# HR-RECYCLER Deliverable D2.2 Impact Assessment Method

Roda, Sara; Kloza, Dariusz; Konstantinou, Ioulia; De Hert, Paul; Borocz, Istvan Mate; Vouloutsi, Vicky

*Publication date:*
2020

*Document Version:*
Final published version

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**

# D2.2 – HR-Recycler Impact Assessment Method

| | |
|---|---|
| WP number and title | WP2 – D2.2 – HR-Recycler Impact Assessment Method |
| Lead Beneficiary | VUB |
| Contributor(s) | IBEC |
| Deliverable type | Report |
| Planned delivery date | 30/09/2019 |
| Last Update | 27/09/2019 |
| 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 UNIVERSITAET MUENCHEN | 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 | FR |
| 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 |
|---|---|---|---|---|
| 0.1-0.3 | 24/07/2019 | Draft | Sara Roda (VUB) | 1st to 3rd drafts |
| 0.4 | 11/09/2019 | Draft | Sara Roda, Dariusz Kloza, Ioulia Konstantinou, István Böröcz, Paul de Hert (VUB) | 4th draft |
| 0.5 | 24/09/2019 | Draft | Sara Roda, Ioulia Konstantinou, István Böröcz, Paul de Hert (VUB) | 5th draft |
| 0.6 | 27/09/2019 | Draft | Sara Roda (VUB), Vicky Vouloutsi (IBEC) | Introducing certain corrections; IBEC's contribution. |
| 0.7 | 30/09/2019 | Final | Apostolos Axenopoulos (CERTH) | Reviewers |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Definitions, Acronyms and Abbreviations

| ACRONYMS / ABBREVIATIONS | DESCRIPTION |
|---|---|
| DPA | Data Protection Authority |
| DPIA | Data protection impact assessment |
| EDPB | European Data Protection Board |
| EDPS | European Data Protection Supervisor |
| GDPR | General Data Protection Regulation |
| WP29 | Article 29 Data Protection Working Party |
| | |
| | |
| | |

# Table of Contents

# List of Tables

# Executive Summary

The present deliverable outlines the TARES Impact Assessment method that the project intends to follow to conduct. This assessment is broader than just a data protection impact assessment (DPIA) pursuant to Article 35 of the General Data Protection Regulation (GDPR).[1] It will not only include the objectives of the latter, but also refer to the ethical and societal concerns of the project (ethical impact assessment - 'EIA') and privacy aspects not falling under the data protection impact assessment (privacy impact assessment – 'PIA').

Nonetheless, greater focus will be given to the DPIA as it is a legal requirement. A DPIA is required where a type of processing, in particular using new technologies, is *"likely to result in a high risk to the rights and freedoms of natural persons"* (Recital 89 and Article 35(1) of the GDPR). The HR-Recycler project needs to conduct a DPIA due to the introduction of a new technology in the workplace – a collaborative human-robot in the industrial recycling of Waste Electrical and Electronic Equipment (WEEE) – combined with the possibility of this technology, directly or indirectly:

i) collect special categories of personal, and,
ii) collect personal data referring to vulnerable subjects (workers).

At this early stage of the project, considering the information exchanged so far, we also foresee two other hypothetical situations for which a DPIA would be required. The processing operations:

iii) may result in an evaluation of aspects concerning the data subject's performance at work, and,
iv) may lead to the possibility of observing, monitoring or controlling (workers).

The TARES impact assessment implies a proactive approach contributing to informed decision-making by considering potential consequences of the project, direct and indirect, to the rights and freedoms of natural persons, before its occurrence. An impact assessment evaluates the origin, nature and severity of impacts that the processing operations, real or hypothetical, of a specific project entail.

The present impact assessment method intends to describe the steps to take in order to generate useful information to consortium partners and assist them in taking informed decisions about the development and deployment of the HR-Recycler technology. There is no one-size-fits all model for conducting impact assessments.

The present impact assessment method is based on the following main parameters:

i) compliance with the legal requirements of the GDPR;
ii) ensure that the *exercise* of workers' data protection and privacy rights is effective;
iii) reduce societal concerns in relation to the use of robots in the recycling sector;
iv) not to create unnecessary barriers or red tape for innovation processes; and,

[1] 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.

v) promote the progress of HR-Recycler technology in line with the principle of innovation[2] and the overall general vision of 'permissionless innovation'.[3]

**The impact assessment milestones overview:**

Phase I – Preparation of the assessment process

- The **first step of the DPIA** consisted of the screening exercised for a DPIA, an EIA and a PIA which occurred before the project started and during M1 of the project.

- The **second step (scoping)** was translated into Deliverable D2.1 – Report on security, data protection, privacy, ethics and societal acceptance. Deliverable D2.1 mapped the fundamental rights likely to be affected during the HR-Recycler project, the relevant applicable legislation when processing personal data, including in the context of employment, safety rules and the ethical and societal concerns underpinning human-robot interaction (HRI). It occurred from M2-M10 of the project.

- The **third step** consists of the present Deliverable D2.2 – the HR-Recycler Impact Assessment Method. It occurred from M9-M10 of the project.

Phase II and III – Assessment and Recommendations

- The **fourth step** (description of the project and information flows), the **fifth step** (assessing the necessity and proportionality of the processing operations), the **sixth step** (identification, analysis and assessment of relevant risks for the rights and freedoms to data subjects) and the **seventh step** (recommendations) will be taken together with Deliverable D2.3 – the TARES impact Assessment. It is estimated between M10-M12 of the project.

Phase IV – On-going steps

- The **on-going eighth step** (stakeholder consultation/ involvement) is carried out at different stages of the project. For example, Work Package 1, with the letter to the works committees and/or workers' participants in the pilots to inform them about the project,[4] and the setup of the Legal and Ethics HR-Recycler sub-committee; Work Package 2, with the development of the principles or moral actions and ethics and the setting up of an External Advisory Board; Work Package 3, with the organisation of workshops by end users with certain workers to identify potential end user needs that can be covered by the technical tasks; Work Package 7, with the human-robot collaboration schemes; and Work Package 10, with pilots studies' demonstration and evaluation. It is expected to be carried out between M9 until M42 of the project.

[2] https://ec.europa.eu/info/research-and-innovation/law-and-regulations/innovation-friendly-legislation_en

[3] The concept of 'permissionless innovation' is developed by Thierer, Adam, *"Permissionless innovation: The continuing case for comprehensive technological freedom"*, Mercatus Center at George Mason University, 2016. The HR-Recycler project sympathises with the overall general vision of positive disposition towards technological change and freedom to experiment in a fairly controlled environment ('regulatory sandbox' concept).

[4] According with the information provided by the end users, the workers operating at the factory floors were not associated with any specific trade union. For this reason, the informational letters were addressed to the works committee for IND, sent directly to participating workers at BNTT, and taken the form of a circular at INT.

- The **on-going ninth step** (documentation and drafting the TARES impact assessment report) concerns all documents and reports which are generated to develop the impact assessment. These are expected in M1, M6, M9, M12, M24, M30, M36 and M42.

- The **on-going tenth step** (quality control), is conducted by the project oversight bodies and the assigned reviewers for each deliverable.

Phase V – Maintenance

- The **eleventh step** will be translated by Deliverables D2.5, D2.6 and D2.7 – monitoring and observance reports on TARES requirements, versions 1, 2 and 3, respectively. It is expected to be conducted in M30, M36 and M42.

A checklist with a number of questions relating to the assessment phase will be sent to partners in M11 to help the assessor in its appraisal process.

# 1 Introduction

## 1.1 Overview

The report summarises the method adopted to conduct a data protection impact assessment pursuant to the General Data Protection Regulation (GDPR) and taking into account the specificities of the HR-Recycler project.

## 1.2 Structure of the deliverable

The deliverable is built on the experience of data protection impact assessment gained through VUB's involvement in two EU funded projects – MaTHISIS[5], FORENSOR[6] and PERSONA.[7]

Is structured as reported below:

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

**Chapter 2 – Preliminary Information** – Provides information about the impact assessment architecture, the main definitions and shedding a light on the specificities of the HR-Recycler project. It also provides additional information relevant to the HR-Recycler TARES Framework (Deliverable D2.1).

**Chapter 3 – DPIA legal requirements** – Explains the legal requirements pursuant to the General Data Protection Regulation to conduct a data protection impact assessment and a justification why a data protection impact assessment is required in HR-Recycler. Explains the reasons to integrate ethical and impact privacy assessments within the HR-Recycler project. The combination of these three assessments result in the TARES impact assessment.

**Chapter 4 – Impact Assessment Method for HR-Recycler** – Explains the TARES impact assessment method adopted for HR-Recycler.

**Chapter 5 – Bibliography**

[5] http://mathisis-project.eu, accessed 20 May 2019.
[6] http://forensor-project.eu, accessed 20 May 2019.
[7] http://persona-project.eu, accessed 22 September 2019.

# 2 Preliminary Information

## 2.1 Impact Assessment architecture

An impact assessment typically consists of two main elements: a 'framework' and 'method'. A framework constitutes an *"essential supporting structure"*,[8] which in our context concerns the definition and description of the structure, principles and rules – also known as 'pillars' – against which the impact assessment will be made. In turn, a method constitutes a *"particular procedure for accomplishing or approaching something"*,[9] defining the consecutive and/or iterative steps to be undertaken, in accordance with the framework, to perform the data protection impact assessment.

There are multiple frameworks and methods for impact assessment in many domains of practice of different applicability and quality. There is a constant need to revise and update previous impact assessments, using past experience or other evaluation techniques, to better serve its goals; to better respond to societal change or societal concern(s) or to give effect to new types or domains of impact assessment (e.g. 'algorithmic impact assessment').[10] Each new and revised framework and method is meant to contribute towards the efficiency (i.e. effectiveness with the least waste of resources), integrity (completeness) and fairness (legitimacy, impartiality and balance) of the assessment process.[11]

The framework consisted of Deliverable 2.1 – Report on security, data protection, privacy, ethics and societal acceptance. This deliverable translated the VUBTARES framework, mapping the fundamental rights likely to be affected during the HR-Recycler project, exploring the ethical and societal concerns underpinning human-robot interaction and identifying certain regulatory frameworks relevant to HR-Recycler that should guide the action of partners. Section 2.3.2 below brings additional elements to that framework.

