This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 820742

HR-Recycler: Hybrid Human-Robot RECYcling plant for electriCal and eLEctRonic equipment

D2.1– Report on security, data protection, privacy, ethics and societal acceptance

WP number and title	WP2 – Regulatory, legal, ethical and societal challenges of robotics in industrial automation
Lead Beneficiary	VUB
Contributor(s)	IBEC, GAIKER, IND, INT, BNTT
Deliverable type	Report
Planned delivery date	07/06/2019
Last Update	03/06/2019
Dissemination level	Public

Disclaimer

The HR-Recycler Consortium consists of the following partners:

Participant No	Participant organisation name	Short Name	Type	Country
1	Centre for Research and Technology Hellas CERTH - ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	RTO	GR
2	FUNDACIO INSTITUT DE BIOENGINYERIA DE CATALUNYA	IBEC	RTO	ES
3	TECHNISCHE UNIVERSITÄT MÜNCHEN	TUM	RTO	DE
4	COMAU SPA	COMAU	IND	IT
5	FUNDACION TECNALIA RESEARCH & INNOVATION	TEC	RTO	ES
6	ROBOTNIK AUTOMATION SLL	ROB	SME	ES
7	FUNDACION GAIKER	GAIKER	RTO	ES
8	SADAKO TECHNOLOGIES SL	SDK	SME	ES
9	DIGINEXT	DXT	IND	BE
10	VRIJE UNIVERSITEIT BRUSSEL	VUB	RTO	BE
11	INDUMETAL RECYCLING, S.A.	IND	SME	ES
12	INTERECYCLING - SOCIEDADE DE RECICLAGEM SA	INT	SME	PT
13	BIANATT ANAKYKLOSI AIIE ANONIMI BIOMICHANIKI EMPORIKI ETAIRIA	BNTT	IND	GR

Document History

VERSION	DATE	STATUS	AUTHORS, REVIEWER	DESCRIPTION
0.1	21/12/2018	Template	CERTH	Project deliverable template
0.2	14/12/2018	Draft	Sara Roda (VUB), István Böröcz (VUB), Eike Gräf (VUB), Ioulia Konstantinou (VUB)	Table of contents and document structure
0.3	28/05/2019	Draft	Sara Roda (VUB), Ioulia Konstantinou (VUB)	First draft
0.5	03/06/2019	Draft	Sara Roda (VUB)	Draft sent for consortium partners
0.5	06/06/2019	Draft	Spyros Karamoutsos (BNTT)	Partner feedback
0.8	06/06/2019	Draft	Sara Roda (VUB), Maider Arieta-araunabeña (IND), Dirk Wollherr (TUM), Belén Garnica (SDK), Sixto Arnaiz (GAIKER), Ana Ferreira (INT), Vicky Vouloutsi (IBEC)	Updates; completing section 5.1.; adding elements in section 3 – ethics; formatting and typo corrections.
0.8	06/06/2019	Draft	Apostolos Axenopoulos (CERTH) and Leire Bastida (TEC)	Internal review
0.9	06/06/2019	Final draft	Sara Roda (VUB) and István Böröcz (VUB)	Final draft before submission
1.0	07/06/2019	Final	CERTH	Final document for submission

Definitions, Acronyms and Abbreviations

ACRONYMS / ABBREVIATIONS	DESCRIPTION
Charter	Charter of Fundamental Rights of the European Union
108 Convention	Convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
CJEU	Court of Justice of the European Union
CoE	Council of Europe
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
HRI	Human-robot interaction
IFR	International Federation of Robotics
ILO	International Labour Organization
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
WEEE	Waste Electrical and Electronic Equipment
WP29	Article 29 Data Protection Working Party of the European Commission

Table of Contents

Executive Summary

The overall goal of the HR-Recycler project is to develop a new generation of collaborative industrial robots and create a human-robot working environment in three recycling plants, respectively located in Greece, Portugal and Spain ('end-users'). More specifically, workers and mobile robots are expected to collaborate in a joint and synchronized manner throughout the typical 3-step of the Waste Electrical and Electronic Equipment (WEEE) recycling process: 1) device classification, through the classification of equipment by recycling categories, 2) device disassembly, by dismantling parts of the equipment both to de-pollute and to recover valuable elements, and 3) components sorting, by sorting out materials for further recycling.

The fundamental aim of the system will be to replace multiple currently manual, expensive, hazardous and time-consuming tasks of WEEE materials pre-processing with correspondingly automatic robotic-based procedures, before materials are sent to a shredding machine or to conventional material separation steps.

The present deliverable outlines the common framework which consortium partners will take into account during their research activities. It intends to serve as a guidance document to partners, and reader friendly, concerning principles, rights and obligations for the processing of personal data. It sets the baseline to reflect on best practices for the processing of personal data when using these new technologies involving human-robot interaction (HRI) in recycling plants.

More precisely, this deliverable translates the VUB TARES framework, which maps the fundamental rights that are likely to be affected during the HR-Recycler project, the ethical and societal concerns underpinning HRI and specific regulatory frameworks that should guide the action of partners. Subsequently, a questionnaire will be sent to each consortium partner to understand how these principles and rules are being met and the results will be fed into deliverable D.2.3 - TARES impact assessment report and contribute to the continuous legal/ethical monitoring and review (deliverables D2.5, D2.6, D2.7 under T2.4).

1 Introduction

1.1 Overview

This report summarises the main findings of Task 2.1, which focuses on identifying and describing i) **fundamental rights** that are likely to be affected during various stages of the HR-Recycler project, such as the right to the protection of personal data, right to privacy, workers' rights to information and consultation within the company, fair working conditions and non-discrimination; ii) **ethical and societal concerns**, analysing, as a first layer, ethical principles relating to truthfulness, appropriateness in the addressed forms of human-robot (HR) interactions and, as a second layer, ethical handling of data relating to employees, stigmatisation and discrimination arising from the HR-Recycler practices; and iii) **regulatory frameworks relevant to HR-Recycler**, in particular where pilots will be deployed.

This task also provides a study about the existing best practices of HR interaction, where appropriate, and the implementation of ethics by design, privacy by design and data protection by design approaches.

1.2 Structure of the deliverable

The deliverable is structured as reported below. Chapters 2 and 3 build on the experience of data protection impact assessment gained through VUB's involvement in two EU funded projects – MaTHISIS [1] and FORENSOR.[2]

Chapter 1 – Introduction – Provides an overview and structure of the deliverable.

Chapter 2 – Mapping Relevant Fundamental Rights – Provides an explanation of the fundamental rights at stake.

Chapter 3 – Ethical and societal concerns – Explains the ethical principles which this research project adheres to and the societal concerns that can emerge from the HR interactions in the industrial recycling sector.

Chapter 4 – Regulatory Frameworks in Member States – Provides an overview of relevant legal frameworks that the deployment of pilots implies at national level.

Chapter 5 – Collection of best practices for the protection of personal data in the context of a human-robot interaction.

Chapter 6 – Bibliographic references.

[1] http://mathisis-project.eu, accessed 20 May 2019.
[2] http://forensor-project.eu, accessed 20 May 2019.

2 Mapping Relevant Fundamental Rights

The use of robots in factories to optimise the recycling process of electronic equipment is increasing. They can have positive effects on workers, as they eliminate dangerous, monotonous and heavy tasks, but also negative, if they render the workers redundant facing the risk of being laid off.

The industrial robots foreseen under the HR-Recycler project are of a collaborative nature which will imply a shared workload process between the human worker and the robot. This method takes into account the experience and skills of human workers, combining robotised and manual operations. The robot is able to learn the task from the human worker when needed and the most dangerous and force demanding tasks are to be carried out by the robot.[3]

Project end-users will need to adapt and streamline the working environment inside the plant. The working cell of the workers will change as they will start operating in smart environments. At this early stage of the project we are not yet able to evaluate if the robots under this Human-Robot Interaction (HRI) will work as a stand-alone system (common tasks and common workspaces where people and robots are working together in the same manufacturing process but on different steps)[4] or if they will be connected to other devices for navigation and interaction, implying a connection to a cloud service or to the Internet of Things (IoT),[5] which may lead to a different manufacturing process (common tasks and separate workspaces, where robots would be more autonomous and would not need direct contact at all times).[6] The use of robotic technologies, and in combination with IoT, might imply the collection of private and personal data, such as information about the users' location, their daily habits or health condition. Data may be transmitted to central servers or shared with other devices or third parties.[7] This may also pose a data security problem – if all systems are networked, they can be easily hacked for malicious purposes. Moreover, technology relies on vulnerable material infrastructures that can be disrupted or destroyed. [8]

It still needs to be further clarified the exact HRI scenario, how the robot will know the position of the human worker and detect a risk of dangerous physical interaction. This is important not only for safety reasons, but also to identify what kind of data is needed to track the human worker body and movements.

---

[3] Esther Alvarez-de-los-Mozos and Arantxa Renteria, Collaborative robots in e-waste management, Procedia Manufacturing 11 (2017) p 55-62, https://www.sciencedirect.com/science/article/pii/S2351978917303372?via%3Dihub, accessed 28 April 2019.

[4] Béni-Trésor Akimana, Maxim Bonnaerens, Jonas Van Wilder, and Bjorn Vuylsteker, A Survey of Human-Robot Interaction in the Internet of Things, 2017, p 15, https://www.researchgate.net/profile/Bjorn_Vuylsteker/publication/318722691_A_Survey_of_Human-Robot_Interaction_in_the_Internet_of_Things/links/5979adbdaca272177c1f4abc/A-Survey-of-Human-Robot-Interaction-in-the-Internet-of-Things.pdf, accessed 27 May 2019.

[5] The Internet of Things (IoT) has been defined in different ways and there is not yet a strict definition. For the purpose of this deliverable, the explanation provided in the European Parliament Member's Research Service Briefing from May 2015 on the Internet of Things – Opportunities and Challenges is sufficient which considers that the Internet of Things (IoT) *"refers to a distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers. The data these devices report can be collected and analysed in order to reveal insights and suggest actions that will produce cost savings, increase efficiency or improve products and services."*, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf, accessed 27 May 2019.

[6] Béni-Trésor Akimana, A Survey of Human-Robot Interaction in the Internet of Things, 2017, p 15.

[7] European Parliament Member's Research Service Briefing from 2015, p 6.

[8] Mark Coeckelbergh, Ethics of artificial intelligence: Some ethical issues and regulatory challenges, Technology and Regulation, 2019, 31–34 • https://doi.org/10.26116/techreg.2019.003 • ISSN: 2666-139X, p 29.

Considering the information sources screened so far, the project includes data exchanged between humans in the loop, sensing devices and limited surveillance tools. The personal data that have been initially identified for collection during the pilots are the following:

i. identification data from workers participating in the research project who have signed the respective consent form,
ii. data concerning health collected through sensors/smart wearable devices, which will measure different type of signals, in particular electrodermal activity (EDA), temperature, heart rate and brain signals, Electroencephalography (EGG), Electromyography (EMG), Galvanic Skin Response (GSR); and
iii. data collected through colour cameras (RGB) but were facial images will be blurred.

This chapter intends to identify the fundamental rights that are likely to be impacted during various stages of the project, such as the right to privacy, the right to the protection of personal data, security, workers' rights to information and consultation within the company, fair and just working conditions and non-discrimination, this to ensure that workers' rights are correctly safeguarded.

2.1 The Right to Privacy or Respect for Private Life

2.1.1 Background information

The discussion about the legal recognition of the right to privacy first came to light in 1890 by the authors Samuel Warren and Louis Brandeis.[9] It came as a reflection upon the appearance of new technologies, namely instantaneous photographs and newspapers enterprises, and the feeling of abuse from those newspapers for collecting and publishing unauthorised portraits of private persons or for commenting private and domestic life affairs. According to the authors, the press had overstepped the limits of propriety and decency, causing harm not only to the individual portrayed but also to the community, lowering social standards and morality. At the time, the right to privacy was considered to be a *right to be left alone*.

