adoption: by end of 2023 → Coming into effect: approx. 2026

Risk-based approach

(i) Unacceptable risk – prohibited (Art 5)

- AI systems exploiting vulnerable groups, social scoring, real-time remote biometric identification systems

(ii) High risk (Art 6)

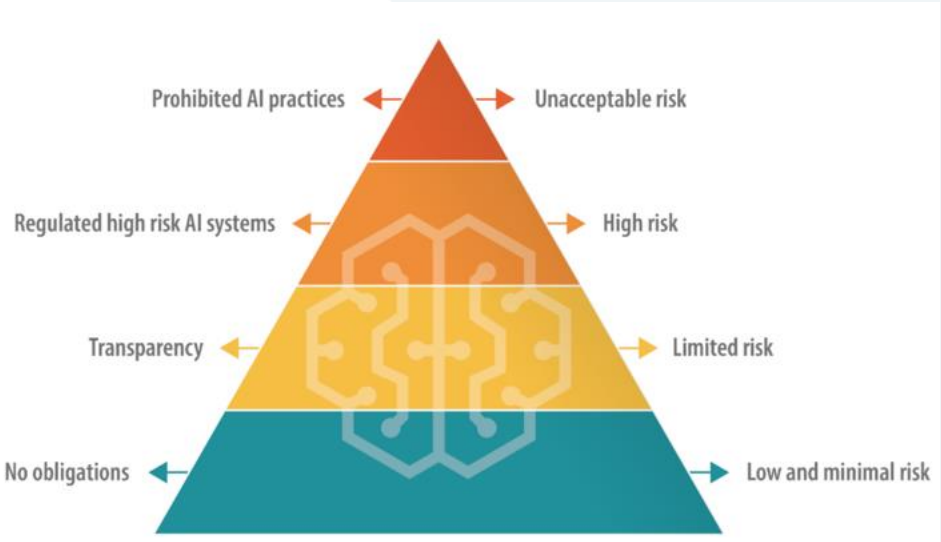
- Management and operation of critical infrastructure, law enforcement, education, employment, administration (see Annex III)

(iii) Limited risk

- E.g. systems that interact with humans (i.e. chatbots), emotion recognition systems
- Limited set of transparency obligations

(iv) Low or minimal risk

- All other systems can by deployed without additional legal obligations



Source: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI%282021%29698792_EN.pdf

Open Questions and Human Rights Impact Assessment

- **Open Questions for trilogue negotiations:**
  - Definition of AI systems
  - List of prohibited and high risk systems
  - Effective ways of implementation

- **Human Rights Impact Assessment**
  - Similar to Data Protection Impact Assessment
  - But: Holistic Approach: „Algorithmic accountability following the various stages of the system's lifecycle"
  - Mandatory in the future

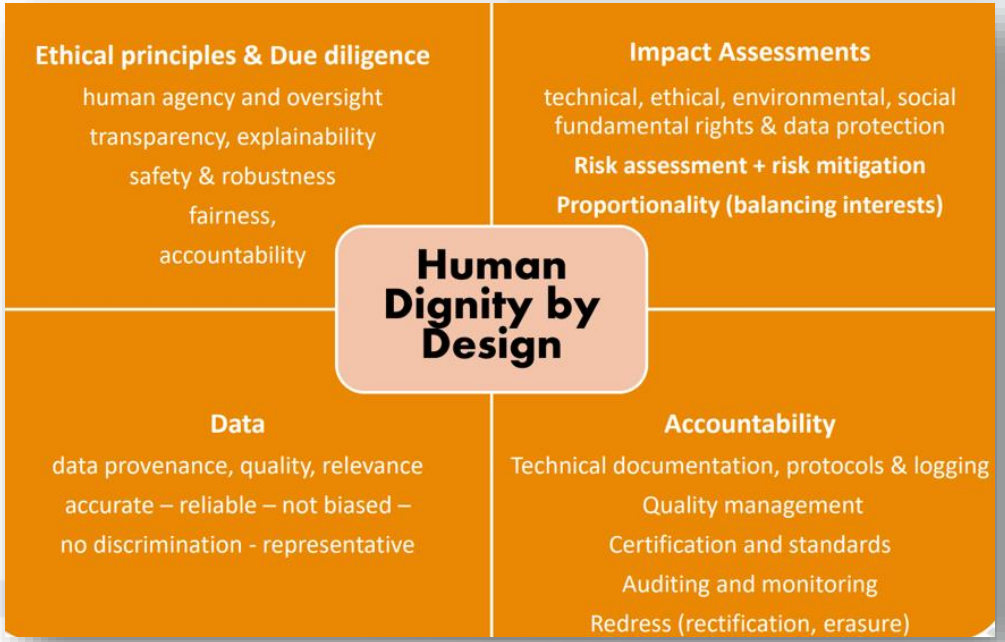
Fundamental Rights Impact Assessment

– 4 steps by *Janssen et al (2022)*

Janssen et al, "Practical fundamental rights impact assessments", in: International Journal of Law and Information Technology, Vol. 30 (2022), 200–232 https://doi.org/10.1093/ijlit/eaac018.