The method consists of the present deliverable D2.2 – the HR-Recycler impact assessment method.

## 2.2 Impact Assessment meaning

The TARES Impact Assessment proposed by the VUB on this project will address the relevant societal concerns (i.e. security, right to the protection of personal data, right to privacy, ethics and societal acceptance) affected by HR-Recycler by identifying and assessing the impacts and risks on the TARES requirements.

The HR-Recycler impact assessment has a broader understanding as it combines several types of assessments and appraisal techniques. It will reunite a data protection impact assessment (a legal requirement from the

---

[8] Kloza, Dariusz, van Dijk, Niels, Casiraghi, Simone, Vazquez Maymir, Sergi, Roda, Sara, Alessia, Tanas & Konstantinou, Ioulia. "Constructing appraisal methods for (data protection) impact assessment for the European Union and beyond", *d.pia.lab Policy Brief* No. 1/2019, VUB: Brussels, p 2 (forthcoming).

[9] Ibid, p 2.

[10] Kloza, Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," *d.pia.lab Policy Brief* 1/2017, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf, accessed 10 August 2019.

[11] Kloza et al. (2017).

GDPR), a privacy impact assessment (translating the importance of this fundamental right to the project) and an ethical impact assessment (including societal acceptance).

A data protection impact assessment (DPIA) is different from a privacy impact assessment (PIA), although at certain instances the term PIA is sometimes used to refer to the same concept. For this project, nonetheless, we take the understanding that these two notions – DPIA and PIA – are different, and we refer to Deliverable D2.1 for the distinction between right to privacy and right to protection of personal data.

A DPIA is a tool designed to describe the processing of personal data, assess its necessity and proportionality in relation to the purposes it pursues and helps manage the risks to the rights and freedoms of natural persons resulting from such processing.[12] Hence, a DPIA helps the data controller to identify in a structured way:

a) The personal data that is being collected and processed;
b) The reasons and legal basis for collecting and processing the personal data;
c) The risks associated with the collection and processing; and,
d) Appropriate measures to mitigate the identified risks.

A DPIA is also a mechanism to ensure the protection of personal data, helping the data controller to demonstrate compliance with the law and accountability towards data protection authorities (Articles 5(2) and 24(1) GDPR). It constitutes evidence of due diligence, which can potentially limit or even exclude legal liability.[13] If conducted in a transparent manner and made publicly available, a DPIA enhances public confidence as it shows that an organisation takes personal data protection and societal concerns seriously.[14]

The DPIA should be carried out at the early stage of the project to allow the implementation of data protection principles, the adoption of safeguards and security measures in proportion to the risks identified, and hence adapt the project in conformity. The DPIA also helps decision-making by considering the potential consequences of the envisaged operation before its occurrence.

The benefits of conducting an impact assessment are numerous:[15]

- Preventing costly adjustments in processes by mitigating privacy and data protection risks.
- Preventing discontinuation of a project by early understanding of major risks.
- Reducing the impact of oversight involvement.
- Improving the quality of personal data (data minimisation and accuracy).
- Improving service and operation processes.
- Improving decision-making concerning data protection.

[12] Article 29 Data Protection Working Party (WP29), "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", WP 248 rev.01, as last revised and adopted on 4 October 2017, p 4. WP29 has been succeeded by the European Data Protection Board (EDPB) (Articles 68 and onwards of the GDPR), who has endorsed the said Guidelines - EDPB, Endorsement 1/2018. The EDPB is an independent European body with legal personality responsible for ensuring the consistent application of data protection rules throughout the European Union and promoting cooperation between the EU's data protection authorities. It is composed of representatives of national data protection authorities and the EDPS.

[13] Kloza et al. (2017), , p 1.

[14] Ibid, p 2.

[15] List identified in Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems", 18 March 2014, https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf, accessed 28 August 2019, p 12.

- Raising privacy awareness within an organisation.
- Improving the feasibility of a project.
- Strengthening confidence of employees or citizens in the way which personal data are processed and privacy is respected.
- Improving communication about privacy and the protection of personal data.

The PIA and the Ethical Impact Assessment (EIA) are not legally binding and it will be narrowed down to the ethical and privacy principles outlined in the TARES Framework – D2.1.

## 2.3 HR-Recycler specificities

The present report is being drafted at an early stage of the project, during month 9. The data sets that are planning to be collected are identified in Deliverable D12.2 – Data and knowledge management plan, and IPR protection strategy, more precisely in the Data Management Plan (DMP) section of the said deliverable. Those data sets can be subsumed into two main categories:

I. technical data, and
II. data which may involve the collection of personal information.

The first version of the DMP (deliverable D12.2) has been drafted during month 6 of the project and therefore only reflects the intentions of the Consortium Partners towards developing the overall project datasets. An updated version of the DMP is planned for month 42 of the project. The DMP aims to describe the data management life cycle for the data to be collected, processed and generated by the project, and for this reason, it will serve as the main base to identify the personal data that will be collected.

The team performing the DPIA also intends to send questionnaires, hold face-to-face meetings with technological and end-users partners to further understand the data flow and carry out desk research i) on other similar DPIAs (which occurred after the entry int force of the GDPR), ii) on data protection authorities guidance, and iii) on relevant doctrine concerning the assessment criteria of "*necessity and proportionality of the processing operations in relation to the purposes"* and of *"the risks to the rights and freedoms of the data subjects"*.

### 2.3.1 Main parameters guiding the HR-Recycler TARES Impact Assessment

The TARES Impact Assessment is intended to implement the general risk assessment logic into the project. With a risk assessment, the decision-maker (data controller) is capable to decide whether the risk (the processing of personal data and the project overall) has negative consequences to a data subject and the society at large, and if so, how to better mitigate them.

The main parameters which will guide the HR-Recycler TARES impact assessment are the following:

vi) compliance with the legal requirements of the GDPR;
vii) ensure that the *exercise* of workers' data protection and privacy rights is effective;
viii) reduce societal concerns in relation to the use of robots in the recycling sector;
ix) not to create unnecessary barriers or red tape for innovation processes; and,

x) promote the progress of HR-Recycler technology in line with the principle of innovation[16] and the overall general vision of 'permissionless innovation'.[17]

### 2.3.2 Additional input for TARES Framework (Deliverable D2.1)

After Deliverable 2.1 – Report on security, data protection, privacy, ethics and societal acceptance has been submitted, the consortium partners met in plenary on 3-4 July 2019 in Barcelona to discuss their work progress and research, and to take the necessary decisions in order to meet the project goals and objectives.

VUB presented additional information on relevant legislation and ethical guidelines for partners awareness during its presentation of Work Package 2 (WP2) progress work. The additional elements mentioned, which should also be taken into consideration in the TARES framework are the following:

**I) Legislative nature:**

- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. This Regulation aims at ensuring that electronic data, apart from personal data, can be processed freely throughout the EU, banning restrictions on where the data can be stored or processed, the so-called 'localisation requirements'. Exceptions on public security grounds are foreseen. These rules are designed to make it easier to do business in the EU and to create a single market for data storage and processing services, such as cloud computing.[18] **The relevance of this Regulation to the HR-Recycler project concerns with the possible use of cloud computing by partners and the free movement of technical data within the EU.**

- 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 sector (Directive on privacy and electronic communications), soon to be the E-Privacy Regulation. Among other aspects, the Directive bans unsolicited communications where the user has not given his/her consent. User consent is also required i) to send short message services (SMSs) and other electronic messaging systems; ii) before information (cookies) is stored on users' computers or devices or before access to that information is obtained (the user must be given clear and full information on the purpose of the storage or access, as well as the right of refusal); iii) before telephone numbers, e-mail addresses or postal addresses can appear in public directories. When traffic data are no

[16] https://ec.europa.eu/info/research-and-innovation/law-and-regulations/innovation-friendly-legislation_en

[17] See footnote 3 above. Thierer, Adam, *"Permissionless innovation: The continuing case for comprehensive technological freedom"*, 2016. This author is a feverous defender of implementing a growth-oriented innovation policy which starts with a positive disposition towards technological change, highlighting how regulatory permission (and the precautionary principle thinking) can harm innovation. According with the author, 'permissionless innovation' refers to the general freedom to experiment and learn through ongoing trial-and-error experimentation, while at the same time due (but extremely limited) account is given to the complex challenges of safety, security, privacy and economic disruption.
The HR-Recycler project sympathises with the overall general vision of positive disposition towards technological change and freedom to experiment in a fairly controlled environment ('regulatory sandbox' concept).

[18] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68. Summary text information available at https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32018R1807, accessed 10 September 2019.

longer required for communication, they must be erased or made anonymous. However, these data may still be processed for marketing purposes for as long as the users concerned give their consent. This consent may be withdrawn at any time.[19] **The relevance of this Directive for HR-Recycler is limited to its website development (cookie policy/rules) and newsletter dissemination in Work Package 11 – dissemination and exploitation.**

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). The Directive proposes a set of measures to boost the level of security of network and information systems (NIS) to secure services vital to the EU economy and society. It aims to ensure, among other points, that EU countries are ready to respond to cyberattacks and it introduces the obligation on essential-services providers and digital service providers to take appropriate security measures and to notify relevant national authorities about serious incidents. A NIS is defined as an electronic communications network, or any device or group of interconnected devices which process digital data, as well as the digital data stored, processed, retrieved or transmitted.[20] Although this Directive is aimed at entities that are considered to provide essential services (that is, private businesses or public entities classified as providing a service that has an important role for the society and economy, and where an incident would have significant disruptive effects on the provision of that service, for example water supply, electricity services, etc.), **the HR-Recycler partners should take note of the Directive's relevance in the discussions of robotic security, especially if connected to the internet.**

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union. The certification attests that the ICT products, services and processes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle (Article 46 and onwards of the Cybersecurity Act). The assurance level of European cybersecurity certification schemes (classified as basic', 'substantial' or 'high') shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident (Article 52 of the

[19] 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 sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47. Summary text information available at https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:32002L0058, accessed 10 September 2019.

[20] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30. Summary text information available at https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32016L1148, accessed 10 September 2019.