The concept from Warren and Brandeis did not however explain what privacy entails and the issues in which individuals should be left alone. It remained a vague and broad definition. Even today there is no single accepted definition of what the right to privacy is.[10] Privacy can be cultural, contextual and evolutive. The author Daniel Solove provides a summary about different theories of privacy and their shortcomings, explaining that the right to privacy could be grouped, *inter alia,* in six categories:[11]

1. The right be let alone, that is *"to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law"*;[12]
2. The limited access to the self, as the ability to shield oneself from unwanted public observation and discussion by others;
3. Secrecy, where privacy is infringed by public disclosure of previously concealed information and where the interest of the individual is to avoid disclosure of personal matters;[13]
4. Control over personal information, meaning the claim of individuals, groups or institutions to determine how, when and to what extent information about them is given to others;[14]

[9] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, in *Harvard Law Review*, 1890, Vol. 4, No. 5, p 193-220.
[10] Robert C. Post, Three Concepts of Privacy, in *Faculty Scholarship Series*, 2001, Paper 185, https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1184&context=fss_papers, accessed in April 2019.
[11] Daniel J. Solove, Understanding Privacy – Chapter 2: Theories of privacy and their shortcomings, Cambridge Massachusetts: Harvard University Press, 2008, p 2.
[12] Justice Abe Fortas as cited in Solove, Understanding Privacy – Chapter 2, 2008, p 2.
[13] Whalen v. Roe (1977) as cited in Solove, Understanding Privacy – Chapter 2, 2008, p 5.
[14] Alan Westin as cited in Solove, Understanding Privacy – Chapter 2, 2008, p 5.

5. Personhood, concerns the protection of the integrity of personality and considered to be *"those attributes of an individual which are irreducible in the selfhood"*; [15] and,
6. Intimacy, where the focus is on the development of personal relationships and different degrees of intimacy and self-revelation.

The concept of 'private life' has been broadly interpreted in case-law, covering sensitive or confidential information, intimate situations, information that could prejudice the perception of the public against the individual, and aspects of an individual's professional life and public behaviour. The assessment on whether there has been an interference or limitation with 'private life' depends on the context and facts of each case.[16]

2.1.2 Universal Declaration of Human Rights

Article 12 of the Universal Declaration of Human Rights

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Adopted in 1948 as a response to the atrocities of the II World War, the Universal Declaration of Human Rights (UDHR) established a universal common standard for the right to privacy.[17] The UDHR consists of a political declaration which is under the umbrella of the United Nations. The right to privacy is considered to be a fundamental human right in the international legal order.

Since 2013, the United Nations adopted two resolutions on the 'right to privacy in the digital age', condemning mass surveillance and stressing the impact such surveillance can have on the right to privacy and freedom of expression and to the functioning of a democratic society.[18] Recent UN resolutions reflect on the growing capabilities of companies to process personal data in a way that can jeopardise the enjoyment of the right to privacy in the digital age. They intend to recall not only the responsibility of state authorities to respect human rights, but also of private entities, which should inform users about the ongoing processing operations and establish transparent processing policies.[19]

2.1.3 European Convention on Human Rights

Article 8 of the European Convention of Human Rights
Right to respect for private and family life

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

---

[15] Solove, Understanding Privacy – Chapter 2, 2008, p 9.
[16] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Luxembourg: Publications Office of the European Union, 2018, p 20.
[17] https://www.un.org/en/universal-declaration-human-rights/, accessed 27 May 2019.
[18] https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx, accessed 27 May 2019.
[19] FRA, Handbook on European Data Protection Law, p 22.

The Convention for the Protection of Human Rights and Fundamental Freedoms, known as the European Convention on Human Rights (ECHR), came into force in 1953. It was the first instrument giving effect and making binding certain rights of the UDHR.[20] The ECHR comes under the umbrella of the Council of Europe (CoE) which is an organisation founded in 1949 to promote democracy and protect human rights and the rule of law in Europe. The CoE is an organisation composed of 47 members, 28 of which are members of the European Union. All members of the CoE have signed the ECHR.[21] To ensure that the Contracting Parties of the ECHR would comply with their obligations, the CoE set up in 1959 the European Court of Human Rights (ECtHR).

The respect for private life is recognised under Article 8 of the ECHR. This right not only obliges states to refrain from any actions that may creep upon private life (negative obligation), but also to actively secure the respect for private life (positive obligation).[22] The right to respect for private life is not absolute, as certain interferences are accepted if i) in accordance with the law, ii) necessary in a democratic society iii) while pursuing legitimate and important public interests. The ECtHR has ruled that the exercise of the right to privacy can compromise other rights, such as freedom of expression, access to information and professional secrecy. When different rights are at stake, there should be a balancing exercise to reconcile them. [23]

2.1.4 Charter of Fundamental Rights of the European Union

Article 7 of the Charter of Fundamental Rights of the European Union
Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 52 of the Charter of Fundamental Rights of the European Union
Scope and interpretation

"1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(…)

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

Under the Charter of Fundamental Rights of the European Union (Charter), the right to privacy is referred to as the right to respect for private life (Article 7).[24] The Charter is one of the most important sources of fundamental rights in the EU legal system which only became legally binding with the Lisbon Treaty in 2009. The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR, with a minor difference of wording, replacing "correspondence" by "communications", to take stock of the technological

[20] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c, accessed 27 May 2019.
[21] The Council of Europe (CoE) is an organisation composed by 47 members, 28 of which are members of the European Union. All members of the CoE have signed the ECHR.
[22] ECtHR, I v Finland, N° 20511, 17 July 2008.
[23] FRA, Handbook on European Data Protection Law, p 24 and 53.
[24] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

world developments. Article 7 is complemented by Article 52(1) and (3) of the Charter which also recognises that the right is not absolute – limitations are allowed if i) provided by law, ii) respect the essence of the right, iii) are necessary and proportionate and iv) meets objectives of general interest, including general objectives of the EU mentioned in Article 3 of the TEU or other protected by specific provisions in the treaties.

2.2 The Right to the Protection of Personal Data

2.2.1 Background information

The right to the protection of personal data is closely related to the right to respect for private life. They both protect similar values, such as autonomy and human dignity of individuals, and aim at creating a personal sphere where individuals are able to develop their personalities freely. They are pre-condition to exercise other rights, such as freedom of expression and freedom of peaceful assembly and association.[25]

The protection of personal data came as a response to the interferences led by governments concerning the collection and use of personal information. It appeared first as a derivation of the right to privacy, as privacy provided for the 'right to informational self-determination' or 'informational privacy'. It then evolved to a separate fundamental right.[26]

The right to the protection of personal data and the right to respect for private life are distinct in formulation and scope: the latter consists of a general prohibition of interference, with certain exceptions, the former is considered to be an 'active right', which implements a system of checks and balances to protect individuals personal data when is being processed. To ensure the efficacy of such a system, the processing i) must be lawful, ii) individuals need to be able to exercise certain rights (explained in section 2.5.6 below) and iii) there should be an independent authority supervising its correct application. [27]

In Europe, data protection is based on two systems: the Council of Europe (CoE) and the European Union. Recital 105 of the General Data Protection Regulation (GDPR)[28] establishes the following:

"Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations."

Both systems will be explained below.

2.2.2 Convention 108 of the CoE

The Convention for the Protection of Individuals with regard to automatic processing of personal data of 28 January 1981, also known as Convention 108,[29] is a legally binding international instrument in the data protection field, for all States ratifying it, which applies to data processing carried out by both the private and

[25] FRA, Handbook on European Data Protection Law, p 19.
[26] Ibid, p 18.
[27] Ibid, p 18.
[28] 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, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119.
[29] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

public sectors, including data processing by the judiciary branch and law enforcement authorities. It is open to every country and currently composed of 54 States, of which 28 are Members States of the EU. The Parties to the Convention commit to a mutual co-operation and to ensure the highest level of data protection.

In 1999, amendments to Convention 108 were proposed to enable the EU to become a party but it never entered into force. In 2001, an Additional Protocol to the Convention 108 was adopted on transborder data flows to non-parties (third countries) and on the mandatory establishment of national data protection supervisory authorities. In 2018, the Convention was modernised (Convention 108+)[30] to respond to the new challenges of the digital era, the globalisation of processing operations and to allow safer exchanges of personal data.[31]

The Convention is not subject to the judicial supervision of the ECtHR but has been taken into consideration in the case law of the ECtHR within the context of Article 8 of the ECHR.[32]

The Convention aims to protect individuals against abuses which may result from the processing of personal data and seeks to regulate the transborder flows of personal data. As regards the processing of personal data, the principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data, for specified legitimate purposes.

2.2.3 Charter of Fundamental Rights of the European Union

Article 8 of the EU Charter of Fundamental Rights

Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.1. Everyone has the right to the protection of personal data concerning him or her."

The right to the protection of personal data is a fundamental right recognised by the Charter.[33] EU institutions and bodies must guarantee and respect this right, as well as Member States when implementing Union law (Article 51 of the Charter). This article was formulated after the Data Protection Directive[34] which included the EU *acquis* on data protection: it recognised the right and certain principles as well as an independent authority to control the implementation of those principles.

The right to the protection of personal data is not absolute. It can suffer limitations under strict conditions of Article 52 (1) and (3) of the Charter. Limitations must be i) **provided by law**, that is, a legal basis that is accessible and formulated with sufficient precision to enable individuals to understand their obligations and regulate their conduct. The legal basis must also clearly define the scope and manner of the exercise of the power by the competent authorities to protect individuals against arbitrary interference; ii) **respect the**

[30] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1, accessed 28 May 2018.
[31] CoE Data protection leaflet, https://rm.coe.int/leaflet-data-protection-final-26-april-2019/1680943556, accessed 28 May 2019.
[32] ECtHR, Zv. Finland, N° 22009/93, 25 February 1997.
[33] Gloria González Fuster, The emergence of personal data protection as a fundamental right of the EU, Vol. 16. Springer Science & Business, 2014.
[34] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

essence of the right, that is, limitations that are so extensive and intrusive emptying a fundamental right of its basic content cannot be justified. If the essence is compromised, the limitation is unlawful, and there is no need to further assess whether it serves an objective of general interest and satisfies the necessity and proportionality criteria;[35] iii) **necessary** (the measure is needed to be adopted to pursue the public interest objective and it must be the less intrusive measure compared to other options for achieving the same goal. The CJEU applies a strict necessity test for limitations on the rights to respect for private life and protection of personal data, holding that *"derogations and limitations must apply only in so far as strictly necessary"*.) **and proportional,** meaning that the advantages resulting from the limitation should outweigh the disadvantages the latter causes on the exercise of the fundamental rights at stake. To reduce disadvantages to the rights at stake, appropriate safeguards are needed;[36] iv) **pursue objectives of general interest** which must be recognised by the Union law or the need to protect the rights and freedoms of other persons (Article 3 of the TEU and Article 23(1) of the GDPR list a series of objectives of general interest). These objectives need to be clearly defined and explained and a detailed description is required in order to assess the necessity of the measure.

2.3 Primary law

EU law is composed of primary and secondary law. The Treaties – Treaty of the Functioning of the European Union (TFEU) and the Treaty on the European Union (TEU) – are part of the primary law. They are binding agreements between EU Member States which define EU objectives, rules for EU institutions, determining how decisions are made and the relationship between the EU and its members. The Treaties are the starting point for every action taken by the EU.[37]

Article 16 of the TFEU

"1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

Article 39 of the TEU

"In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

[35] CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015; CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014; FRA, Handbook on data protection, p 44-45.

[36] EDPS (2017), Necessity Toolkit, 11 April 2017, p 5; FRA, Handbook on data protection, p 46.

[37] https://ec.europa.eu/info/law/law-making-process/types-eu-law_en, accessed 30 May 2019.

The right to the protection of personal data is specifically recognised by Article 16 of the TFEU and Article 39 of the TEU. Article 16 of the TFEU also creates a new independent legal basis for EU co-legislators (the European Council and the European Parliament) to legislate on data protection matters. Initially, EU data protection rules were based on the internal market legal basis and on the need to approximate national laws (Article 114 of the TFEU) so that the free movement of data within the EU was not constrained.