Ethical Guidelines and „Human Dignity by Design"

- Transparency
- Justice, Fairness, Non-discrimination
- Non-maleficence, safety, robustness
- Accountability
- Privacy, Data Protection
- Beneficence
- Autonomy, Freedom, Human Agency
- Sustainability
- Human Dignity
- Solidarity, Inclusion, Accessibility
- Participation
- Democracy and Rule of Law
- Efficiency
- Trust



Principle	Key concepts	References
Transparency	Explainability, explicability, understandability, interpretability, disclosure, communication, AI literacy	• Jobin et al., „Artificial Intelligence: the global landscape of ethics guidelines", in: Nature Machine Intelligence Vol 1. (2019), pp396 • CAHAI-feasibility study 2020, adopted by CoE • Leitfaden Digitale Verwaltung und Ethik • EU High-Level Expert Group on Artificial Intelligence (AI-HLEG) – Ethic Guidelines for Trustworthy AI (2019) • CoE Commissioner for Human Rights: Unboxing Artificial Intelligence: 10 steps to protect Human Rights (2019) • UNESCO Recommendation on the Ethics of Artificial Intelligence (2022) • OECD AI principles 2019 • Selbstverpflichtende Leitlinien für den KI-Einsatz in der behördlichen Praxis der Arbeit und Sozialverwaltung des deutschen Bundesministeriums für Arbeit und Soziales (BMAS 2022) • Assessment List for Trustworthy AI (ALTAI) 2020 • Mandatory Ethical Principles for the use of AI (NSW) • Guidance on AI and data protection ICO • ICDPPC Declaration on Ethics and Data Protection in AI (2018) • An audit of algorithms – Algemene Rekenkamer (2022) • European Group on Ethics in Science and New Technologies – Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems 2018 • OECD Advancing Accountability in AI – Governing and managing risks throughout the lifecycle for trustworthy AI (2023) • Consolidated Working Draft of the Framework Convention on Artificial Intelligence, human rights, democracy and the rule of Law – CAI (July 2023) • EU Declaration on Digital Rights and Principles (2022)
Justice, Fairness, Non-discrimination	Equality, equity, non-bias, diversity, plurality, access and distribution, stakeholder participation	
Non-maleficence, safety, robustness	Security, no harm, protection, precaution, prevention, integrity, non-subversion, risk assessment, cybersecurity	
Accountability	Responsibility, liability, acting with integrity, due diligence, monitoring, remedies	
Privacy, Data Protection	Personal or private information, privacy-by-design, impact assessment	
Beneficence	Benefits, well-being, peace, social good, common good	
Autonomy, Freedom, Human Agency	Consent, choice, self-determination, liberty, empowerment, AI-Literacy, „opt-out"	
Sustainability	Environment, nature, energy, resources	
Human Dignity	Human-centred approach, human oversight	
Solidarity, Inclusion, Accessibility	Social security, cohesion, protection of vulnerable groups, accessibility, diversity, stakeholder participation	
Participation	Participation in decision-making processes	
Democracy and Rule of Law	Use of AI-systems based on legal foundations, transparent and integrative monitoring mechanisms	
Efficiency	Efficient systems that without impairment of human situation	
Trust	Trustworthy AI-systems, researcher, developer, organisations, compliance tools	

In a nutshell

- ✓ Technology needs to be „Human Centred"(„Human Dignity by Design")
- ✓ Not the data needs protection but the legitimate interests of humans behind the data!
- ✓ Balance of security and freedom needs an open dialogue
- ✓ Implicit inclusion of the human rights of older persons by a mandatory risk based approach
- ✓ Normative gaps need to be closed by new international framework, e.g. modelled on GDPR and AI Act as examples of good practice
- ✓ Technology needs to respect limits of human rights („Privacy by Design")
- ✓ Impact Assessment is the most important instrument in this development

Thank you for your attention!

research institute

Dr. Madeleine Müller, BA, MU
Researcher | Consultant

office@researchinstitute.at
Research Institute AG & Co KG
Digital Human Rights Center