Cybersecurity Act).[21] **The relevance of this Regulation is to raise awareness among HR-Recycler partners working within the robotic industry.**

- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. This Directive establishes the principle of liability without fault applicable to European producers. Where a defective product causes damage to a consumer (e.g., death, personal injuries, damage to private property), the producer may be liable even without negligence or fault on their part. EU countries may set a limit for the total liability of a producer, in the case of death or personal injury. A defective products means a product that does not provide the safety which a person is entitled to expect, taking into account i) the presentation of the product, ii) the use to which the product could reasonably be expected to be put under; and iii) the time when the product was placed into circulation.[22] **This Directive is relevant to HR-Recycler project in what concerns the movable technology (the product) that is being developed by the technical partners.**

- Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, also known as the General Product Safety Directive (GPSD). The Directive requires firms to ensure that items on sale are safe and to take corrective action when that is found not to be the case. In order for a product to be considered safe it must meet national requirements or EU standards, and it must bear information enabling such product to be traced, for example by providing the manufacturer's identity and a product reference. If necessary, for safe use, products must be accompanied by warnings and information about any inherent risks. In case no such requirements or standards exist, a safety assessment must be based on i) Commission guidelines, ii) best practice in the sector concerned, iii) state of the art and technology, and iv) reasonable consumer safety expectations. National enforcement authorities have powers to monitor product safety and take appropriate action against unsafe items.[23] **This Directive is relevant for HR-Recycler technical partners developing the movable technology (the product).**

**II) Ethical nature:**

The non-exhaustive list below is representative of the developments and technical progress made in the digital area which could be relevant for HR-Recycler partners dealing with IT.

- Standards on interoperability for artificial intelligence in manufacturing. Further information at https://www.cencenelec.eu/News/Brief_News/Pages/TN-2018-016.aspx.
- ENISA guidelines:
  - Guidance and gaps analysis for European standardisation. This study aims to explore how the standards-developing world is responding to the fast-changing and demanding realm of privacy, by mapping existing available standards and initiatives in the area, and to provide insights on the "state-of-the-art" of privacy standards in the information security

[21] Further information at https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity. See also https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.
[22] Further information at https://osha.europa.eu/en/legislation/directives/council-directive-85-374-eec.
[23] Further information at https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32001L0095.

context through a relevant gap analysis. The study is available at https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation;

- Guidelines on assessing DSP security and OES compliance with the NISD security requirements. This report presents the steps of an information security audit process for the OES compliance, as well as of a self-assessment/ management framework for the DSP security against the security requirements set by the NIS Directive. In addition, it provides an analysis of the most relevant information security standards and frameworks to support OES and DSP in practicing the above exercises in the most tailored and efficient manner. The report is available at https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements;
- Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation. The scope of this report is to explore the concept of pseudonymisation alongside different pseusonymisation techniques and their possible implementation. The report is part of ENISA's work in the area of privacy and data protection, which focuses on analysing technical solutions for the implementation of GDPR, privacy by design and security of personal data processing. The report is available at https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions;
- Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default. This report aims to shed some light on what the data-protection-by-default principle means in information technology design, what is the situation today, as well as how the new GDPR obligation could support controllers in selecting data-protection-friendly defaults. The report is available at https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2;
- Reinforcing trust and security in the area of electronic communications and online services. This study provides an overview of well-established security practices, for the purpose of sketching the notion of “state-of-the-art” in a number of categories of measures, as they are listed in ENISA’s guidelines for SMEs on the security of personal data processing. The study is available at https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services.

- IPEN - Internet Privacy Engineering Network which supports engineers working on (re-)usable building blocks, design patterns and other tools for selected internet use cases where privacy is at stake. Further information at https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards.

Moreover, IBEC proposed and explained the need to differentiate between Human-Robot-Interaction (HRI) and Human-Robot Collaboration (HRC). This difference will be considered onwards. More specifically, HRI is the study of "humans, robots, and the ways they influence each other".[24] Typically, HRI involves a variety of actors (mainly comprising of humans and robots) and interactions may occur in all directions (between humans, robots, and the environment). The robot's autonomy may vary from manual to fully autonomous and the interaction (by definition) implies communication between the actors. The communication between the actors may include a variety of communication channels that include speech, natural language, gaze, facial expressions, prosody, gestures and others. Interactions can be either remote, where the actors are not spatially co-located and, in several cases, this interaction is referred to as *teleoperation* or proximal, where the actors share the same physical space. In the latter, if there is physical contact between the actors, it is called physical Human-Robot Interaction (pHRI). For Goodrich,[25] interaction is the process of *working together to accomplish a goal*. As one of the actors in HRI is a human, the interaction can be considered social, which includes not only social but also emotive and cognitive aspects and are often described in terms of goals, intentions, actions, perception and evaluation.[26] It is worth noting that social interactions are inherently dynamic. The main goal of HRI is not the effective collaboration with humans, but rather, the appropriate design of interaction modalities that support any task that requires interactions with robots: the design of a *"mutually shared interactive space"* that humans will want to use to achieve or support their goals.

HRC differs from HRI, as HRI may include collaboration. Usually, interaction involves action on someone else (or the environment) without necessarily profiting from it and it may not always have a clear task or goal. In contrast, collaboration is the process in which two or more parties work together to achieve shared goals. More specifically, collaboration is *"the mutually beneficial and well-defined relationship of two or more entities to achieve a common goal"*[27] and this may be one of the key differences between HRI and HRC: benefiting from the interaction and achieving a common goal. Indeed, HRC in work settings can be beneficial, as robots can improve safety, productivity, the quality of the outcome as well as alleviate the physical and cognitive load of the human co-worker. A team is formed when two or more entities, or agents, that have complementary skills perform common tasks and share common goals. In HRC settings, the team is mixed and typically comprises of humans and robots working together. For collaboration to be efficient, the robot is required to robustly perform a given task, be trustworthy and effectively communicate with the human co-worker. Additionally, we highlight the importance of safe operation, as the robot will be required to function in close proximity to humans. For efficient collaboration, a common plan for all team members is essential and that includes joint attention, intention and action planning, which may not be commonly used in most HRI scenarios. Nonetheless, HRI and HCI both share common challenges, as for robots to be accepted as co-workers or communication partners, they need to exhibit autonomous and transparent behaviors that are easily understood and explained,[28] as humans tend to intuitively apply the same social rules when they interact with machines or robots as when they interact with other humans.

[24] Fong, T., C. Thorpe, and C. Baur. "Collaboration, dialogue and human-robot interaction, 10th international sumposium of robotics research (lorne, victoria, australia)." Proceedings of the 10th International Symposium of Robotics Research. 2001.

[25] Goodrich, Michael A., and Alan C. Schultz. "Human–robot interaction: a survey." Foundations and Trends® in Human–Computer Interaction 1.3 (2008): 203-275.

[26] Bensch, Suna, Aleksandar Jevtic, and Thomas Hellström. "On interaction quality in human-robot interaction." ICAART 2017 Proceedings of the 9th International Conference on Agents and Artificial Intelligence, vol. 1. SciTePress, 2017.

[27] Mattessich, Paul W., and Barbara R. Monsey. Collaboration: what makes it work. A review of research literature on factors influencing successful collaboration. Amherst H. Wilder Foundation, 919 Lafond, St. Paul, MN 55104., 1992.

[28] Duffy, Brian R. "Anthropomorphism and the social robot." Robotics and autonomous systems 42.3-4 (2003): 177-190.

# 3 DPIA Legal Requirements

The General Data Protection Regulation (GDPR)[29] introduced a new obligation for the data controller to conduct a DPIA prior to certain processing operations of personal data take place. In particular, a DPIA is required when data processing operations are *"likely to result in a high risk to the rights and freedoms of natural persons"*.

**This might occur by virtue of their i) nature, ii) scope, iii) context and iv) purposes, but also when it involves v) using new technologies** where no data protection impact assessment has been made before by the controller. These criteria are not further defined, although they may include, concerning the 'nature' of processing operations – e.g., special categories of personal data or data relating to criminal convictions and offences, data related to security measures or biometric data; the 'scope' – e.g., the amount of data processed, the geographical reach and the number of people affected; the 'context' – e.g., in publicly accessible areas, working environment; the 'purpose' – e.g., data for profiling or automated decision-making (Recital 91 of the GDPR).[30] What qualifies as a 'new technology' can be difficult to define, as any innovation is always built on previous innovations. Subjectivity also lies within knowing for how long a technology should be considered 'new'.[31]

The approach of the GDPR is **risk-based** which means an identification, analysis and management of risks related to potential negative impacts on the data subjects. A 'risk' is a scenario describing an event and its consequences, estimated in terms of severity and likelihood.[32] For Gellert (2017), risk analysis has a two-fold dimension: risk assessment, which measures the level of risk in terms of likelihood and severity, and risk management, which is to decide whether or not to take the risk.[33] In practice, this means that controllers must continuously review and regularly (re)assess the risks created by their processing activities in order to identify when a type of processing is "*likely to result in a high risk to the rights and freedoms of natural persons"*.

The risks are mostly to data protection and privacy rights, but may also involve other fundamental rights, such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion, workers' rights to information and consultation within the company, fair working conditions and non-discrimination. The infringement could lead to physical, material and non-material damage (Recital 75 of the GDPR).

[29] 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.

[30] "Constructing appraisal methods for (data protection) impact assessment for the European Union and beyond", d.pia.lab Policy Brief No. 1/2019, VUB: Brussels, p 2. (forthcomming).