2.4 Secondary law

Secondary law is the body of law that comes from the principles and objectives of the EU treaties and includes regulations, directives, decisions, recommendations and opinions.[38] Article 16 of the TFEU served as legal basis to adopt the GDPR,[39] the Law Enforcement Directive[40] and is currently being used to replace the e-Privacy Directive[41] by a regulation concerning the respect for private life and the protection of personal data in electronic communications.[42] An additional legal instrument relevant in the area of data protection is Regulation (EU) 2018/1725 which applies to the processing of personal data by EU institutions and bodies.[43]

Certain institutions at EU level assume a core role in the defence of the data protection rights. These are:

- The European Data Protection Supervisor (EDPS) – it is an EU independent data protection authority which supervises the processing of personal data by EU Institutions and bodies. It also advises those entities on all matters relating to the processing of personal data, on request or at their own initiative. In particular, they are consulted by the European Commission on proposals for legislation, international agreements, as well as implementing and delegated acts with an impact on data protection and privacy. The EDPS monitors new technology that may affect the protection of personal information.[44]
- The European Data Protection Board (EDPB) - is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities. It is composed of representatives of the national data protection authorities, and the EDPS. The EDPB was established by the GDPR and replaced the Working Party 29. The European Commission has the right to participate in the activities and meetings of the Board without voting rights.

2.5 Principles, rights and obligations under the General Data Protection Regulation

The GDPR sets out general principles and safeguards concerning the processing of personal data.

---

[38] Ibid.

[39] Regulation (EU) 2016/679, OJ 2016 L 119.

[40] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4 May 2016.

[41] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, OJ L 201 (Directive on privacy and electronic communications or e-Privacy Directive).

[42] The legislative process is still ongoing - Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

[43] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21 November 2018, p 39–98.

[44] https://edps.europa.eu/about-edps_en, accessed 29 May 2019.

2.5.1 Core definitions

The core definitions which will be relevant for the HR-Recycler project are the following (Article 4, 9 and recital 51 of the GDPR):

Personal data	Any information relating to an identified or identifiable natural person (data subject). Examples include names, dates of birth, photographs, email addresses and telephone numbers, content of communications, etc.
Identifiable natural person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g. IP addresses) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Data concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Sensitive data	Personal data which are, by their nature, particularly sensitive as the context of their processing could create significant risks to the fundamental rights and freedoms. It may include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, 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.
Data subject	Any natural person whose personal data is being processed.
Data controller	A natural or legal person who, alone or jointly, determines the purposes and means of processing.
Data processor	A natural or legal person who processes personal data on behalf of the controller.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	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
Pseudonymisation	Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Consent of the data subject	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Personal data breach	Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

HR-Recycler project: The data protection framework becomes applicable when the data subjects (the workers) are identifiable through the collected data whether it occurs during the pilot or later on when the system is deployed.

2.5.2 General principles

The GDPR has two core objectives [Article 1(2) and (3)]: i) the protection of fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data, and ii) the free movement of personal data within the EU.

The principles that must be applied whenever personal data processing occurs in the HR-Recycler project are described below. Certain principles have been codified at constitutional level by Article 8 of the Charter, as it states that personal data *"must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law".*

General Data Protection Regulation

Data Protection Principles	GDPR
Lawfulness, fairness, transparency Article 5 (1)(a)	The processing of personal data shall be fair, lawful and transparent. Lawfulness requires the data subject's consent, or another legitimate ground provided in Article 6 and/or 9 of GDPR. Fairness and transparency imply that the data subjects, mainly **workers in HR-Recycler**, should be able to know what information has been collected about them, the purpose and means of collection, who can access and use it, how to access the collected information and how to control who has access to it. Data controllers should be clearly identified and respond to the data subjects' requests.
Purpose limitation Article 5(1)(b)	The collection of personal data must be for specific, explicit and legitimate purposes and cannot be further processed for a purpose incompatible with the initial purposes. The purpose should be specified at the time of collection. Further processing for scientific or historical research purposes or statistical purposes is not considered to be incompatible with the initial purposes.
Data minimisation Article 5(1)(c)	The collection of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected. This is particularly important in the context of new technology.

Accuracy Article 5(1)(d)	Personal data should be accurate and kept up to date. Inaccurate personal data should be erased or rectified without undue delay. Irrelevant data should not be collected and if it occurs it must be deleted.
Storage limitation Article 5(1)(e)	Personal data should be kept in a form which permits identification of data subjects for the period necessary to fulfil the purpose for which those data were collected; personal data may be stored for longer periods for scientific, historical or statistical purposes. Where possible, personal data should be anonymised.
Integrity and confidentiality Article 5(1)(f)	Personal data should be kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage. Appropriate technical and organisational measures need to be put in place to ensure compliance with these principles. This point is further mentioned in section 2.5.7.2 below.
Accountability Article 5(2)	The controller [entity that defines alone or jointly with others the purposes (why) and the means (how) of the processing operations] is responsible for and must be able to actively demonstrate compliance with the previous principles, and not wait for data subjects and supervisory authorities to point out the shortcomings. To facilitate the compliance with this requirement, controllers can i) record the processing activities, making them available to the supervisory authority upon request (Article 30 GDPR); ii) adhere to approved codes of conduct or certification mechanism; iii) designate a Data Protection Officer; iv) undertake a Data Protection Impact Assessment; iv) ensure data protection by design and by default; v) adopt policies and procedures, and implement them, to allow the exercise of the rights of data subjects.

2.5.3 Legal basis for processing personal data

Article 6 of the GDPR stipulates that in order to be lawful, personal data should be processed for one of the following reasons:

- Freely given, specific and informed consent of the data subject;
- Performance of a contract to which data subject is a party;
- Compliance with the legal duties of the controller;
- Protection of the vital interests of the data subject;
- Activity carried out in the public interest or exercise of official authority;
- Legitimate interest pursued by the data controller, as long as it is not overridden by the interests or the fundamental rights of the data subjects.

HR Recycler project: processing of personal data will be based on the consent of the data subject. This section provides a more detailed explanation concerning the use of consent in order to process either personal data or 'sensitive' personal data. Article 6(4) and recital 50 of the GDPR allow the possibility of

further processing of the collected data for research purposes - the provisions consider that this further processing is compatible with the GDPR. The procedure to ensure an informed consent from research participants in HR-Recycler was outlined in deliverable D1.1: H – Ethics Requirement to which we refer to. The related safeguards and guarantees are detailed therein.

Consent as a legal basis of processing personal data has three building blocks:

- Data subject must give his consent freely, without undue pressure. The consent is freely given if the data subject is able to exercise a real choice (opt-in) and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent;[45]
- Data subject must have sufficient information before taking a decision; the language used must be clear and understandable and the consequences of not giving consent must be included as well;
- The consent must be specific, given in unambiguous terms and related to the reasonable expectations of an average data subject. There ought to be no reasonable doubt that the data subject wanted to convey his/her agreement to allow the processing of data.

2.5.4 Processing sensitive personal data – 'special categories of personal data'

The HR-Recycler project foresees the collection and processing of **special categories of data**, in particular health and biometric data, using sensors and smart wearable devices (such as Electroencephalography (EGG), Electromyography (EMG) or Galvanic Skin Response (GSR)). These technologies will measure different type of signals, such as electrodermal activity (EDA), temperature, heart rate and brain signals.

Processing special categories of data requires compliance with stricter requirements due to the risks that their disclosure or misuse might cause. Article 9(1) of the GDPR prohibits *"processing of personal data revealing 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."* The processing this sensitive data needs to comply with the fundamental principles of data protection, notably data minimisation.

Derogations to the general prohibition rule exist but are applied strictly (Article 9(2) of the GDPR). The most important ones relating to HR-Recycler are highlighted below:

- **Explicit consent:** a derogation from the ban is allowed where "*the data subject has given his explicit consent to the processing of those data"*. See in previous section the conditions to provide lawful consent. Explicit consent must be traceable; thus, proof must be kept, and it is given usually in written form. **In HR-Recycler the use of explicit consent of the data subjects as a legal basis to process sensitive data will have an essential role;**
- **Employment law, social security and social protection law (Article 9(2)(b) of the GDPR):** the prohibition can be lifted if the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. The processing needs to be authorised either by EU law, national law or collective agreement and appropriate safeguards for the fundamental rights and the

[45] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, 2017.

interests of the data subject established. **Examples may include trade union membership or health information;**

- **Vital interests of the data subject or another person (Article 9(2)(c) of the GDPR)**: This derogation can only be used if it is not possible to ask the data subject for consent (e.g. unconscious, or absent and cannot be reached). Concerning using to protect the vital interests of another person, this derogation can only be used when another legal basis is not possible (see also recital 46 of the GDPR);
- **Processing of data by health professionals (Article 9(2)(h)of the GDPR):** derogation allowed whenever it *"is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of union or member state law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*" [persons subjected to professional secrecy];
- **Archiving, scientific, historical or statistical purposes (Article 9(2)(j) of the GDPR):** this derogation must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate measures to safeguard rights and interests of the data subject.

2.5.5 Automated decision making, including profiling

Automated decisions are decisions taken using personal data processed solely by automated means without human intervention. Article 22 of the GDPR stipulates that data subjects must not be subject to automated decisions which produce legal effects or have similarly significant effects. If such decisions are likely to have a significant impact on the lives of individuals as they relate, for example, to performance at work, or the analysis of conduct or reliability, then special protection is necessary to avoid negative consequences.[46]

Automated decision-making includes profiling. Profiling implies categorising individuals according to their personal characteristics. These characteristics can be 'unchangeable', such as age or height, or 'changeable' such as habits, preferences and other elements of behaviour. [47] Profiling includes data mining, whereby individuals are categorised according to some of their observable characteristics in order to infer others that are not observable.[48]

However, certain exceptions concerning the use of automated decision making with legal effects or scientifically affecting individuals are accepted. Article 22(2) and (3) of the GDPR allow if it is necessary for entering a contract or the performance of a contract between the data controller and data subject, or if the data subject gave explicit consent, or if it is authorised by law and the data subject's rights, freedoms and legitimate interests are appropriately safeguarded. **The controller needs to inform in advance about the automated decision-making activity and the profiling** (Article 12 of the GDPR) **and the legal consequences that it can engender to the data subject. The data subject as the right to obtain human intervention, to express his or her point of view, to obtain an explanation about the decision reached after such assessment** [Articles 15(1)(h) and 13(2)(f) of the GDPR] **and to challenge the decision** [Article 22(3) of the GDPR].

[46] FRA, Handbook on European Data Protection Law, p 233. Further guidance can be found in Article 29 Working Party, Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679, WP 251, 3 October 2017, p. 15.

[47] FRA, Handbook on Preventing Unlawful Profiling Today and in the Future: A Guide, Luxembourg: Publications Office of the European Union, 2018, p 15.

[48] Dinant, J.-M., Lazaro, C., Poullet Y., Lefever, N. and Rouvroy, A. (2008), Application of Convention 108 to the Profiling Mechanism - Some ideas for the future work of the consultative committee (T-PD), Doc. T-PD 01, p. 3, as cited in FRA Handbook on Preventing Unlawful Profiling (2018).

2.5.6 Rights of the data subject

The data subject has certain rights under the GDPR:

- **Right to be informed (Article 12 of the GDPR)**: the controller is obliged to inform the data subject when personal data are collected about the intended processing. The data subject does not need to justify its request. The information provided must be concise, transparent, intelligible and easily accessible, using clear and plain language. The information can be provided in writing, or orally if requested by the data subject. The information shall be provided without excessive delay and free of charge (exceptions are foreseen);
- **Right of access (Article 15 of the GDPR):** every data subject has the right to *"obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data"*. This right is necessary to enable the data subject to exercise his rights under Article 12. The following information needs to be provided:
  - processing purposes;
  - categories of data concerned;
  - recipients or categories of recipients to whom the data are disclosed;
  - period for which the data is intended to be stored, or, if not possible, the criteria used to determine that period;
  - any available information about the source of the data undergoing processing if the data are not collected from the data subject;
  - existence of automated-decision making, including profiling and meaningful information about the logic involved and the consequences of such processing for the data subject.
- **Right to rectification (Article 16 of the GDPR):** *"the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."* The accuracy of personal data is meant to guarantee a high level of data protection for data subjects;
- **Right to erasure, also known as "the right to be forgotten" (Article 17 of the GDPR):** grants the right to the data subject to have his personal data erased without undue delay and it is directly linked to the data minimisation principle. In particular, this right applies, *inter alia,* where:
  - the personal data are no longer necessary regarding the purposes for which they were collected or otherwise processed;
  - the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing;
  - the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
  - the personal data have been unlawfully processed;
  - the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- **Right to data portability (Article 20 of the GDPR):** *"the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided";*
- **Right to object (Article 21 of the GDPR):** the data subject has the right to object, at any time, on grounds relating to the data subject's particular situation, but also against profiling and direct marketing purposes. This provision tried to strike a balance between the data subject's rights and

the legitimate interests of others in processing their data (which can override the interests and rights of the data subject). A successful objection forbids the continuation of the data processing, although processing operations prior to the objection remain legitimate;[49]

- **Right to lodge a complaint with a supervisory authority (Article 78 of the GDPR):** every data subject can lodge requests and/or complaints to the competent supervisory authority, if they believe that the processing of his/her personal data is not being carried out in accordance with the law;
- **Right to a judicial remedy and to receive compensation (Articles 79 and 82 of the GDPR):** whenever the data subject considers that his or her rights under GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR, he or she has the right to an effective judicial remedy and the right to receive compensation according to;
- **The right to restriction of processing (Article 18 of the GDPR):** data subjects can temporarily restrict a controller from processing their personal data, when one of the following applies:
    - the accuracy of personal data is contested by the data subject;
    - the processing is unlawful and the data subject requests that the use of the personal data is restricted instead of erased;
    - the data must be kept for the exercise or defence of legal claims;
    - a decision is pending on the legitimate interests of the data controller prevailing over the interests of the data subject, pursuant to Article 21(1) of the GDPR.

2.5.7 Obligations of the data controller

Pursuant to Articles 5(2) and 24 of the GDPR, the data controller needs to ensure and demonstrate compliance with the GDPR when processing personal data – accountability principle. In order to do so, the controller needs to map, predict and assess the effects and consequences of his activity. The following obligations should be interpreted as accountability measures or clear reflections of the accountability principle.

HR-Recycler project: For the purposes of the GDPR, the partner that resumes the role of data controller will be examined on a case-by-case basis considering each data set identified in the Data Management Plan, Deliverable D12.2. The obligations and principles that each data controller will have to comply with are set below.

2.5.7.1 Record of processing activities (Article 30 of the GDPR)

This provision requires a detailed documentation about the controller, the processor (if any) and the processing operation. The documentation helps the identification of risks by the controller by the supervisory authority. The maintenance of a register is not mandatory when the controller has less than 250 employees. However, such a register can be beneficial to better assess risks and to trace the controllers' procedures;

2.5.7.2 Data Security (Article 32 of the GDPR)

The data controller, as well as the processor, need to take appropriate technical and organisational measures against accidental, unauthorised or unlawful access, destruction, loss, use, modification, disclosure or damage, in order to ensure the security of the personal data.

[49] FRA, Handbook on European Data Protection, p 230-231.

The level of data security is determined by:

- the security features available in the market for any particular type of processing;
- the costs of implementation;
- the risks of processing the data for fundamental rights and freedoms of data subjects. [50]

These technical measures include, among others:

- pseudonymising (personal data attributes are kept separately to keep personal identities secret) and encrypting personal data;
- ensuring that the processing system and service maintain confidentiality, integrity, availability and resilience;
- restoring the availability of and access to personal data in the event of data loss in a timely manner;
- a process for testing, assessing and evaluating the effectiveness of the measures to ensure the security of processing. [51]

Organisational measures can be:

- Inform and train all employees about data security rules and their obligations under data protection law, in particular their confidentiality obligations;
- Clearly distribute responsibilities and outline competencies in matters of data processing, particularly when deciding to process personal data and to transmit data to third parties or to data subjects;
- Use or authorise the use of personal data only according to precise instructions given by the competent person, otherwise refrain from collecting or authorising;
- Protect access to locations and to hard- and software of the controller or processor, including checks on authorisation for access;
- Regularly check protocols on access to and disclosure of personal data and document those, to demonstrate that no illegal data transmissions have taken place;
- Carry out internal and external audits to ensure that the appropriate measures are being implemented and work in practice (and that just do not exist on paper). [52]

2.5.7.3 Privacy by design and by default

Article 25 and Recital 78 of the GDPR requires that data controllers comply with a general principle of data protection by design and by default, taking into account the state of the art, the costs of implementation, the nature, scope and purposes of personal data processing and the risks and severity for the rights and freedoms of the data subject.

Data protection by design: the objective is to integrate privacy into engineering processes, which need to consider privacy in the whole life cycle of a product or service, from the initial conception to disposal.[53] Companies are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles from the start. For example: use of pseudonymisation and encryption (encoding messages so only those authorised can read them).[54]

---

[50] FRA, Handbook on European Data Protection Law, p. 132, 166-168.
[51] Ibid.
[52] Ibid.
[53] EDPS Preliminary Opinion 5/2018 on privacy by design, 31 May 2018.
[54] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en, accessed 29 May 2019.

Data protection by default: companies should ensure that personal data is processed with the highest privacy protection, for example only data that is necessary should be processed, there should be short storage period and limited accessibility, so that by default personal data is not made accessible to an indefinite number of persons.[55] Another example is to set users' profile settings on a website in the most privacy-friendly setting (e.g cookies should be only functional, avoid using newsletters that can allow access to user's profile to an indefinite number of persons).

2.5.7.4 Data breach notification (Articles 33 and 3 of the GDPR)

Controllers must notify certain data breaches to the supervisory authorities without undue delay and, where feasible, within 72 hours of the moment they become aware of the breach. If they exceed the 72-hour timeframe, the notification needs to be accompanied by an explanation for the delay. Controllers are exempt from the notification requirement only where they are able to demonstrate that the data breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned. Furthermore, if a data breach is likely to cause high risks to the rights and freedoms of individuals, controllers must also inform them of the breach without undue delay.[56]

2.5.7.5 Sanctions (83(1) of the GDPR)

Fines must be effective, proportionate and dissuasive. The proportionality depends on the interpretation of the imposing authority, and its effectiveness is directly proportional to its dissuasiveness. To increase effectiveness the amount of fine has been significantly increased and it can reach 20 million EUR or up to 4% of the total worldwide annual turnover of the preceding year.

2.5.7.6 Data Protection Impact Assessment (35 of the GDPR)

A data controller needs to conduct an impact assessment on the processing of its personal data operations, when the processing is likely to result in a high risk for the rights and freedoms of the individual.[57] **Amongst the operations considered high risk, there is the processing of sensitive data or processing using new technologies, as it is the case of HR-Recycler.**

Data protection impact assessment is intended to implement the general risk assessment logic into data protection law. With a risk assessment the decision-maker (data controller) is capable to decide whether the risk (the processing of personal data) has negative consequences and if so, how to better mitigate them. Such activity will be carried out in WP2, deliverable D2.3.

2.5.7.7 Prior consultation (Article 36 of the GDPR)

A data controller needs to consult the supervisory authority, prior to processing of personal data, when the data protection impact assessment indicates that the processing would result in a high risk, and the controller decided not to take measures to mitigate such risk.

---

[55] Ibid.

[56] FRA, Handbook on European Data Protection Law, p 171-173; Article 29 Working Party, Guidelines on Personal Data Breach Notification under Regulation 2016/679, 2017.

[57] See also Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, 2017.

2.5.7.8 Stakeholders consultation (Article 35(9) of the GDPR

Where appropriate, controllers should seek the views of the data subjects or their representatives on the processing operations that will take place. This point will be further developed in deliverable D2.2 – Impact assessment method.

2.5.8 Processing personal data in the context of employment

2.5.8.1 The GDPR requirements

The processing of personal data under an employment relationship is specifically foreseen in Article 9(2) of the GDPR on the processing of sensitive data. Article 88 of the GDPR allows Member States to establish more specific rules to ensure the protection of employees' rights and freedoms in respect of their personal data in the employment context. For example, the CJEU has ruled that recording a worker's working time indicating when working hours begin and end, as well as the corresponding breaks and intervals, is recording personal data. However, if a national law requires an employer to record the working time and make it available to the national authority responsible for monitoring employees working conditions, to allow such authority to monitor the application of the legislation on working conditions, that requirement is lawful.[58]

The use of consent as a legal basis in the employment context is questionable, according to Article 29 Data Protection Working Party (WP29),[59] due to the economic imbalance between employer and employees. There can be doubts on whether the consent was freely given. [60] As a result, the context in which consent is given needs to be carefully assessed.[61] Employees should be informed about their rights and the time length that the data will be stored before consent is given and it is very important to clearly distinguish the data to which the employee freely consents for processing and the purposes for which his/her data are stored. If a breach of personal data is likely to result in a high risk to the rights and freedoms of natural persons, the employer must communicate this breach to the employee.[62]

General prohibitions about the private use of communication facilities at work can be considered disproportionate and unrealistic by the Courts. Employers should apply more preventative measures instead of monitoring employees' internet usage.[63]

---

[58] CJEU, C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 30 May 2013, para 19.

[59] Working Party 29 was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy. Its tasks were described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The WP29 was replaced by the European Data Protection Board (https://edpb.europa.eu/about-edpb/about-edpb_en) and established by the GDPR (Articles 68 and onwards of the GDPR).

[60] See further developed in section 2.5.8.3 below.

[61] FRA, Handbook on Data protection, P 331; WP29, Opinion 2/2017 on data processing at work, WP249, Brussels, 8 June 2017; WP29, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP114, Brussels, 25 November 2005.

[62] FRA, Handbook on Data protection, P 331.

[63] ECtHR, Copland v. the United Kingdom, No. 62617/00, 3 April 2007. In this case the telephone, email and internet usage of an employee was secretly monitored to ascertain whether she was making excessive use of facilities for personal purposes. The Court held that telephone calls, emails and personal internet usage from work were covered by the right for of private life and correspondence and therefore protected by Article 8 of the ECHR. There needed to be a provision regulating the circumstances under which employers could monitor employees' use of telephone, email and the internet; FRA, Handbook on Data protection, p 331.

2.5.8.2 The CoE Employment Recommendation[64]

The CoE issued a recommendation on the processing of personal data for employment purposes in both private and public sectors. The processing must comply with certain principles and restrictions. Among others, the recommendations advocates for:

- Transparency in the processing operations;
- Respecting for the privacy and human dignity of employees, in particular the possibility of exercising social and individual relations at the place of work;
- Informing or consulting employees or their representatives (e.g. work committees, trade unions, etc.) about i) the introduction or adaptation of automated systems for collection and use of personal data; ii) introduction or adaptation of technical devices designed to monitor movements or productivity of employees; iii) sought agreement of employees or their representatives before the introduction or adaptation of such systems or devices where there is a risk of infringement of employees' right to respect for privacy and human dignity (unless national law or practice provides other appropriate safeguards).
- Storing of health data covered by medical secrecy by personnel bound by rules on medical secrecy. In specific circumstances, such information can be communicated to the administration (if it is indispensable for decision-making by the latter and if it is in accordance with national law); storing separately health data covered by medical secrecy from other categories of personal data held by the employer. Security measures should be taken to prevent persons outside the medical service having access to the data.

2.5.8.3 Article 29 Working Party on personal data processing at work[65]

The WP29 Opinion highlights the risks of monitoring technologies used to process employee personal data, including: chilling effects on confidential communications between employees, incompatible further processing of employee data, unjustifiable and intrusive employee surveillance, and obstructing an employee's ability to report colleagues' and superiors' illegal actions.[66]

The Opinion identifies nine different data processing at work scenarios where new technologies have, or may have, the potential to result in high risks to employees' privacy. **The ones that could be relevant for the HR-Recycler project include processing operations** (1) resulting from in-employment screening, (2) resulting from monitoring ICT usage at the workplace, (3) resulting from monitoring ICT usage outside the workplace, (4) relating to time and attendance, (5) using video monitoring systems, (6) involving disclosure of employee data to third parties, and (7) involving international transfers of HR and other employee data.[67]

The Opinion alerts for the following:

- Consent cannot form a valid legal basis due to the imbalance of power between employers and employees. Valid grounds may include, processing being necessary for the performance of the employment contract (e.g. pay salary) or processing data in connection with obligations imposed by employment law (e.g. tax calculation);
- Relying on the legitimate interest ground to process employee data, the processing must be *strictly necessary* for a legitimate purpose and must be *proportionate* to the business need. A proportionality

[64] Council of Europe, Committee of Ministers (2015), Recommendation (2015) to Member States on the processing of personal data in the context of employment, April 2015, https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf, accessed 29 May 2019.