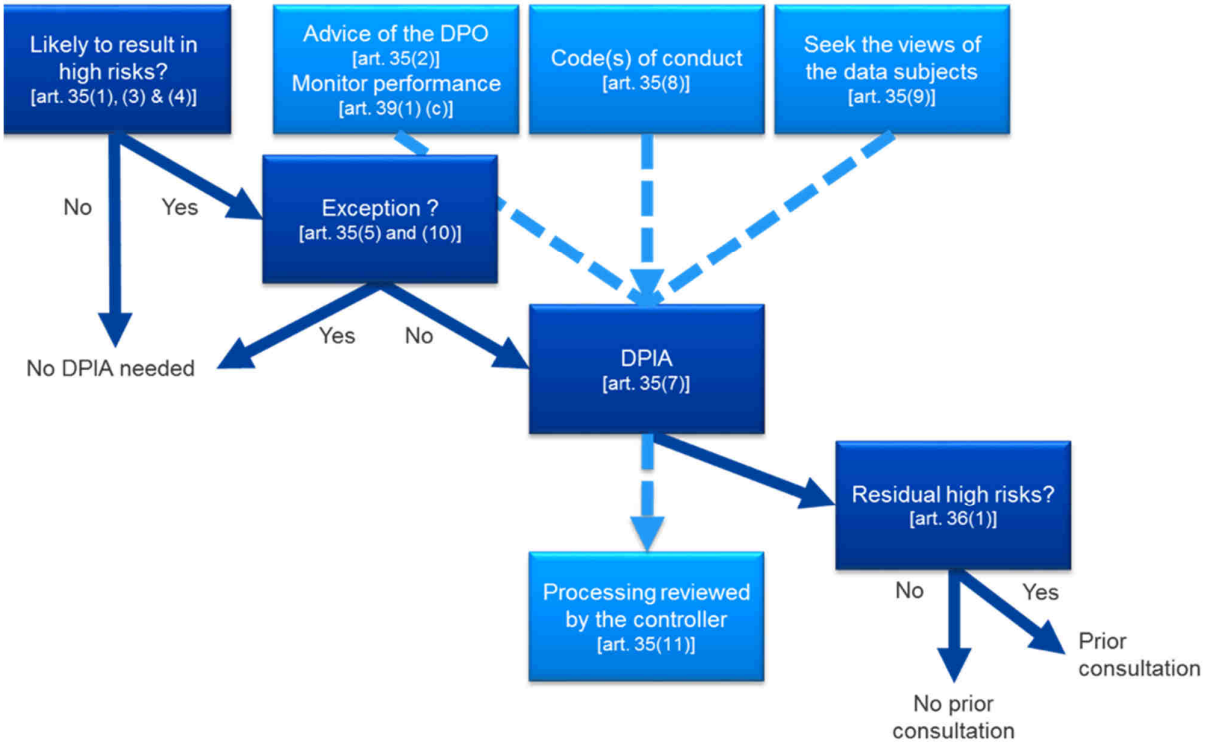
[31] European Parliamentary Research Service, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?", study written by Dr Michèle Finck at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, PE 634.445, July 2019, p 1-120, pp 87-88.

[32] WP29, Guidelines on Data Protection Impact Assessment (DPIA), as endorsed by the EDPB, p 6.

[33] Gellert, Raphaël, Understanding the notion of risk in the General Data Protection Regulation, Computer Law & Security Review 34, no. 2 (2018): 279-288, quoting Warner F., Introduction in the Royal Society, editor, Risk: analysis, perception and management – a report of a royal society group, London, The Royal Society, 1992, p 1-12.

In order to decide if a certain processing operation results in a 'high risk' to the rights and freedoms of data subjects, Article 29 Data Protection Working Party (WP29)[34] has developed, among others, guidelines to promote the development of a common list at European Union level for which a DPIA is considered to be mandatory, as well as a common EU list for which a DPIA is not necessary, and common criteria on the methodology for carrying out a DPIA (Article 35(5) of the GDPR).[35] In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless, as a DPIA is a useful tool to help controllers comply with data protection law.[36]

The table 1 below illustrates the basic reasoning to screen the need for a DPIA in the GDPR:




Source: WP29, Guidelines on Data Protection Impact Assessment (DPIA), WP 248 rev.01, p 7.

The criteria developed by WP29 to qualify certain processing operations as involving a 'high risk', and subsequently require a mandatory DPIA, which are (or may be) relevant for HR-Recycler are the following:

a. when the processing operations concern data from vulnerable data subjects, such as employees who are in an imbalanced position with respect to the controller (Recitals 84, 89 and Article 35 GDPR). The processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, being that

[34] Succeeded by the European Data Protection Board (EDPB).
[35] WP29, Guidelines on Data Protection Impact Assessment, as endorsed by the EDPB, p 4.
[36] Ibid, p 8.

individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights;

b. when the processing operations may lead to the possibility of observing, monitoring or controlling data subjects (workers) in a systematic way, including data collected through networks. The WP29 interprets 'systematic' as i) occurring according to a system, or ii) pre-arranged, organised or methodical, or iii) taking place as part of a general plan for data collection, or iv) carried out as part of a strategy.[37]

c. when the processing operations involve sensitive data or data of a highly personal nature, which includes special categories of personal data (e.g., data concerning health, biometric data, etc.) (Article 9 of the GDPR). These personal data are considered sensitive because they are linked to domestic and private activities, or the processing operation impacts the data subjects' daily life or his/her fundamental right/freedom.

d. when the processing operations involve novel forms of collection and usage by using new technological or organisational solutions, as they could have personal and social consequences which are unknown. This criterion obliges the data controller to reflect and is balanced against *"the achieved state of technological knowledge"* (Recital 91 of the GDPR).

e. when the processing operations may result in an evaluation or scoring of aspects concerning the data subject's performance at work (Recitals 71 and 91 of the GDPR).

f. when the processing operations match or combine datasets, for example, which come from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. This situation would also imply verifying the respect of the purpose limitation principle.

g. where personal data are processed for taking automatic decisions with legal or similar significant effects on data subjects, following a systematic and extensive evaluation of personal aspects relating to natural persons or following processing special categories of personal data, biometric data (Recitals 84, 91 and Article 35 of the GDPR).

*[Note: The project and the foreseen pilots do not foresee any systematic and extensive profiling of workers or any automatic decision with legal or similar effects on data subjects being taken against workers. This 'high risk' criterion is mentioned herein as a reminder hypothetical scenario and to question if this would be possible at the end of the project considering the technology being developed].*

For WP29 the more criteria met, the more likely it is to present a risk to the rights and freedoms of data subjects. If the processing operations meet at least two criteria, the data controller needs to carry out a DPIA. In case the DPIA is not carried out, the data controller needs to justify the reasons in a document and include the views of the data protection officer, when one has been designated.

[37] WP29, "Guidelines on Data Protection Officer", WP 243, adopted on 13 December 2016, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A, accessed 30 August 2019, p 8.

Determining whether a processing operation is considered to be 'high risk' or concluding that the residual risks are high enough to trigger the Data Protection Authority (DPA) consultation obligation (Article 36 of the GDPR) is a matter for the data controller, who enjoys a certain amount of discretion.[38] WP29 exemplifies that a residual risk persists when the data subject may encounter significant or even irreversible consequences, which he/she may not overcome (e.g., an illegitimate access to data leading to a life threat situation of the data subjects, a layoff, a financial jeopardy) and/or when it is obvious that the risk will occur (e.g., by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not fixed). [39]

Non-compliance with DPIA requirements can lead to fines imposed by national DPAs. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1), (3) and (4) of the GDPR), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9) of the GDPR), or failing to consult the DPA where required (Article 36(3)(e) of the GDPR), can result in an administrative fine of up to €10 million euros, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[40]

| **General Data Protection Regulation**<br>**Relevant Articles for a DPIA** | |
|---|---|
| ***Recital 75*** | *The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to* ***physical, material or non-material damage****, in particular: where the processing may give rise to* ***discrimination****, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or* ***prevented from exercising control over their personal data****; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular* ***analysing or predicting aspects concerning performance at work****, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where* ***personal data of vulnerable natural persons****, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.* |
| ***Recital 76*** | *The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.* |
| ***Recital 84*** | *In order to enhance compliance with this Regulation* ***where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin,*** |

[38] Kloza, Dariusz et al., d.pia.lab Policy Brief 1/2017, p 3.
[39] WP29, Guidelines on Data Protection Impact Assessment (DPIA), p 19.
[40] Ibid, p 4.

| | |
|---|---|
| | ***nature, particularity and severity of that risk. T****he outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.* |
| ***Recital 89*** | *Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which f****ocus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller,*** *or where they become necessary in the light of the time that has elapsed since the initial processing.* |
| ***Recital 90*** | *In such cases, a data protection impact assessment should be carried out by the controller* ***prior to the processing in order to assess the particular likelihood and severity of the high risk****, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.* |
| ***Recital 91*** | *This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights.* ***A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data,*** *or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.* |
| ***Article 35*** | *1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights* |

| | |
|---|---|
| | *and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*<br>*[…]*<br>*7. The assessment shall contain at least:*<br>*a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*<br>*b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*<br>*c) an assessment of the risks to the rights and freedoms of data subjects […]; and*<br>*d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. […]*<br>*Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.* |
| ***Article 36*** | *1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment […] indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.*<br>*2. Where the supervisory authority is of the opinion that the intended processing […] would infringe [the] Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall […] provide written advice to the controller and, where applicable to the processor, and may use any of its powers […].* |

## 3.1 Why a DPIA in HR-Recycler TARES Impact Assessment

The HR-Recycler project needs to conduct a DPIA due to the introduction of a new technology in the workplace – human-robot collaboration in the industrial recycling of Waste Electrical and Electronic Equipment (WEEE) – combined with the possibility of this technology directly or indirectly:

i) collect special categories of personal (i.e., data concerning health, meaning data related to the physical or mental health of a natural person which reveal information about his or her health status), and,

ii) collect personal data referring to vulnerable subjects (i.e., employees in the working environment).

At present, considering the information exchanged so far, we also foresee two other hypothetical situations for which a DPIA would be required. The processing operations:

iii) may result in an evaluation of aspects concerning the data subject's performance at work, and,

iv) may lead to the possibility of observing, monitoring or controlling data subjects (workers) in a systematic way.

These are all processing operations that have been considered by the WP29 as *"likely to result in a high risk"* pursuant to Article 35 of the GDPR.

The DPIA will provide clarity in terms of identifying and analysing:

a) the personal data that will be collected, recorded, stored, shared, consulted, used and erased;
b) the respective data flows;
c) the data controllers and processors of each data set;
d) the risks to personal data protection and other fundamental rights to the data subjects, such as privacy, human dignity, physical and mental integrity of the person, non-discrimination, self-determination and autonomy freedom of expression, workers' right to information and consultation within the undertaking, freedom of peaceful assembly and association, freedom of movement;
e) the measures (solutions and actions) envisaged to address those risks, including safeguards, security measures and mechanisms to ensure compliance with the GDPR. That is, to mitigate the risks to an acceptable level.

## 3.2 Why an Ethical and Privacy Impact Assessments in HR-Recycler TARES Impact Assessment

The Ethical Impact Assessment (EIA) and the Privacy Impact Assessment (PIA) are not required by law but desired as good practice.