[65] WP29, Opinion 2/2017 on data processing at work, 8 June 2017.

[66] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/07/Opinion22017ondataprocessingatwork-wp249.pdf, accessed 20 May 2019.

[67] Ibid.

test should be carried out prior to the deployment of any monitoring tool to consider whether all data are necessary, whether the processing outweighs the general privacy rights that employees have in the workplace, and whether appropriate measures have been put in place to ensure a balance with the rights and freedoms of employees;

- **Employees must be informed of the existence of any monitoring and the purposes for the monitoring. Policies relating to workplace monitoring must be clear and readily accessible;**[68]
- Data processing at work must be a proportionate response to risks faced by an employer. For example, if it is possible to block websites, instead of continuously monitoring all communications, blocking should be chosen;
- **Health data processed by wearable devices should be accessible only to the employee and not the employer. The reason for this is that data in this context is unlikely to be truly anonymous and employees are not able to provide free consent to an employer;**
- **Employers should refrain from using facial recognition technologies in the context of video analytics at the workplace, as this may be deemed disproportionate;**
- **Employers must take the principle of data minimisation into account when deciding on the deployment of new technologies. Information should be stored for the minimum amount of time necessary and deleted when no longer needed, and the employer should have a specified retention period;**
- Use of most cloud applications may result in the international transfer of employee data. Any transfers to third countries may take place only where an adequate level of protection is ensured, and data shared outside the EEA and accessed by other entities within the organisation must remain limited to the minimum necessary for the intended purposes. [69]

2.5.9 Transfers of personal data within and outside the EU

The GDPR distinguishes between transfers of personal data within the EU and transfers to third countries.

The general principle regarding transfers of personal data within the EU is the free movement/flow of personal data (Article 1(3) of the GDPR): *"The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data"*.

For transfers of personal data to third countries, the GDPR foresee specific conditions specified in Chapter V – Articles 44-50. In brief, transfers of personal data may take place on the basis of i) an **adequacy decision** by the European Commission. The CJEU has clarified that the country in question needs to offer an adequate level of protection, meaning that is must be 'essentially equivalent' as the EU level;[70] or, ii) in the absence of such an adequacy decision, the controller or processor provides **appropriate safeguards**, including enforceable rights and legal remedies for the data subject; iii) in the absence of either an adequacy decision or appropriate safeguards, a number of derogations are available.

[68] Concerning the involvement of employees and their representatives prior to any monitoring measures see in this sense Clara Fritsch, Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite, in Gutwirth S., Leenes R., de Hert P. (eds), 'Reforming European Data Protection Law', Law, Governance and Technology Series, vol 20, Springer, Dordrecht , 2015, p 147-167, p 152.

[69] Ibid.

[70] CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015, para. 96.

HR-Recycler project: No data collected during the tests and the demonstrations will be sent or processed outside the EU. Personal data will be stored and processed in the local and secure servers of the relevant consortium partners.

2.6 Safety

Industrial collaborative robots are designed to be in direct interaction with humans in the same workspace. The risk of workers injuries can result from engineering errors and human errors. Engineering errors include errors in robot's mechanics (e.g., loose connections across parts, faulty electronics) and errors in programming (e.g., bugs, faulty algorithm, connecting sensors). Human errors include errors in judgement related to control panels and workers becoming too familiar with robot's surplus gestures, placing themselves in hazardous positions.[71]

The International Organization for Standardization (ISO) has developed specific requirements and guidelines related to safe design, protective measures and information for use of industrial robots. In particular, the **ISO standards governing robot safety include ISO 10218-1:2011 and ISO 10218-2:2011 Safety requirements for industrial robots, Parts 1[72] and 2[73]; ISO/TS 15066:2016 Safety requirements for collaborative robots**.[74] These standards relate to the introduction of protective devices with safety functions (e.g. force and speed limitation, padding and soft/round covers, constrain toll orientation – e.g. downward) and of protective measures (e.g. free escape space, alerts and signalling).[75]

In Europe, safety is regulated through the **EU Machinery Directive**.[76] The Directive applies to products that are to be placed on the EU market for the first time and promotes harmonisation of health and safety requirements by combining mandatory and voluntary harmonised standards. The directive covers machinery, interchangeable equipment, safety components, lifting accessories, chains, ropes and webbing, removable mechanical transmission devices and partly completed machinery. Manufacturers must: i) carry out a risk assessment to identify which health and safety requirements apply to their machinery; ii) keep the risk assessment in mind when designing and building their machinery; iii) determine what limits there are on using the machinery; iv) identify any possible hazards; v) assess the risk of their machinery causing severe injury or damage and take action to make their machinery safer; vi) make sure that their machinery complies with the essential health and safety requirements listed in Annex I to the directive; vii) provide a technical document confirming that the machinery meets the directive's requirements; viii) make sure that they are applying conformity assessment procedures and that they are making all necessary information available, including instructions for assembly and use; ix) check that they have filled in the EC declaration of conformity and that the CE conformity marking has been put on the machinery so that it can be used anywhere in the EU.

---

[71] Vladimir Murashov, Frank Hearl, John Howard. (2016) Working safely with robot workers: Recommendations for the new workplace. Journal of Occupational and Environmental Hygiene 13:3, pages D61-D71.

[72] https://www.iso.org/standard/51330.html

[73] https://www.iso.org/standard/41571.html

[74] https://www.iso.org/standard/62996.html;

[75] Federico Vicentini, slides on Safety of collaborative robots, ETUI/EFBWW Conference Improving Machinery Safety: new technologies, automation, robotics and the new Machinery Directive, 11-12 February 2019, Brussels, https://www.etui.org/content/download/36046/359644/file/2019_ETUI_vicentini_collaborative+robotics.pdf, accessed 19 may 2019.

[76] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042, OJ L 157, p. 24–86

In the US, the safe application of robots is regulated by the Occupational Safety and Health Administration (OSHA) Guidelines for Robotic Safety.[77] The American National Standards Institute (ANSI) has also published the American National Standard for Industrial Robots and Robot Systems – Safety requirements and the U.S. National Institute for Occupational Safety and Health (NIOSH) published preventing the injury of workers by robots.

HR-Recycler project: The robotic system, the training of workers and their supervision should be designed and developed in a way that prevents injuries and ensures workers utmost safety. The EU Machinery Directive may be of application.

2.7 Privacy and protection of personal data in HR-Recycler Project

KEY POINTS:

- The emergence of HRIs evokes new types of interference with the right to privacy and the right to the protection of personal data of the individual. The understanding of the categories of data collected, reflecting emotion, attention, cognition and physiological information needs to continue to be thoroughly assessed.
- The HR-Recycler consortium expects that the interference to the right to privacy and protection of personal data upon the users (workers) will be limited to what is necessary and proportional to the objectives that the project in its entirety requires (e.g. testing of the pilots, final results, dissemination activities including the website), and that it will not affect the essence of those rights. The data collection will be compliant with the respective legal requirements at EU and national level and meet a public interest of developing scientific research in the area of robotics, HRI and artificial intelligence.
- The HRI will necessarily gather data on individual workers and work-related activities. Personal data will be collected and used only for the purpose related to the project and will not be used to take any measures that effect the rights of workers to privacy in the workplace.
- Nonetheless, as precautionary measure from a privacy and personal data protection perspective, and as a goal of the Work Package 2 (WP2), particular attention is given to the implementation of the system and on whether the workers' personal data is effectively used to monitor their work performance and behaviour. Appropriate safeguards would need to be put in place as it could be a source of concern for workers, their representative organisations within the company and outside (trade unions) but also for society as a whole (if it is considered to be the beginning of a 'new industrial era'). For example, automated decision-making evaluating or 'indirectly' analysing aspects concerning a worker's performance at work capable of producing legal effects concerning him/her would need to be based on the explicit consent of the worker and be subject to suitable safeguards (e.g. right to obtain an explanation of the decision reached and to challenge a decision), pursuant to Article 22(2)(c), (3) and recital 71 of the GDPR.[78] The worker could also obtain, under the right of access, meaningful information about the logic involved.[79]

[77] https://www.osha.gov/enforcement/directives/std-01-12-002

[78] Article 29 Working Party, Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679, WP 251, 3 October 2017. Other situations allowing the use of automated decision-making are described in Article 22(2)(a) and b) of the GDPR.

[79] Article 15(1)(h) of the GDPR. Under the right of access, it is considered acceptable that: *"a health insurance company using automated decision-making on applications should provide data subjects with general information on how the algorithm works and which factors the algorithm uses to calculate their insurance premium"*, in the FRA, Handbook on European Data Protection Law, p 234.

- The HR-Recycler consortium and WP2 activities will take particular attention on whether any collection of personal data can cause particular physical or mental discomfort to the data subject affected; if there can be any other methods that should be considered more effective concerning the collection of personal data and still allow achieving the same goals of the project; if there will be any operations that can be considered of an intimate nature (i.e. by intimate it should be understood as something that is generally not seen by others).
- HR-Recycler consortium and WP2 will be particular vigilant on whether the surveillance activities that are not likely to use personal information from workers (e.g. camera with blur faces or pointing to working line only) still infer psychological pressure upon them, causing workers a compelling feeling to alter their behaviour. The fear of being monitored can bring consequences to their sense of privacy.
- The impact assessment against the VUB TARES framework (deliverable D2.3 due in month 12) will ensure that any high risks that are likely to occur to the rights and freedoms of the workers which result from the processing operations of their data or work-related activities (e.g., collection, use, access, sharing, transfer, storage, consultation, disclosure, recording, organisation, erasure, restriction, destruction), in the employment context, will be addressed and mitigated to ensure compliance with the privacy and data protection rules. In particular, if the processing may give rise to discrimination, damage to the reputation, financial loss or any other significant economic or social disadvantage, unauthorised access to personal data or unauthorised reversal of pseudonymisation, loss of confidentiality, inability to exercise rights, inability to access services or opportunities, loss of control over the use of personal data, physical harm, predicting aspects concerning performance at work in order to create or use personal profiles, modification of personal data, undue back doors, loss/disappearance of personal data, privacy interferences (e.g. systematic and permanent record of information related to life/habits of workers, exploitation and surveillance) and ethical interferences (e.g. algorithmic bias, loss of dignity, significant humiliation, injury of data subjects feelings, trust erosion, harming workers autonomy), etc.
- The purpose of processing in HR-Recycler project is conducting research, in particular the training and evaluating computer algorithms, in adherence to article 89 of the GDPR.
- The legal basis for the processing of personal data is the consent of the research participant pursuant to articles 6(1)(a) and 9 of the GDPR.

3 Ethical and Societal Concerns

3.1 Ethical principles

In the industrial field the classic ethical tensions that can arise relate to the relation between employers and employees and the techniques used to scale up production and profit maximisation in detriment of certain values and ethical principles. In a robotic industrial world, new tensions may appear.

The HR-Recycler project proposed to analyse in WP2 the ethical HRI scenarios under the ethical principles of truthfulness, appropriateness, ethical handling of data relating to employees, stigmatisation and discrimination arising from the HR-Recycler practices.

This section does not intend to be comprehensive, but rather pragmatic and exploratory to help having a clear overview what can lie ahead. The answers to the questions below should be discussed throughout the project and further reported in the next deliverables D2.3, D2.4, D2.5 and D2.6.

3.2 Ethical concerns and societal acceptance

The use of robots in factories to optimise the recycling process of electronic equipment is increasing. They can have positive effects on workers, as they eliminate dangerous, monotonous, time-consuming and heavy tasks, diminish the health and safety risks for human workers due to potentially hazardous waste materials often processed in the plant and provides the opportunity for workers to focus on higher-skilled, higher-quality and higher-paid tasks. But also, negative, if they render the workers redundant facing the risk of being laid off, possible de-humanisation of the workforce (if workers are subjugated to robots' behaviour and pace) and face-to-face human interaction reduced.

The robots of the HR-Recycler project are of a collaborative nature, so certain fears (e.g. mass unemployment from plants workers) should be excluded. Nonetheless, end-users will be adapting and streamline plants working environment. The classic platforms for workers to proceed with classification, dismantle and sorting of materials for further recycling will change, as well as the tasks executed by them, some of which replaced by automatic robotic-based procedures.[80]

3.2.1 What consequences to workforce industry?

These collaborative robots are introduced to solve certain challenges in the recycling industry, in particular the low recycling rates, considering the amount of new electric and electronic devices generated every year, and the hard-working conditions of employees when carrying out certain tasks in the plant.

- Are these technological solutions the best way to deal with these challenges?
- What consequences will the introduction of these robots have for the European recycling industry?
- Are these collaborative industrial robots a threat to jobs or any kind of 'craftsmanship' in recycling factories?
- Will human workers be turned into 'tools of tasks' decided by robots and their algorithms? Or are the machines the workers' partners?
- Will workers be free from routine and repetitive tasks or will they be restricted having no room for manoeuvre or free will?

[80] The Institute of Electrical and Electronics Engineers (IEEE), an international technical professional organisation, has taken a a global initiative to produce guidelines for ethical design and prioritise human well-being with autonomous and intelligent systems. The first edition of the 'Ethically Aligned Design' can be downloaded here https://ethicsinaction.ieee.org, accessed 6 June 2019.

Some of these questions have been made by trade unions in Europe which in general are, according to the International Federation of Robotics (IFR), positive about the potential of automation for higher-skilled, higher paid and more satisfying jobs. However, they stress the need for workers to be involved in process design and the importance of continuous training and up-skilling (European Trade Union Institution 2016), (Trades Union Congress 2017).[81]

HR-Recycler project should ensure a positive involvement from workers in process design and during pilots, and continuous training and up-skilling competencies.

3.2.2 What consequences to human relations in the factory?

A fear that work relations will be de-humanised, as well as lack of empathy and warmth among colleagues are relevant points to consider. Human workers have different social and emotional needs. Appraisals and recognition of their value are indispensable for a good working environment.

- Will the lack of human contact be compensated by other activities/relations involving only human workers?

HR-Recycler project should ensure that the automation does not lead to an impoverishment of social relations and communication within the plant. Particular attention should also be given to workers' motivation and wellbeing.

3.2.3 What consequences for human-robot interaction?

The science fiction author Isaac Asimov as formulated three laws of robotics:

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given to it by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

The writer later added another law which overrides the previous ones: *'0. A robot may not harm humanity, or, by inaction, allow humanity to come to harm.'* Although these laws are fictional, they can be used to define a general ethical framework concerning the problems associated with robotics and artificial intelligence.[82]

Points to reflect upon throughout the HR-Recycler project:[83]

- **Autonomy** – the project foresees that the robot carries out certain tasks without the continuous guidance and assistance of the human worker. What will be the level of autonomy of the robot? Will there always be human supervision?

---

[81] IFR, Paper on Robots and the Workplace of the Future, March 2018, https://www.ifr.org/downloads/papers/IFR_Robots_and_the_Workplace_of_the_Future_Positioning_Paper.pdf, accessed 18 May 2019.

[82] In this sense see European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf, accessed 6 June 2019.

[83] Bernd Carsten Stahl and Mark Coeckelbergh, Ethics of healthcare robotics: Towards responsible research and innovation, Robotics and Autonomous Systems 86 (2016), p 152-161.

- **Role and tasks** – in the production process, what should be the role and tasks of the robot and of the human? When should they do what?
- **Moral agency** – robots do not seem to have the capacity of moral reasoning or of dealing with problematic ethical situations. When a moral dilemma arises, in a human-robot interaction model, who should deal with that situation? Are there ethical aspects that can be imbedded in the system from the start? A specific deliverable will be dealing with this aspect - D2.4 – Moral actions based on an ethics engine, due in month 24. The aspects of autonomy and role should also be address in this point.
- **Responsibility** – this point is also related with autonomy and role. If the robot takes over certain human-tasks, who will be responsible for those tasks? If the factory representatives are the ultimate responsible, considering that the robot cannot be morally responsible, how can they exercise this responsibility if they do not have direct control over the robot or do not continuously supervise the robot?
- **Trust** – when performing its tasks, the robot will be placed physically near the human worker; autonomous systems are prone to error. Can the robot be trusted not to hurt a human? How to inject the socio-emotional elements of interpersonal human team dynamics into human-robot teams?[84] What impact (positive/ negative/ indifferent) could there be to human relations the creation of deep bonds between humans and robots? The risk of overtrusting the robot could also occur. [85]
- **Safety and avoidance of harm** – robots should not harm workers and should be safe to work with. Is the robot safe?
- **Privacy and data protection** – the use of robotics in the employment contexts raises questions about which data is collected, how it is stored and used, who has access to it, who owns such data, etc. Does the robot provide sufficient technical safeguards and respect privacy by design and by default?
- **Explainability** – people should have the right to know why a decision that affects them is taken. If a decision cannot be explained, that is considered unjust. Using machine learning systems where outcomes (recommendations) are not technically understandable because they cannot be traced back to a chain of decisions or reasoning, as in the case of decision tree models, raises the problem of transparency and explainability.[86] Can the AI and machine leaning system in the project take any decision that cannot be explained which could affect workers?
- **Bias** – means that some individuals or groups are disadvantaged by the outcome of the system. It can arise during the various stages of machine learning and data science process, such as in the selection of the data set, in the training of the data set, in the algorithm used, in the applicating of the data set, etc.[87] Can there be any AI technology used in the HR-Recycler project that could be biased and discriminate workers in an unfair and unjust way? Could such AI perpetuate or increase the impact of bias and discrimination to workers?

The has EU set up a High-Level Expert Group on AI (HLEG AI) which published the '*Ethical Guidelines for Trustworthy AI*'.[88] According to the HLEG AI, a trustworthy AI system has three components:

1) it should be lawful, complying with applicable laws and regulations;
2) it should be ethical, adhering to ethical principles and values; and,

---

[84] Jesse Kirkpatrick, Erin N. Hahn, and Amy J. Haufler, Trust and Human-Robot Interactions, Chapter 10 in *Robot Ethics 2.0 from autonomous cars to artificial intelligence*, edited by Patrick Lin, Ryan Jenkins and Keith Abney, 2017, Oxford University Press, p142-156, p 148.

[85] Ibid.

[86] Mark Coeckelbergh, Ethics of artificial intelligence: Some ethical issues and regulatory challenges, Technology and Regulation, 2019, p 31–34 • https://doi.org/10.26116/techreg.2019.003 • ISSN: 2666-139X, p 32.

[87] Ibid.

[88] The Guidelines are available at https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.

3) it should be robust, from a technical and social perspective (good intentions).

The Guidelines deal with points 2 and 3, listing seven key requirements that AI systems should meet in order to be trustworthy: i) human agency and oversight; ii) technical robustness and safety; iii) privacy and data governance; iv) transparency; v) diversity, non-discrimination and fairness; vi) societal and environmental well-being; and vii) accountability.

3.3 Avoiding stigma and discrimination

Stigma *"refers to attitudes and beliefs that lead people to reject, avoid, or fear those they perceive as being different."*[89] The word 'Stigma' comes from Greek and it referred to a kind of mark that was cut or burned into the skin. It identified people as criminals, slaves, or traitors to be shunned.[90] Discrimination follows stigma and *"occurs when individuals or institutions unjustly deprive others of their rights and life opportunities (…). Discrimination may result in the exclusion or marginalization of people and deprive them of their civil rights, such as (…) opportunities for employment, education, and full participation in civic life. (…) Discrimination includes 'disparate or different treatment'"*. [91]

Concerning HR-Recycler, stigmatisation might be an accidental consequence and the harmfulness depends on the perception reflected by workers or local community. Individuals wrongly stigmatised can fuel division and tensions or be less cooperative. If such a risk is likely to occur, it needs to be addressed both in the design and implementation of the HR Recycler project.

HR-Recycler project – the HRI ethical scenario:

- Introducing robots is part of an evolution of the industrial process. Tasks that are repetitive and dangerous may be delegated to automated machines, and tasks that require recognition of materials, fine motor skills but also creativity, social skills, emotional intelligence may be assigned to human workers.
- There are already some early examples of robots and people teaming up. For example, soldiers use drones for surveillance and ground robots for bomb disposal as they carry out military missions. These human-robot teams will soon start working in other fields, such as manufacturing.[92]
- It is important to continue to scrutinise the effect that this new technology can bring to the sector and if it will only benefit a segment of society, and if the gains in productivity can lead to higher wages and fewer working hours are shared with the working class.
- The evaluation of ethical and social consequences of technology should be done together with designers, engineers, end-users and other partners in the consortium. Involving external stakeholders could be beneficial and relates to the idea of responsible innovation implementation.
- Workers should not experience physical and psychological pressure. Workers should be offered reassurance that by working together with a robot their working conditions will not be subsumed to the fast and consistent pace of robots. Robots should be placed to serve workers and not workers serving robots (dehumanisation effect). Assurances also in case of work intensity, workers

[89] https://www.disabilityrightsca.org/system/files/file-attachments/CM0401.pdf, accessed 20 May 2019.
[90] Ibid.
[91] Ibid.
[92] Nancy Cook, Here are 5 ways we can help robots and people work together, 28 November 2018, https://www.weforum.org/agenda/2018/11/5-ways-to-help-robots-work-together-with-people/, accessed 20 April 2019.

should receive adequate compensation translated by a higher salary or similar benefit which reflects the extra effort.

- Robots will not replace human workers, as the factory assembly line is being conceived in a way that the human is part of the process. Grasping and manipulation capabilities of robots are still very limited, and automatically learning new tasks by themselves or by human demonstration requires time and repetition.
- AI ethics is a key component. As proposed by the High-Level Expert Group on AI, AI principles should be based **on fundamental rights** (human dignity, freedom of the individual, respect for democracy, justice and the rule of law, citizen's rights and freedoms) and **ethical principles** [no harm (requiring AI algorithms to avoid discrimination, negative profiling, manipulation, etc.) and, explainability,[93] that is traceability technically ensured].

[93] Mark Coeckelbergh, Ethics of artificial intelligence, p 32-33.

4 Collection of best practices of Human Robots Interaction for the protection of personal data

This section aims at providing best practices on the processing of personal data in an HRI scenario in the context of a workplace cell.

The International Federation of Robotics (IFR) has confirmed that the most common collaborative robot applications are shared workspace applications where robot and employee work alongside each other, completing tasks sequentially. Case studies presenting real-world collaborative applications of different collaboration intensity can be found on the IFR's website (https://ifr.org/case- studies/collaborative-robots).[94]

At this early stage of the project, it is difficult to ascertain what personal data robots will effectively collect from human workers on a daily basis for the cell to function and consequently what should be the essential recommended safeguards to be put in place to protect workers privacy and data protection and unwanted disclosure of personal information.

Nonetheless, the recommendations below are based on the **WP29 Opinion 2/2017** of 8 June 2017 on data processing at work.[95] The WP29 highlights that is important that data is not used to single out individual workers with particular health indications such as high blood pressure or obesity. In addition, a robot that tracks workers time and attendance, can be very invasive. There needs to be a justification, a legal basis and workers need to be aware of that practice. Concerning the use of videos, the WP29 considered that i) the possibility to remotely access personal data collected via smartphone or another network system, ii) the high definition of cameras and the reduction of their sizes, iii) the processing made by video analytics (e.g. facial recognition systems), or iv) the possibility of seeing facial expressions of workers as they deviate from the pattern movements, can be very invasive and disproportionate. Overall, these systems are capable of continuous capture of the behaviour of workers. The WP29 added that the tracking of employees should be limited to what is strictly necessary for a legitimate purpose (which can be the legitimate interests of the employer) and comply with the principle of proportionality and necessity. The proportionality test should be conducted prior to the monitoring activity to consider i) whether all data are necessary, ii) the processing outweighs the right to privacy and protection of personal data of employees and their freedom of expression, and iii) which measures should be taken to ensure that limitations to those rights and freedoms are restricted to the minimum necessary. Effective communication should be provided to employees concerning any monitoring, the purposes of the monitoring, and the circumstances, as well as the possibilities, if any, to prevent their personal data being captured in monitoring technologies. The policies and rules considering legitimate monitoring must be clear and readily accessible. The information registered from the ongoing monitoring as well as the information shown to the employers should be minimised, as much as possible. The principle of data minimisation should be taken into account when deploying the HRI and the information should be stored for the minimum amount of time needed with a retention period specified. Whenever the information is no longer needed, it should be deleted. The use of a cloud service to store the data from the HRI needs to take into account the GDPR rules about the transfer of personal data outside the EU if that is the case.