The EIA is of particular importance considering that the present initiative is carried out in the employment context and consent is not considered to be freely given.[41] Moreover, the possible transformation that the HR-Recycler technology can bring in the recycler sector (although expected to be positive), pertaining to a human-robot environment, requires an impact analysis. There no explicit criteria provided by law; hence it is up to the assessor to determine whether the threshold to conduct an EIA is met. Several concerns about data protection and privacy might also be perceived as ethical matters. As a result, possible intersections and overlaps between those subjects can occur. The role of the independent External Advisory Board (EAB) and of the Legal and Ethics Sub-Committee of the HR-Recycler project will take particular attention to the ethical concerns identified and raised throughout the project.

The PIA in the present TARES Impact Assessment will focus on privacy aspects which are not covered by the DPIA. There may be situations where the privacy of workers is affected independently from personal data protection under the GDPR.

## 3.3 Conclusion

Due to the fact that a DPIA is a legal requirement, the HR-Recycler TARES Impact Assessment Method will follow the systematic and structured approach of the DPIA as established in the GDPR. Also, for this reason, the DPIA will be explained in more detail and in each step of the DPIA method, appropriate references will be made to the EIA and PIA. Security aspects are dealt within the DPIA pursuant to Article 32 of the GDPR.

[41] WP29, Guidelines on Consent under Regulation 2016/679, WP 259rev.01, as last revised and adopted on 10 April 2018., p 7; WP29, Opinion 2/2017 on data processing at work, WP 249, Brussels, 8 June 2017, paragraph 6.2.

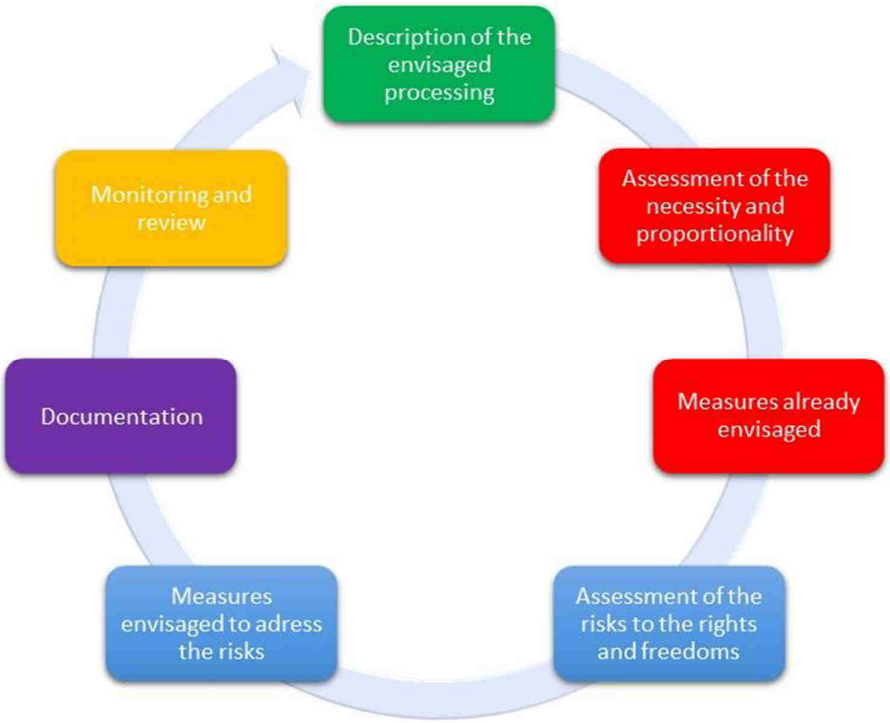
# 4 Impact Assessment Method for HR-Recycler

There are many different impact assessment (IA) methodologies and there is no 'one size fits all' solution.

An IA method should reflect the diversity of the industry and governance sectors, the specific risks attached to those sectors, as well as respect legal, cultural, social or ethical differences of multiple jurisdictions.[42] The appropriate method is the one that allows the data controller to best understand and treat the possible consequences of the initiative.[43]

The method should also allow the data controller to generate useful information for decision-making within the consortium and to assist partners in taking informed decisions regarding the development and deployment of the HR-Recycler technology.

The table 2 below illustrates a generic interactive process for carrying out a DPIA proposed by WP29. The latter takes the view that each stage can be revisited multiple times before the DPIA can be completed.




Source: WP29 Guidelines on Data Protection Impact Assessment (DPIA), WP 248 rev.01, 4 October 2017, p 16

[42] Ibid, p 4.
[43] Ibid, p 3.

## 4.1 TARES Impact Assessment Method[44]

Taking into account the specific parameters of the project, as well as its goals, objectives and timeline, the method adopted herein consists of eleven steps (seven consecutive steps, three executed throughout the entire process and one step to be revisited at M30, M36 and 42 of the project), grouped in five phases. Some of these steps follow a logical sequence, some other are a function of the principles embodied in the framework.

Phase I: Preparation of the assessment process

- Step 1: Screening
- Step 2: Scoping
- Step 3: Planning and preparation

Phase II: Assessment

- Step 4: Description of the project and information flows
- Step 5: Assessing the necessity and proportionality of the processing operations
- Step 6: Identification, analysis and assessment of relevant risks for the rights and freedoms to data subjects

Phase III: Recommendations

- Step 7: Recommendations.

Phase IV: On-going steps

- Step 8: Stakeholder consultation/ involvement
- Step 9: Documentation and drafting the TARES report
- Step 10: Quality control

Phase V: Maintenance

- Step 11: Monitoring and observance reports

## 4.2 Guidance for the execution of the TARES Impact Assessment

This section describes in more detail the steps to be taken when conducting the HR-Recycler TARES Impact Assessment (IA).

Phase I: Preparation of the assessment process

*Step 1: Screening*

The purpose of this step is to determine whether the impact assessment process is needed or desired. To help on this analysis and decision, the screening is conducted based on an initial description of the initiative. Effort needs to be made to gather as much information as possible, both contextual and technical from partners, prior to the start of the project.

[44] The guidance described herein is mostly based on the *d.pia.lab Policy Brief No. 1/2019* "Constructing appraisal methods for (data protection) impact assessment for the European Union and beyond", VUB: Brussels, p 2. (forthcomming).

Considering that the present TARES impact assessment combines a DPIA, a EIA and a PIA, the screening should involve these three assessments:

I - DPIA

The criterion for decision for a DPIA is taken from the General Data Protection Regulation (GDPR) and the WP29 Guidelines on Data Protection Impact Assessment, as endorsed by the European Data Protection Board (EDPB).

- *Criterion 1 – high risk*

At a most general level, the GDPR requires a DPIA for processing operations likely to present high risk to the rights and freedoms of data subjects, taking into account four qualitative criteria of personal data processing operations: i) nature, ii) scope, iii) context and iv) purposes, and one independent criteria of novel technologies.[45] It is for the data controller to determine whether a risk is 'high', for which determination the controller is held accountable.

- *Criterion 2 – enumeration*

The GDPR expressly foresees three types of data processing operations for which a DPIA is required (Article 35(3) GDPR). These are:

- *"systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person"*;
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or
- *"systematic monitoring of a publicly accessible area on a large scale"*.

- *Criterion 3 – positive enumeration by data protection authorities*

A national or regional DPA is entitled to determine for its own jurisdiction further types of data processing operations for which a process of DPIA is required (Article 35(4) GDPR). The list is communicated to the EDPB, for which the consistency mechanism applies, and an opinion of the EDPB issued, if such lists describe processing operations which can involve cross-border activities, namely offering of goods and services to data subjects or the monitoring of their behaviour in several Member States, and activities which may substantially affect the free movement of personal data within the European Union (Article 35(4)-(6) GDPR).

- *Criterion 4 – negative enumeration by DPAs*

A national or regional DPA may determine for its own jurisdiction other types of data processing operations for which a process of DPIA is *not* required (Article 35(5) GDPR). The list is also communicated to the EDPB, for which the consistency mechanism applies in the same manner as mentioned in the previous paragraph (Article 35(4)-(6) GDPR).

- *Criterion 5 – selected previous assessment processes*

Unless Member States decide otherwise, a DPIA is no longer required when two cases are of application – processing is necessary to comply with a legal obligation (Article 6(1)(c) GDPR) or processing is

[45] See explanation in Chapter 3 above.

necessary for the performance of a task carried out in a public interest or in the exercise of official authority vested in the data controller (Article 6(1)(e) GDPR) – which are imposed either by EU or national law, and those processing operations have already been assessed in the context of the adoption of that legal disposition provided that the later assessment essentially satisfies the conditions laid down in the GDPR (Article 35(10) GDPR).

- *Criterion 6 – exemptions for specific professions*

The GDPR foresees certain exemptions for processing operations which concern *"personal data from patients or clients by an individual physician, other health care professional or lawyer"*. The Regulation does not consider these operations to be on a large scale and hence the process of DPIA is not required (Recital 91 GDPR).

If any of the first three criteria are satisfied, a process of DPIA is mandatory. Conversely, if any of the three last criteria are satisfied, a data controller is exempted from carrying out the assessment process.

**The reason to perform a DPIA in HR-Recycler is explained in section 3.1 above.**

**The actions taken by VUB, which can be subsumed under this step, consisted of sending a preliminary questionnaire to partners in July 2018 to collect information about the pilots and the processing of personal data after the pilots. The responses to that questionnaire were also relevant to feed in step 2 and for future steps 4 to 8 of this DPIA.**

II – EIA

The threshold analysis to conduct an EIA relates to the ethical and societal concerns. A preliminary exercise has been carried out and identified in section 3 of Deliverable D2.1. The ethical assessment should not only focus on ensuring observance with the ethical principles of truthfulness, appropriateness, ethical handling of data relating to employees, stigmatisation and discrimination arising from the HR-Recycler practices, but also on the impacts to the workforce industry in the recycling sector, the overall human relations in the factory and the consequences for the human-robot interaction and human robot collaboration. The health and safety of workers should also be considered.

The ethics threshold analysis can be subsumed in answering the following questions:

- Does the HR-Recycler project result in the development and/or use of technology/procedures that:
  - Could require the informed consent of workers/research participants?
  - Could involve invasive techniques (e.g., physical interventions, invasive studies on the brain) on workers/research participants?
  - Could cause harm or endanger workers/research participants?
  - Could have a negative impact on worker's/research participant's identity?
  - Could be misused (e.g. unethical handling of data relating to workers)?
  - Could generate stigma and discrimination for workers/research participants?
  - Could generate inequalities for workers/research participants?
  - Could generate unfair and inappropriate data, capable of humiliating workers/research participants?
  - Could not be sufficiently transparent to workers/research participants?