[94] International Federation of Robotics (IFR), Position Paper on Demystifying Collaborative Industrial Robots, December 2018, https://www.ifr.org/downloads/papers/IFR_Demystifying_Collaborative_Robots.pdf, accessed 18 May 2019.

[95] WP29 Opinion 2/2017 of 8 June 2017 on data processing at work, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631

5 Relevant Regulatory Frameworks in Member States

The HR-Recycler project will need to take into consideration national legislative frameworks. The GDPR contains many open clauses which need to be filled in by national legislation.[96] There can be differences concerning the **implementation of data processing in the context of employment** pursuant to Article 88 of the GDPR. Specifically, Member States may by law or by collective agreement provide for more specific rules to ensure the protection of the rights and freedoms of employees' personal data, in particular in relation to planning and organisation of work, equality and diversity in the workplace, health and safety at work, etc. Such rules need to ensure suitable and specific measures to safeguard employees' (data subject) human dignity, legitimate interests and fundamental rights, with specific attention to the transparency of processing, the transfer of personal data within a group of enterprises engaged in a joint economic activity and monitoring systems at the work place. There can also be different regimes concerning the **use of video surveillance systems**.

The present chapter does not intend to be exhaustive, but to illustrate relevant legal provisions and different legal regimes that can be relevant to the HR-Recycler project.

5.1 Germany

The Federal Data Protection Act (FDPA) (*Bundesdatenschutzgesetz, BDSG*), which previously implemented the 95/46/EC Data Protection Directive, supplements the directly applicable General Data Protection Regulation (GDPR) on certain 'open clauses' in the GDPR. Furthermore, it regulates the processing operations of the federal state and of the 16 states when they implement federal law. The GDPR is further supplemented by the data protection laws of the states (Länder). Each federal state has its own independent supervisory authority, which can be contacted on data protection issues.

The State of Bavaria has two different supervisory authorities for data processing by public and private bodies. On a national level, Germany has its own supervisory authority, which is primarily responsible for data processing by federal public authorities.

5.1.1 Video Surveillance Systems and employees

Systematic monitoring of publicly accessible areas on a large scale (e.g. using CCTV) implies that a DPIA must be undertaken with the assistance of the Data Protection Officer (DPO). For private entities, the CCTV must be necessary for the purposes of the legitimate interests pursued by the controller or a third party and those interests cannot override the interests of the data subject (section 4 FDPA). If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals, the controller must consult the data protection authority (DPA) prior to any action being taken. If the DPA is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks.[97]

Employee monitoring is only allowed in very strict circumstances, for example to discover criminal conducts or severe breaches of employees' contractual obligations (section 26 FDPA). Sporadic monitoring for quality and training purposes may be allowed if not excessive and formal requirements are met (e.g. the employer must provide a detailed notice before to the employee and if a works council exist, the agreement of this body is usually required, and employees should be informed about such agreement). Section 87(1) and (6) of

[96] https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/, accessed 4 June 2019.

[97] https://iclg.com/practice-areas/data-protection-laws-and-regulations/germany, accessed 4 June 2019.

the Works Constitution Act (*Betriebsverfassungsgesetz*) requires that the works council must be informed and agree to all measures that concern how employees' behaviour is regulated and whenever technical means to monitor employees' behaviour and performance are to be introduced. [98]

HR Recycler project: employee monitoring for research purposes will only be of a temporary nature and therefore could fit in the previous situation if formal requirements are met. However, as pilots are to occur within end-users' premises, this situation is only hypothetical.

5.2 Greece[99]

The Hellenic Data Protection Authority (HDPA) is a constitutionally consolidated independent Authority. The Hellenic Data Protection Authority was established with Law 2472/97, which incorporates into the Greek law the Data Protection Directive 95/46/EC. In addition, the Hellenic Data Protection Authority implements Law 3471/2006 with respect to the electronic communications sector which incorporates into the Greek law European Directive 58/2002.[100]

A bill of law, implementing the GDPR into Greek national law, was published on February 20, 2018 and was submitted afterwards to public consultation. This Bill provides for both the legal measures implementing the Regulation 2016/679 (GDPR) in Greece, as well as the integration into the Greek legal order of Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Despite the fact that public consultation has been completed, the Bill has not been enacted yet. It is expected to be finalized in the very near future though.

5.3 Portugal[101]

The Portuguese data protection authority is CNDP - Comissão Nacional de Protecção de Dados.[102] It is an independent body with powers to act throughout the entire Portuguese national territory. It has been assigned the tasks and powers foreseen under Articles 57 to 59 of the GDPR.

5.3.1 Portuguese Constitution

This is the most relevant legal document in Portugal which guarantees fundamental rights and freedoms to the people of Portugal and establishes the basic principles of democracy, ensuring the primacy of a democratic state based on the rule of law. Articles 26(1) and 35 of the Portuguese Constitution are relevant.[103]

---

[98] Ibid.

[99] Industrial background general information about Greece: https://www.etui.org/ReformsWatch/Greece.

[100] http://www.dpa.gr/

[101] Industrial background general information on Portugal: https://www.etui.org/ReformsWatch/Portugal

[102] www.cndp.pt

[103] https://wipolex.wipo.int/en/text/206670. Article 26(1) (Other personal rights): *"1. Everyone shall possess the right to a personal identity, to the development of their personality, to civil capacity, to citizenship, to a good name and reputation, to their likeness, to speak out, to protect the privacy of their personal and family life, and to legal protection against any form of discrimination.";* Article 35 (Use of computerised data): *"1. All citizens have the right of access to any computerised data relating to them and the right to be informed of the use for which the data is intended, under the law; they are entitled to require that the contents of the*

5.3.2 Act Proposal 120/XIII

Portugal is preparing a draft implementing act of the GDPR, Act Proposal 120/XIII[104], and its procedure took longer than expected. For this reason, the act which transposed the Data Protection Directive - Act 67/98 of 26 of October transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - is still in place in everything that does not go against the GDPR.

5.3.3 Portuguese Labour Code

Law 7/2009 of 12 February 2009, as amended by Law 53/2011 of 14 October 2011, Law 23/2012 of 25 June 2012, Law 47/ 2012 of 29 August 2012, Law 69/2013 of 30 august 2013, Law 27/2014 of 8 May 2014, Law 55/2014 of 25 August 2014.

The relevant articles are 16 (right to privacy), 17 (right to the protection of personal data), 18 (biometric data), 20 (surveillance systems at distance), 21 (the use of surveillance systems at distance)

Most rules are mandatory and therefore can only be modified by collective agreements or agreements between the parties if such amendment is intended to improve the position or rights of the employees.

5.3.4 Video surveillance Systems and employees

The draft implementing act of the GDPR will contain rules on video surveillance when the purpose is to protect people and goods (Article 19). At present, **Law 34/2013,** concerning the adoption of security measures including rules on the use of video surveillance tools by public or private entities to prevent crimes, continues to apply.[105] In case of (permanent) monitoring, the definition of its form and conditions should be specified in the company's internal Rules of Procedure.[106]

An important ruling of the Portuguese Supreme Court of 8 March 2006 defined the conditions under which employers can use video surveillance systems at the workplace.[107] The Court considered unlawful, for violating the right to private life, to capture images through video cameras installed in the workplace and directed to workers, in such a way that the work activity is subject to a continuous and permanent observation.

---

files and records be corrected and brought up to date. 2. The law shall determine what are personal data as well as the conditions applicable to automatic processing, connection, transmission and use thereof, and shall guarantee its protection by means of an independent administrative body. 3. Computerised storage shall not be used for information concerning a person's ideological or political convictions, party or trade union affiliations, religious beliefs, private life or ethnic origin, except where there is express consent from the data subject, authorisation provided under the law with guarantees of non-discrimination or, in the case of data, for statistical purposes, which does not identify individuals. 4. Access to personal data of third parties is prohibited, except in exceptional cases as prescribed by law. 5. Citizens shall not be given an all-purpose national identity number. 6. Everyone shall be guaranteed free access to public information networks and the law shall define the regulations applicable to the transborder data flows and the adequate norms of protection for personal data and for data that should be safeguarded in the national interest. 7. Personal data kept on manual files shall benefit from protection identical to that provided for in the above articles, in accordance with the law."

[104] *"Proposta de Lei 120/XIII, Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados"*, https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368, accessed 24 May 2019.

[105] *"Lei 34/2013 de 16 de Maio que estabelece o regime do exercício da atividade de segurança privada e procede à primeira alteração à Lei n.º 49/2008, de 27 de Agosto (Lei de Organização da Investigação Criminal)"*, https://dre.pt/web/guest/pesquisa/-/search/261089/details/maximized, accessed 24 May 2019.

[106] https://iclg.com/practice-areas/data-protection-laws-and-regulations/portugal, accessed 4 June 2019.

[107] http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/65e859e4729cc7688025712d00421026?OpenDocument

5.4 Spain[108]

The Spanish data protection authority is the AEPD - Agencia Española de Protección de Datos.

The Law 3/2018 on data protection and digital rights ('Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales') implemented the GDPR.

5.4.1 Spanish Labour Code

Royal law decree 2/2015 of 23 October, adopting the Employees Statutes Law ("Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores").[109]

Relevant articles are:

- Article 18 (the inviable right of the workers)

"Records of workers can only be made, in their lockers and private areas, when they are necessary for the protection of business assets and that of other workers of the company, within the workplace and during working hours. During its execution, the dignity and privacy of the worker will be utmost and the worker will have the assistance of a legal representative or, in his/her absence, of another worker of the company, whenever this is possible." (free translation from Spanish)

- Article 20 bis (workers' rights to privacy in the digital sphere and to disconnect) which says:

"Workers have the right to privacy in the use of digital devices placed at their disposal by the employer, the right to digital disconnection and privacy against the use of video surveillance and geolocation devices pursuant to the current legislation on the protection of personal data and guarantee of digital rights." (free translation from Spanish).

5.4.2 Video surveillance Systems and employees

- Guide on video surveillance for security and other purposes ("Guía sobre el uso de videocámaras para seguridad y otras finalidades"), https://www.aepd.es/media/guias/guia-videovigilancia.pdf
- AEPD legal opinions on the use of cameras:
  - https://www.aepd.es/media/fichas/ficha-videovigilancia-control-empresarial.pdf
  - https://www.aepd.es/media/informes/informe-juridico-rgpd-videovigilancia-tiempo-real.pdf
  - https://www.aepd.es/media/informes/informe-juridico-rgpd-videovigilancia-interes-legitimo-parking.pdf
  - https://www.aepd.es/media/informes/informe-juridico-rgpd-camaras-en-tiempo-real.pdf

[108] Industrial background general information about Spain: https://www.etui.org/ReformsWatch/Spain.
[109] https://www.boe.es/legislacion/codigos/codigo.php?id=93&modo=1&nota=0&tab=2, accessed 29 May 2019.

6 Relevant International Frameworks

6.1 International Labour Organization (ILO)

The International Labour Organizations was founded in 1919 to promote social justice and contribute to universal and lasting peace. It brings together governments, employers and workers of 187 Member States, setting labour standards, developing policies and planning programmes promoting decent work for all women and men.[110]

6.1.1 ILO's Code of Practice on the protection of workers' personal data

In 1997, ILO published a first Code of Practice on the protection of workers' personal data. Its objective was to be transversal and provide general guidance when developing new related policies and legislation, drafting collective agreements or even when adopting specific measures within a company. when the collection of workers' personal data was involved. The standards recommended therein have no binding force, but they have been influential over time. They aim at safeguarding workers' dignity, protect their privacy and guarantee their fundamental right to determine who may use which data for what purposes and under what conditions covering general principles and specific provisions regarding data collection, security, storage, use and communication.[111]

The commentary section to the Code of Practice explains that *'the systematic collection and retrieval of personal data has far-reaching consequences. The gathering of a large number of data and the many different uses to which they are put not only multiply the risk of false or misunderstood information, but also permit close monitoring of the persons concerned and intensify tendencies to influence or even to manipulate their behaviour. The less, therefore, that the persons concerned know about who is processing which data for which purposes, the less they are able to assess their individual situation and to express and defend their interests: in short, they have difficulty in determining their own personal development. The quest for principles to govern the processing of personal data expresses, therefore, the need to protect human dignity."*

Below a copy of relevant provisions for the HR-recycler project:

Article 5

General principles

5.1. Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.

5.2. Personal data should, in principle, be used only for the purposes for which they were originally collected.

5.3. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context.

[110] https://www.ilo.org/global/about-the-ilo/lang--en/index.htm, accessed 28 May 2019.
[111] https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf, p V, accessed 28 May 2019.

5.4. Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.

5.5. Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.

5.6. Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance.

5.7. Employers should regularly assess their data processing practices:

(a) to reduce as far as possible the kind and amount of personal data collected; and

(b) to improve ways of protecting the privacy of workers.

5.8. Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights.

5.9. Persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role in the application of the principles in this code.

5.10. The processing of personal data should not have the effect of unlawfully discriminating in employment or occupation.

5.11. Employers, workers and their representatives should cooperate in protecting personal data and in developing policies on workers' privacy consistent with the principles in this code.

5.12. All persons, including employers, workers' representatives, employment agencies and workers, who have access to personal data, should be bound to a rule of confidentiality consistent with the performance of their duties and the principles in this code.

5.13. Workers may not waive their privacy rights.

Article 6

Collection of personal data

(…)

6.14.

(1) If workers are monitored they should be informed in advance of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers.

(2) Secret monitoring should be permitted only:

(a) if it is in conformity with national legislation; or

(b) if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing.

(3) Continuous monitoring should be permitted only if required for health and safety or the protection of property.

Article 8

Storage of personal data

(…)

8.2. Personal data covered by medical confidentiality should be stored only by personnel bound by rules on medical secrecy and should be maintained apart from all other personal data.

Article 12

Collective rights

12.1. All negotiations concerning the processing of workers' personal data should be guided and bound by the principles in this code that protect the individual worker's right to know and decide which personal data concerning that worker should be used, under which conditions, and for which purposes.

12.2. The workers' representatives, where they exist, and in conformity with national law and practice, should be informed and consulted:

(a) concerning the introduction or modification of automated systems that process worker's personal data;
(b) before the introduction of any electronic monitoring of workers' behaviour in the workplace;
(c) about the purpose, contents and the manner of administering and interpreting any questionnaires and tests concerning the personal data of the workers.

7 References

Primary Sources

EU treaties and legislation

- Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47
- Charter of Fundamental Rights of the European Union [2012] OJ C326/39
- 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, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119.
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21 November 2018, p 39–98.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4 May 2016.
- Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, OJ L 201 (Directive on privacy and electronic communications or e-Privacy Directive).
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

National Legislation

- "Proposta de Lei 120/XIII, Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368, accessed 24 May 2019.

Cases

- CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015.
- CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014.
- CJEU, C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 30 May 2013, para 19.
- ECtHR, I v Finland, N° 20511, 17 July 2008.
- ECtHR, Copland v. the United Kingdom, No. 62617/00, 3 April 2007.
- ECtHR, Z v. Finland, N° 22009/93, 25 February 1997.

Secondary sources

Books

- Fuster, Gloria González, The emergence of personal data protection as a fundamental right of the EU, Vol. 16. Springer Science & Business, 2014.
- Hildebrandt, Mireille, and Serge Gutwirth, eds., Profiling the European citizen – Cross Disciplinary Perspectives, Dordrecht: Springer, 2008.
- Leenes, Ronald, Rosamunde van Brakel, Serge Gutwirth, and Paul De Hert, eds., Data Protection and Privacy: The Internet of Bodies. Bloomsbury Publishing, 2018.

Articles

- Alvarez-de-los-Mozos Esther and Arantxa Renteria, Collaborative robots in e-waste management, Procedia Manufacturing 11 (2017) p 55-62, https://www.sciencedirect.com/science/article/pii/S2351978917303372?via%3Dihub, accessed 28 April 2019
- Akimana Béni-Trésor, Maxim Bonnaerens, Jonas Van Wilder, and Bjorn Vuylsteker, A Survey of Human-Robot Interaction in the Internet of Things, 2017, p 15, https://www.researchgate.net/profile/Bjorn_Vuylsteker/publication/318722691_A_Survey_of_Human-Robot_Interaction_in_the_Internet_of_Things/links/5979adbdaca272177c1f4abc/A-Survey-of-Human-Robot-Interaction-in-the-Internet-of-Things.pdf, accessed 27 May 2019.
- Coeckelbergh, Mark, Ethics of artificial intelligence: Some ethical issues and regulatory challenges, Technology and Regulation, 2019, p 31–34 • https://doi.org/10.26116/techreg.2019.003 • ISSN: 2666-139X
- Dinant, J.-M., Lazaro, C., Poullet Y., Lefever, N. and Rouvroy, A. (2008), Application of Convention 108 to the Profiling Mechanism - Some ideas for the future work of the consultative committee (T-PD), Doc. T-PD 01, p. 3, as cited in FRA Handbook on Preventing Unlawful Profiling (2018).
- Fritsch, Clara, Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite, in Gutwirth S., Leenes R., de Hert P. (eds), 'Reforming European Data Protection Law', Law, Governance and Technology Series, vol 20, Springer, Dordrecht , 2015, p 147-167.
- Kirkpatrick, Jesse, Erin N. Hahn, and Amy J. Haufler, Trust and Human-Robot Interactions, Chapter 10 in Robot Ethics 2.0 from autonomous cars to artificial intelligence, edited by Patrick Lin, Ryan Jenkins and Keith Abney, 2017, Oxford University Press, p142-156.
- Panagiota Tsarouchi, George Michalos, Sotiris Makris, Thanasis Athanasatos, Konstantinos Dimoulas & George Chryssolouris (2017) On a human–robot workplace design and task allocation system, International Journal of Computer Integrated Manufacturing, 30:12, 1272-1279, DOI: 10.1080/0951192X.2017.1307524
- Pham, Q. C., Madhavan, R., Righetti, L., Smart, W., & Chatila, R. (2018). The Impact of Robotics and Automation on Working Conditions and Employment [Ethical, Legal, and Societal Issues]. IEEE Robotics & Automation Magazine, 25(2), 126-128.
- Solove Daniel J., Understanding Privacy, Cambridge Massachusetts: Harvard University Press, Chapter 2, 2008.
- Stahl, Bernd Carsten, and Mark Coeckelbergh. "Ethics of healthcare robotics: Towards responsible research and innovation." Robotics and Autonomous Systems 86 (2016): 152-161.
- Vicentini, Federico, Slides on Safety of collaborative robots, ETUI/EFBWW Conference Improving Machinery Safety: new technologies, automation, robotics and the new Machinery Directive, 11-12 February 2019, Brussels,

https://www.etui.org/content/download/36046/359644/file/2019_ETUI_vicentini_collaborative+robotics.pdf, accessed 19 may 2019.

- Vladimir Murashov, Frank Hearl, John Howard. (2016) Working safely with robot workers: Recommendations for the new workplace. Journal of Occupational and Environmental Hygiene 13:3, pages D61-D71, p. 8, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4779796/#R55, accessed 19 May 2019.
- Voss, Eckhard and Riede, Hannah, Report to the European Trade Union Confederation (ETUC) of September 2018 on Digitalisation and Workers Participation: What trade unions, company level workers and online platform workers in Europe think, https://www.etuc.org/sites/default/files/publication/file/2018-09/Voss%20Report%20EN2.pdf, accessed 18 May 2019.
- Warren Samuel D. & Brandeis Louis D., The Right to Privacy, in Harvard Law Review, 1890, Vol. 4, No. 5, pp. 193-220.

Other secondary sources

- WP29:
  - Guidelines on Automated Individual Decision-Making and profiling for the Purposes of Regulation 679/2016, WP251, 3 October 2017.
  - Opinion 2/2017 on data processing at work, WP 249, Brussels, 8 June 2017.
  - Guidelines on Consent under Regulation 2016/679, 2017.
  - Guidelines on Personal Data Breach Notification under Regulation 2016/679, 2017.
  - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is *"likely to result in high risk"* for the purposes of Regulation 2016/679, 2017.
  - Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 November 2005.
- Council of Europe
  - Data protection leaflet, https://rm.coe.int/leaflet-data-protection-final-26-april-2019/1680943556, accessed 28 May 2019.
  - Recommendation (2015) to Member States on the processing of personal data in the context of employment, April 2015, https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf, accessed 29 May 2019.
  - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.
- European Commission:
  - Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).
- European Data Protection Board (EDPB):
- European Data Protection Supervisor (EDPS):
  - Opinion 5/2018, Preliminary Opinion on Privacy by Design of 31 May 2018
  - 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' [2017] ('Necessity toolkit')
  - 'Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights' [2016]

- European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and 'Autonomous Systems' of 9 March 2018, European Commission, Directorate-General for Research and Innovation, Luxembourg: Publications Office of the European Union 2018.
- European Parliament, Report of the Committee on Legal Affairs of 27 January 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [2017] A8-005/2017
- European Parliament Member's Research Service Briefing, The Internet of Things – Opportunities and Challenges, May 2015, http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf, accessed 27 May 2019.
- European Union Agency for Fundamental Rights (FRA), Handbook on Preventing Unlawful Profiling Today and in the Future: A Guide, Luxembourg: Publications Office of the European Union, 2018.
- European Union Agency for Fundamental Rights (FRA) and Council of Europe, Handbook on European Data Protection Law, Luxembourg: Publications Office of the European Union, 2018 edition.
- High-Level Expert Group on Artificial Intelligence (AI HLEG) set up by the European Commission in June 2018, Ethics Guidelines for Trustworthy Artificial Intelligence (AI), April 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58477, accessed 4 June 2019.
- International Federation of Robotics (IFR)
    - Position Paper on Robots and the Workplace of the Future, March 2018, https://www.ifr.org/downloads/papers/IFR_Robots_and_the_Workplace_of_the_Future_Positioning_Paper.pdf.
    - Media Backgrounder on Artificial Intelligence, May 2018, https://www.ifr.org/downloads/papers/Media_Backgrounder_on_Artificial_Intelligence_in_Robotics_May_2018.pdf.
    - Position Paper on Demystifying Collaborative Industrial Robots, December 2018, https://www.ifr.org/downloads/papers/IFR_Demystifying_Collaborative_Robots.pdf
- RoboLaw project, funded by the European Union Seventh Framework Programme (FP7/2007-2013) under the grant agreement 289092.
- VIRT-EU Project – Values and Ethics for Responsible Technology in Europe, Deliverable 4.1 – First Report – limits of GDPR and innovation opportunities, of 28 December 2017, Horizon 2020, ICT-35-2016 – Enabling Responsible ICT-related research and innovation, Project n° 732027.

Websites and blogs

- www.edps.europa.eu
- www.cndp.pt
- https://www.aepd.es
- http://mathisis-project.eu
- http://forensor-project.eu
- www.robolaw.eu
- https://www.un.org/en/universal-declaration-human-rights/
- https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
- https://www.osha.gov/enforcement/directives/std-01-12-002
- https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c
- https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
- https://ec.europa.eu/info/law/law-making-process/types-eu-law_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en
- https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/07/Opinion22017ondataprocessingatwork-wp249.pdf

- https://www.iso.org/standard/51330.html
- https://www.iso.org/standard/41571.html
- https://www.iso.org/standard/62996.html
- https://wipolex.wipo.int/en/text/206670
- https://www.ilo.org/global/about-the-ilo/lang--en/index.htm
- https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf
- https://ethicsinaction.ieee.org
- https://www.boe.es/legislacion/codigos/codigo.php?id=93&modo=1&nota=0&tab=2
- http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/65e859e4729cc7688025712d00421026?OpenDocument
- http://noticias.juridicas.com/nuevalopd/noticias/13509-los-nuevos-derechos-digitales-reconocidos-por-la-ley-organica-3-2018-de-proteccion-de-datos-y-garantia-de-los-derechos-digitales/
- Industrial background general information, Greece, https://www.etui.org/ReformsWatch/Greece
- Industrial background general information, Portugal, https://www.etui.org/ReformsWatch/Portugal
- https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/, accessed 4 June 2019.:
- Cook Nancy, Here are 5 ways we can help robots and people work together, 28 November 2018, https://www.weforum.org/agenda/2018/11/5-ways-to-help-robots-work-together-with-people/, accessed 20 April 2019.

***