- Could not have mechanisms for determining accountability (of designers, manufacturers, programmers, end users) in place?
- Could have a negative impact on the human relations in the plant?
- Could have a negative impact on the workforce industry?

III – PIA

The threshold analysis to conduct a PIA can be subsumed in answering to the following question:

- Would the HR-Recycler technology impact the workers' privacy in a severe way?

If yes, then a PIA should be warranted.

*Step 2: Scoping*

A step, based on the initial description, to identify:

a) the applicable fundamental rights framework, specifically the rights to privacy and protection of personal data, and inter alia in the Charter of Fundamental Rights of the European Union in the context of the tasks carried out within the HR-Recycler system.

b) the ethical and societal framework, specifically taking into account interactions between humans and robots, ethical handling of data relating to employees, stigmatization and discrimination arising from HR-Recycler practices, including the societal concern(s). This may also comprise exploratory information on stakeholders who might be affected, concerned or interested in the project or possess expert knowledge, as well as the level of their involvement.;

c) the relevant legal and other regulatory frameworks, including the EU data protection framework, the Council of Europe's Framework, certain national frameworks where the pilots will be deployed; and,

Not all of these elements might be identifiable at the beginning of the assessment process and hence their identification might need to be revised periodically. The involvement of external ethical experts, such as an external advisory board, might bring more richness to the scoping exercise. Other techniques to identify potential ethical issues can be used, for example, literature review, checklists approaches, foresight methods, stakeholders consultation/involvement.

In HR-Recycler, the **scoping exercise** started with research desk and internal discussion about the main legal premises, continued through the gathering of further information from partners via the teleconference held on 29 October 2018, the kick-off meeting on 18-19 December 2018, in Thessaloniki, Greece, as well as the teleconferences held, respectively, on 22 January, 1 February and 8 February of 2019.

A specific questionnaire was prepared for oral discussion at the second plenary meeting held on 13-14 March 2019, in Tondela, Portugal, and the first meeting of the HR-Recycler Legal and Ethics Sub-committee. The objective of this questionnaire was to identify direct and indirect groups that could be affected by the project (e.g., end users' workers, etc.) or contribute positively to it (e.g., data protection officers, legal or human resources departments from consortium partners, etc.); to understand compliance

to the project's ethical requirements (e.g., oversight bodies, consent forms and procedures, incidental findings policy and ethics decision-making engine); to explore possible effects that the use of robots could have on end users' workers, facilitating an oral report by the end users on the workers' view of the overall project (if sufficient progress had been made in that regard); to deepen the understanding of the kind of data that would be collected, at what stages and by/from whom (e.g., independent research participants, end users' workers, which partners, etc.); and to discuss possible applicable EU and national legal frameworks.

The meeting of the Legal and Ethics Sub-committee helped to follow-up and raise awareness to the ethical aspects of the project and to the protection of personal data, in particular to understand the necessity of including the collection of health data, namely Galvanic Skin Response (GSR), Electromyography (EMG), Electroencephalography (EGG) and Electrodermal activity (EDA), from the research participants. **A detailed justification concerning the collection of sensitive data was submitted in WP1, D1.2 – POPD Requirement No.2**. The meeting also allowed the exchange views on the involvement of workers, works' committees and trade unions (level and moment).

**These meetings contributed to the preparation of draft information sheets and consent forms for research participants to participate in the pilots and to process their personal data for research purposes, as well as to draft the information consent procedures – WP1, D1.1 – H – Requirements No. 1.**

**The scoping step was translated in Deliverable 2.1 – Report on security, data protection, privacy, ethics and societal acceptance.**

*Step 3: Planning and preparation.*

The overall purpose of this step is to define the terms of reference for conducting the assessment process. These may include, among others, the main objectives and specificities of the project, the resources to conduct the impact assessment (i.e. duration, allocated budget, team members availability and their level of expertise, etc.), the procedures and time-frames of the assessment process, the criteria adopted by the consortium on the acceptable risks (if already defined), etc.

The extent of the latter (small, medium or large) is greatly influenced by the internal procedures of an organisation, the complexity of the impact assessment, the impact that may raise to data subject and the available resources of the organisation.

**In HR-Recycler, the planning and preparation of the TARES impact assessment is translated in the present deliverable D2.2 – Impact Assessment Method.**

- **The TARES method for this project is being carried out by the VUB with direct contribution from IBEC.**

- **The knowledge and expertise are multidisciplinary as it combines partners with different expertise in the legal, technical (project and risk management, information security, IT architecture and system engineering) and ethical domains.**
- **The first TARES impact assessment report needs to be delivered by M12 of the project.**

Phase II: Assessment

*Step 4: Description of the project and information data flows*

The purpose of this step is to provide a detailed account of the planned project based on the initial description (step 1). The GDPR requires the assessment process to commence with a *"systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller"* (Article 35(7)(a) of the GDPR). Such a description implies knowing very well the life cycle and flows of the processing operations, as well as the actors and elements involved in the processing operations.

This necessarily includes:[46]

a) a contextual description of the project, in particular:
   i. the nature;
   ii. scope;
   iii. context of its deployment (including information on expected benefits and drawbacks);
   iv. purposes of processing operations; and,
   v. stakeholders involved (e.g., data subjects or their representatives, HR-Recycler External Advisory Board and partners, data protection officers, if designated, and public authorities);

b) a technical description, that is a description of the data life cycle and flows. The life cycle can be divided in the following main elements:[47]
   i. collection of data, which can be made via paper or web forms, interviews, video and audio recordings, sensors, etc.,
   ii. classification of data into categories and assign data for posterior archive. Due respect for Article 5 of the GDPR is required, implying an evaluation of the importance and need of the data for the purpose of the operation, which is linked with step 5,
   iii. data usage, that is identify any activity or operation involving the processing of personal data, and if it is done automatically or manually,

[46] WP29, Guidelines on Data Protection Impact Assessment (DPIA), Annex 2, p 22.

[47] Agencia Española de Protección de Datos, "Guía Prática para las Evaluaciónes de Impacto en la Protección de los Datos Sujetas al RGPD" ('Practical Guide for DPIAs', free translation), 2014, https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf , accessed 20 August 2019, p 13.

iv. transfer to a third party, that is identify such cases, and
v. destruction of the data, to ensure that it can no longer be recovered;

c) A description of the ethical and societal concerns as well as residual privacy aspects not covered under the personal data protection regime.

For each element there should be an indication of the following items: [48]

- processing operation(s) involved (Article 4 (2) of the GDPR),
- personal data involved,
- recipients, that is all natural and legal persons involved in the processing activities, identifying also their role and responsibilities (it can be at the level of a department when personnel rotativity is high within a company or when the company's digital structure is tailored as such – e.g., functional mailbox per department),
- period for which the personal data will be stored,
- technology used, that is identify relevant hardware (e.g., cloud systems, computers, USB drives, hard drives, remote terminal units, work stations, servers) software (e.g. operating systems, databases, business applications, messaging), networks (e.g. wireless, electricity and data cable, routing and switching devices, fibre optic), paper transmission channels (e.g. personalised web-portals), paper media (e.g., printing, photocopying), but without entering into a very technical description.

d) reference to approved codes of conduct for which partners adhere or comply to.

**Example table to describe the life cycle: [49]**

| | Life cycle | | | | | |
|---|---|---|---|---|---|---|
| Elements | | Way of collection | Classification into categories | Data usage | Transfer to third parties | Destruction |
| | Precise processing operation | | | | | |
| | Personal data | | | | | |
| | Recipients | | | | | |
| | Period of storage | | | | | |
| | Technology used | | | | | |

[48] Ibid, p 13-19.
[49] Based on Annex I of the Spanish Data Protection Authority 'Practical Guide for DPIAs', ibid, p 39.

*Step 5: Assessing the necessity and proportionality of the processing operations*

Once a clear picture is made about the personal data that is going to be processed, how it is going to be carried out (including its origin) and for what purpose, is it important to understand the legal basis for the processing operations, as well as the **necessity and proportionality of the processing operations in relation to their purposes** (Article 35(7)(b) of the GDPR).

Recital 39 of the GDPR sheds some light on **how to assess the necessity of processing operations**. It reflects the need to observe compliance with the personal data protection principles of Articles 5 and 6 of the GDPR.[50]

- *"Personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed*." This requirement relates to Article 5 (1) (c) GDPR) and the **principle of data minimisation**;
- "*The period for which the personal data are stored is limited to a strict minimum*." This requirement relates to Article 5 (1) (e) GDPR and the **principle of storage limitation**;
- *"Any processing of personal data should be lawful and fair*". This requirement relates to Article 6 of the GDPR and the **principle of lawfulness of processing** (legal basis). The same processing operation can be connected to different legal basis depending on their purpose/usage (for example, there can be the case where primary usage is consent and the secondary usage is legitimate interest). The use of consent as a legal basis requires the data controller to demonstrate that the data subjects' consent was free, specific, informed and unambiguous.[51] The use of 'legitimate interest' as a legal basis for processing requires specific justification and a balancing exercise by the data controller.[52]
- *"The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.*" This requirement relates to Article 5(1) (b) of the GDPR and the **purpose limitation principle**. The principle also postulates that personal data should not be further processed in an incompatible manner with the initial purpose.

**The proportionality requirement** is also explained in recital 39 of the GDPR when it is determined that: *"Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means".* This implies for example verifying if other data could be used instead or reducing the universe of concerned data subjects (quantitatively or qualitatively) or limiting the use of an intrusive technology. The proportionality principle is decomposed in three parts:

- **Adequacy/suitability** – analyse if the processing operation is able to attain the objective proposed (means used vis-à-vis objective);

[50] In this sense, see the Spanish Data Protection Authority 'Practical Guide for DPIAs', ibid, p 20-21; and Annex II of the WP29 Guidelines on Data Protection Impact Assessment, which explains that a DPIA to be sufficiently comprehensive to comply with the GDPR is dependent on the observance of the personal data protection principles under this assessment step.

[51] For a more detailed explanation about consent see WP29, Guidelines on Consent under Regulation 2016/679, WP 259rev.01, as last revised and adopted on 10 April 2018.

[52] WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, adopted on 9 April 2014, https://www.dataprotection.ro/servlet/ViewDocument?id=1086, accessed 10 September 2019. Although the notion refers to the previous Directive 95/46/EC, it is still contains useful and relevant examples to cary out the balancing exercise required under Article 6 (1) (f) GDPR).

- **Necessity** – analyse whether all proposed processing operations or all datasets are needed or whether could there be other less intrusive operations/datasets to the rights and freedoms of data subjects which would have the same effect and effectiveness. The objective would be to choose the less intrusive measure that accomplishes the purpose by comparing among the different 'adequate' measures;

- **Proportionality stricto sensu** / balance exercise – the benefits which result from the 'adequate and necessary' processing operations need to be higher than the impact that it will cause for the rights and freedoms of the data subjects. This last dimension offers some margin of appreciation, where the reasoning is to evaluate if the choice made (sacrificing the right and freedoms of the data subject against the processing operations) is valid in light of the nature, scope, context and purposes of the processing operations (objective parameters).

The UK ICO resumes the necessity and proportionality assessment into the following two questions:[53]
- Does the collection you foresee helps you to achieve your purpose?
- Is there any other reasonable way to achieve the same result?

*Step 6: Identification, analysis and assessment of relevant risks for the rights and freedoms to data subjects*

The purpose of this step is to identify, analyse and assess the severity and likelihood of risks in relation to the rights and freedoms of data subjects as a result of the processing of personal data from workers (Article 35 (7) (c) of the GDPR). Some risk analysis should also be made about the societal concern(s) and privacy residual aspects not covered under the data protection regime.

The Spanish Data Protection Authority, explains that it is necessary to **identify the origin of risks** (e.g. cloud systems can imply loss of confidentiality, availability and integrity), **analyse the situations that can bring risk** (e.g., in the cloud example, there is a risk of unauthorised access, loss of data or modification of data due to a cyberattack), **give a value to that risk in terms of likelihood and impact** (e.g., if no security measures are adopted the probability of the risk to materialise can be high as well as the impact), and **propose measures to treat those risks** in order to avoid potential harms to the data subjects.[54]

Recital 75 of the GDPR specifies that the **impacts or harms to individuals can be divided into three categories**: **physical damage** (actions that can lead or inflict harm to the data subject's physical integrity), **material damage** (actions that can lead to economic losses, property damages, job, etc) or **non-material damage** (actions that can lead or inflict mental or moral harm to the data subject's).

The UK Data Protection Commissioner (ICO) provides the following guidance: *"Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk".*[55]

---

[53] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/.

[54] Spanish Data Protection Authority 'Practical Guide for DPIAs', p 22-35.

[55] ICO, How do we do a DPIA?, URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/.

Recitals 75 and 76 provide further explanation on the type of damage that the processing operations of personal data can bring to data subjects and their rights.

**The HR-Recycler project will group the risks into the following categories:**

1. Inability to exercise rights (including but not limited to privacy rights);
2. Inability to access services or opportunities;
3. Loss of control over the use of personal data;
4. Discrimination;
5. Identity theft or fraud;
6. Financial loss;
7. Reputational damage;
8. Physical harm;
9. Loss of confidentiality;
10. Re-identification of pseudonymised data;
11. Any other significant economic or social disadvantage;
12. Denial of rights and freedoms;
13. Diffusion of *sensitive* data; or
14. Societal concerns.

**These risks have to be assessed against the likelihood of their occurrence and the severity of their impact. Quantitative and qualitative appraisal techniques are used.**

**The formula can be translated as follows:** [56]

**Risk = Likelihood X Impact**

In order to weigh the likelihood of the harm and the severity of the impact for these generic risks, the risk matrix below will be followed.[57] The risk analysis is made from the viewpoint of the data subject, and not from the entity (data controller) conducting the impact assessment.

| |
|---|
| Low risk – If the value is between 1 and 2; |
| Moderate – If the value is higher than 2 and lower than 5; |
| Medium – If the value is higher than 5 and lower than 9; |
| High – If the value is higher than 9 and lower that 12; |
| Very High – if the value is higher than 12. |

[56] Spanish Data Protection Authority 'Practical Guide for DPIAs', p 26.
[57] Inspired from the Spanish Data Protection Authority 'Practical Guide for DPIAs', p 23-33.

| Likelihood | | Impact | | | | |
|---|---|---|---|---|---|---|
| | | **Low (1)** Inconvenience /Being annoyed) | **Moderate (2)** Feeling loss of data control/minor material damages/ stress or no significant physical damages) | **Medium (3)** Financial disadvantage/ higher stress levels or physical damage/ rights and freedoms are restricted | **High (4)** (Being constraint/significant consequences that can be overcome with difficulty by data subjects) | **Very High (5)** Being in danger/significant or even irreversible damage to rights and freedoms of data subjects) |
| | **Remote (1)** | **1** | **2** | **3** | **4** | **5** |
| | **Rare, unlikely (2)** | **2** | **4** | **6** | **8** | **10** |
| | **Occasional, Reasonable possibility (3)** | **3** | **6** | **9** | **12** | **15** |
| | **Likely (4)** | **4** | **8** | **12** | **16** | **20** |
| | **Frequent, Almost certain (5)** | **5** | **10** | **15** | **20** | **25** |

Concerning ethics impact assessment, the suggested appraisal techniques can be the following:

- applied ethics,
- stakeholders' consultation,
- ethical checklist approaches,
- scenario-based approaches.

As regards privacy impact assessment, the appraisal techniques can include the above risk matrix, scenario planning and cost benefit analysis.

Phase III: Recommendations

*Step 7: Recommendations*

The purpose of this step is to propose concrete and detailed measures (controls, safeguards, security measures, organisational, technical, etc.) to partners, as well as possible timeframes to mitigate the risks associated with the project in relation to personal data, to minimise possible negative consequences to the rights and legitimate interests of the data subjects or other persons concerned and to maximise positive ones. The concepts of 'negative' and 'positive' are subjective. The recommendations also demonstrate compliance with the GDPR (Article 35 (7) (d) of the GDPR).

Taking into account the specific recommendations, the project coordinator and/or the involved partners in the respective dataset collection take a decision on which measures should be adopted, knowing that a processing activity might be cancelled altogether if the consequences would be unacceptable.

**Example table of generic protection measures (non-exhaustive):**[58]

| PROTECTION GOAL (security of processing) | COMPONENT (of what) | MEASURE |
|---|---|---|
| Ensuring availability (protection against disappearance of personal data, denial of service, loss of power, hardware loss) | Data, systems, processes | Preparation of backups, redundancy of hardware or software, implementation of repair strategies and alternative processes, rules of substitution for absent employees, documentation of data syntax |
| Ensuring integrity | Data | Comparing hash values |

[58] Based on the table made by Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A process for data protection impact assessment under the European General Data Protection Regulation" (2016) in *4th Annual Privacy Forum,* APF 2016, 7-8 September 2016 proceedings, Frankfurt/Main, Germany, Springer, pp. 21-37, p 33; and on section 7 of the Standard Data Protection Model, p 27-32.

| | | |
|---|---|---|
| (protection against unauthorised, unwanted modifications and deletions) | Systems | Restriction of writing and modification permissions, use of electronic seals and signatures in accordance with the cryptographic concept, regular integrity checks |
| | Processes | Specification of the nominal behaviour of workflow or processes and regular testing of the process, logging |
| Ensuring confidentiality results (protection against unauthorised access and illegal processing) | Data, systems | Encryption of stored or transferred data, specified environment (buildings, rooms), protection against external influences (espionage, hacking), limitation of authorised personal to those who are verifiably responsible, qualified, reliable (security clearance), formally approved and where no conflict of interest may arise in the exercise of their duties |
| | Processes | Definition of rights and roles concepts according to the principle of necessity (identity management by controller), specification of internal regulations and contractual obligations (obligation to secrecy, confidentiality agreements), specification and control of communication channels |
| Ensuring unlinkability through definitions of purposes (protection to process data only for the purposes for which it was collected) | Data | Anonymity, pseudonymity, attribute-based credentials |
| | Systems | Separation (isolation) of stored data |
| | Processes | Identity management, anonymity infrastructures, audits |
| Ensuring transparency | Data | Documentation, logging |
| | Systems | System documentation, logging of configuration changes |
| | Processes | Documentation of procedures, logging |
| Ensuring the exercise of data subject rights through anchor points (rectification, blocking, erasure, objection requests) | Data | Access of persons concerned to their data (information, rectification, blocking, deletion) |
| | Systems | Off-switch |
| | Processes | Helpdesk/single point of contact for modification/deletion, change management |

Phase IV: On-going steps

*Step 8: Stakeholder consultation/involvement*

The first step in stakeholder consultation/ involvement is their **identification**. A stakeholder is someone who holds an interest in something. In the context of an impact assessment, it is someone who is or might be affected by, concerned about or interested in a planned initiative, positively and/or negatively. At the same time, it can be someone who possesses specific knowledge and know-how about the initiative (an expert). The concept of stakeholder is open-ended, and a stakeholder might not even be aware of his/her quality. Stakeholders can be individuals or collective entities, irrespective of whether being formally recognised as such. Stakeholders can be grouped into internal (e.g. employees) and external ones (e.g. customers or non-governmental organisations); primary (i.e. those with a direct stake in the initiative, e.g. investors) and secondary (i.e. those with an indirect interest yet influential, e.g. the state); or they can be classified by their attributes: power, legitimacy and urgency.

The second step in stakeholder consultation/involvement is to **define their level of involvement**. It can range from: (a) merely being informed about a planned initiative (low level); to (b) dialogue and consultation, in which their views on the initiative are sought and taken into consideration (middle level); or even (c) to co-decision about the deployment of the initiative in question and, subsequently, partnership in its implementation (high level).

The third step is to **involve stakeholders in the assessment process** and there exists a plethora of techniques for doing so, ranging from i) information notices, to interviews, questionnaires and surveys (participants are asked specific questions in a pre-structure way. The responses gathered can help to identify concerns, solutions and gaps), to focus groups (small groups of people invited to discuss a theme and provide insights), roundtables (participants agree on a topic to discuss and are given equal opportunity to express their view), workshops (meeting with a small group of key stakeholders to discuss possible scenarios and different viewpoints) and citizens panels (citizens are requested to collaborate by developing scenarios and deliberate upon one to address the initiative), to specific techniques, such as 'world café' or Delphi (people with different background take part in a series of facilitated discussions, not necessarily face to face meetings; the responses are anonymous). The appropriate technique(s) is selected depending on the pursued level of stakeholder involvement, the planned initiative and context of its deployment, and the resources at the disposal of the sponsoring organisation.

Stakeholder consultation/involvement can provide several benefits to the assessment. For example, it can enhance its quality, credibility and legitimacy, and consequently its outcome. Nonetheless, it can also bring drawbacks, which can be connected to their representativeness (over or under representation), fairness (manipulation, astroturfing), resistance, communication barriers, clash between public and private interests or the resource-intensiveness of the entire stakeholder involvement process. In case stakeholder involvement is neither warranted nor necessary, such a choice is reasoned and documented.

**Pursuant to the GDPR, the purpose of this step is to foresee the involvement of data subjects and/or their representatives in the assessment process, without prejudice to the protection of commercial or public interests or the security of processing operation (Article 35(9) GDPR).**

**In the present deliverable, we will give a wide understanding to the notion of 'stakeholder consultation/involvement' in order to include external relevant third parties, such as the HR-Recycler**

**External Advisory Board, and to allow a certain level of flexibility to include different levels of participation, either formal or informal, and distinct modalities to collect their views.**

**The category of stakeholders that might affect or be affected by the project are:**

- **Employees and works committees**
- **Policy makers (including legislators and executive, EU bodies and agencies)**
- **NGOs defending industrial workers' rights**
- **Trade Unions related to the industrial workforce**
- **Experts, including academia**
- **Technology providers (e.g. AI solutions)**
- **DPOs**
- **Public opinion**

**The consultation of workers will be carried out at different stages of the project**. For example, in Work Package 1, with the letter to the works committees and/or workers' participants in the pilots to inform them about the project; in Work Package 2, with the development of the principles or moral actions and ethics; in Work Package 3, with the organisation of workshops (or focus groups) by end-users with certain workers to identify potential end-user needs that can be covered by the technical tasks; in Work Package 7, with the human-robot collaboration schemes; and in Work Package 10, with pilots studies' demonstration and evaluation.

*Step 9: Documentation and drafting the TARES impact assessment report*

The purpose of this step is to keep intelligible records, in writing or in other permanent form, about all activities undertaken during the assessment process. This step includes the preparation of a final report of the assessment process which presents the results of the TARES Impact Assessment. The TARES Impact Assessment can be structured according to the phases described in this document, presenting the results of each phase, annexing any relevant supporting document or material used in the assessment.[59]

The objective of the documentation is to facilitate the implementation of the process and to present to national Data Protection Authorities and/or the European Commission services upon request with due respect for legitimate confidentiality. The TARES Impact Assessment may handle classified information from partners related products and services, with special confidentiality requirements. As such, the analysis performed, and its documentation may need to be appropriately secured in accordance with partners' information classification scheme.[60]

*Step 10: Quality control*

[59] Smart Grid Task Force 2012-14, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems", 18 March 2014, p 35.

[60] Ibid.

The purpose of this step is to check the adherence to the adopted quality standard (e.g., rules and principles described in the framework), either internally (e.g. monitoring or a review within the organisation) or externally (e.g. by an independent authority, e.g. audit, advisory boards) or both. The quality control can occur equally during or after the assessment process, or both.

**In HR-Recycler the quality control is done by the project coordinator and by the oversight bodies, in particular, the Legal and Ethical Manager, the Legal and Ethics sub-committee and the External Advisory Board, as well as by the European Commission services during the reviews' meetings.**

Phase V: Maintenance

*Step 11: Monitoring and observance reports*

The purpose of this step is to ensure that the project is conducted and implemented according to the TARES Impact Assessment recommendations. This step ensures the continuity of the assessment process.

The following tasks are foreseen:

- Deliverable D2.5 – Monitoring and observance reports on TARES requirements (version 1), due in month 30;
- Deliverable D2.6 – Monitoring and observance reports on TARES requirements (version 2), due in month 36; and,
- Deliverable D2.7 – Monitoring and observance reports on TARES requirements (version 3), due in month 42.

***

# 5 Bibliography

**Primary Sources**

EU treaties and legislation


- 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.


**Secondary sources**

Books


- Thierer, Adam, "Permissionless innovation: The continuing case for comprehensive technological freedom", Mercatus Center at George Mason University, 2016.


Articles / Studies


- Bensch, Suna, Aleksandar Jevtic, and Thomas Hellström. "On interaction quality in human-robot interaction." ICAART 2017 Proceedings of the 9th International Conference on Agents and Artificial Intelligence, vol. 1. SciTePress, 2017.Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A process for data protection impact assessment under the European General Data Protection Regulation" (2016) in *4th Annual Privacy Forum,* APF 2016, 7-8 September 2016 proceedings, Frankfurt/Main, Germany, Springer, pp. 21-37.
- Duffy, Brian R. "Anthropomorphism and the social robot." Robotics and autonomous systems 42.3-4 (2003): 177-190.
- Fong, T., C. Thorpe, and C. Baur. "Collaboration, dialogue and human-robot interaction, 10th international symposium of robotics research (lorne, victoria, australia)." Proceedings of the 10th International Symposium of Robotics Research. 2001.
- Goodrich, Michael A., and Alan C. Schultz. "Human–robot interaction: a survey." Foundations and Trends® in Human–Computer Interaction 1.3 (2008): 203-275.
- Mattessich, Paul W., and Barbara R. Monsey. Collaboration: what makes it work. A review of research literature on factors influencing successful collaboration. Amherst H. Wilder Foundation, 919 Lafond, St. Paul, MN 55104., 1992.
- Nas, Sjoera and Roosendaal, Arnold, "DPIA Diagnotic Data in Microsoft Office Plus", 5 November 2018, Provacy Company, study commissioned by the Ministry of Justice and Security for the benefit of SLM Rijk (Styrategic Vendor Management Microsoft Dutch Government).
- van Dijk Niels, Raphaël Gellert and Kjetil Rommetveit, "A risk to a right? Beyond data protection risk assessments" (2016), *Computer Law & Security Review*, 32(2), pp. 286–306, doi: 10.1016/j.clsr.2015.12.017.
- Spiekermann-Hoff, Sarah and Oetzel, Marie Caroline, "A systematic methodology for privacy impact assessments: a design science approach" (2014) *European Journal of Information Systems (EJIS)*, Vol. 23, No. (2). pp. 128-150. ISSN 1476-9344 (original citation), http://epub.wu.ac.at/5495/1/EJIS_PIA_vs9_final_circ.pdf, accessed 2 July 2019.
- Wright David, De Hert Paul, "Introduction to Privacy Impact Assessment" (2012), in Wright D., De Hert P. (eds) Privacy Impact Assessment, Law, Governance and Technology Series, vol 6, Springer, Dordrecht.

Other secondary sources


- Agencia Española de Protección de Datos, "Guía Prática para las Evaluaciónes de Impacto en la Protección de los Datos Sujetas al RGPD", 2014, https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf , accessed 20 August 2019;

- Commission nationale de l'informatique et des libertés, "PIA Methodology", 2018, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-enmethodology.pdf, accessed 1 July 2019;

- d.pia.lab:
  - Kloza, Dariusz, van Dijk, Niels, Gellert, Raphaël, Böröcz, István, Tanas, Alessia, Mantovani, Eugenio and Quinn, Paul, "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," (2017) *d.pia.lab Policy Brief* 1/2017, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.
  - Kloza, Dariusz, van Dijk, Niels, Casiraghi, Simone, Vazquez Maymir, Sergi, Roda, Sara, Tanas, Alessia & Konstantinou, Ioulia. "Constructing appraisal methods for (data protection) impact assessment for the European Union and beyond", *d.pia.lab Policy Brief No. 1/2019*, VUB: Brussels (forthcoming).

- European Parliamentary Research Service (EPRS), "How the General Data Protection Regulation changes the rules for scientific research", study conducted by the Health Ethics and Policy Lab, ETH Zurich, at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit within the Directorate-general for Parliamentary Research Services (DG EPRS) of the European Parliament, PE 634.447, July 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634447, and respective Annex I, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447(ANN1)_EN.pdf, both accessed 29 August 2019.

- Article 29 Working Party (WP29):
  - Opinion 2/2017 on data processing at work, WP 249, Brussels, 8 June 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, WP 248 rev.01, as last revised and adopted on 4 October 2017.
  - Guidelines on Consent under Regulation 2016/679, WP 259rev.01, as last revised and adopted on 10 April 2018.
  - Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, adopted on 9 April 2014, https://www.dataprotection.ro/servlet/ViewDocument?id=1086, accessed 10 September 2019.

- Information Commissioner's Office, "Conducting privacy impact assessments Code of practice", 25 February 2014, https://www.pdpjournals.com/docs/88317.pdf, accessed 8 July 2019.

- Deliverable D4.3 Second Report: Report to the internal members of the consortium on the PESIA methodology and initial guidelines, VIRT-EU – Values and Ethics in Innovation for Responsible Technology in Europe, project no. 732027 funded by the European Union under Horizon 2020, ICT-35-2016 – Enabling responsible ICT-related research and innovation, 31 December 2018, https://blogit.itu.dk/inda/wp-content/uploads/sites/66/2019/02/Deliverable-4.3.pdf, accessed 27 June 2019.

- "The Standard Data Protection Model (SDM) – A concept for inspection and consultation on the basis of unified protection goals", V.1.0 – Trial version, Unanimously and affirmatively acknowledged (under the abstention of Bavaria) by the 92th Conference of the >Independent Data Protection Authorities of the Bund and Länder in Kühlungsborn on 9-10 November 2016, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methodology_V1_EN1.pdf, accessed 28 August 2019.
- Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment,
  - "Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems", 18 March 2014, https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf, accessed 28 August 2019.
  - "Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems", version 2 of 13 September 2018, https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf, accessed 28 August 2019.


Websites and blogs


- www.edps.europa.eu
- https://www.cnil.fr
- https://www.aepd.es
- https://ico.org.uk
- http://mathisis-project.eu
- http://forensor-project.eu
- https://virteuproject.eu
- http://www.europarl.europa.eu/thinktank/en/home.html
- https://ec.europa.eu/info/research-and-innovation/law-and-regulations/innovation-friendly-legislation_en