
# WHITE-LABEL SHOP FOR DIGITAL INTELLIGENT ASSISTANCE AND HUMAN-AI COLLABORATION IN MANUFACTURING

| | |
|---|---|
| **Title** | Contract and tort law for AI-based digital assistance solutions in manufacturing – interim report |
| **Document Owners** | KU Leuven |
| **Contributors** | KU Leuven |
| **Dissemination** | Sensitive |
| **Date** | 21/05/2024 |
| **Version** | 2.0 |

Co-funded by the Horizon Europe programme of the European Union under Grant Agreement № 101092176

# VERSION HISTORY

| Nr. | Date | Author (Organization) | Description | Dissemination |
|---|---|---|---|---|
| **0.1** | 31/03/2024 | Arno Cuypers<br>KUL | Initial Draft | Sensitive |
| **0.2** | 15/05/2024 | Maja Nisevic<br>KUL | Additions | Sensitive |
| **1.0** | 21/05/2024 | Arno Cuypers<br>KUL | Final version for internal review | Sensitive |
| **1.1** | 29/05/2024 | Arno Cuypers<br>KUL | Updates after internal review | Sensitive |
| **2.0** | 31/05/2024 | Arno Cuypers<br>KUL | Submitted version | Sensitive |

# REVIEWERS

| Name | Organization |
|---|---|
| Stefan WELLSANDT<br>Mina FOOSHERIAN | BIBA |
| Jan NAUMANN | UBREMEN |

# DISCLAIMER



# ACKNOWLEDGEMENT

This document is a deliverable of the WASABI project. This project has received funding from the European Union's Horizon Europe programme under grant agreement N° 101092176.

# CONTENTS

# 1. EXECUTIVE SUMMARY

This report represents deliverable 3.5 of KU Leuven – CiTiP in the WASABI project. This deliverable investigates the tort law ecosystem and its implications for applying digital assistance solutions in manufacturing. It maps and describes the EU regulatory framework applicable in the context of WASABI, and discusses liability for lack of compliance with EU law. Specifically, this deliverable focusses on the following EU Regulations and Directives: the AI Act, the proposal for an AI Liability Directive, the (revised) Product Liability Directive, and the General Data Protection Regulation. This deliverable provides an in depth exposition of the content of these legal acts, and applies them in the context of digital assistance solutions in manufacturing.

# 2. INTRODUCTION

## 2.1 Purpose and scope of the deliverable

This report investigates the tort law regime for applying digital assistance solutions in manufacturing. It gives an overview of the EU liability rules that are relevant in the context of WASABI. Liability refers to the act of being legally accountable for one's actions or omissions. This means that liability requires persons[1] to compensate those whom they injure[2] in certain ways. A distinction can be made between two kinds of liability: contractual and extra-contractual liability. Contractual liability means being liable for a breach of contract. Extra-contractual liability means being liable for something else than a breach of contract. The distinctive criteria is thus whether or not a contract exists between two or more parties.

Because WASABI is an EU funded project, the scope of this deliverable is limited to EU law. We will therefore not consider national law. This means that contract law falls outside the scope of this deliverable, since contract law is mainly a national matter. In addition, the EU legal framework protecting consumers when contracting with traders does not apply in the business-to-business (B2B) context of WASABI. Indeed, end-users of the WASABI digital assistants are manufacturers acting for business purposes. Since B2B contracts are not harmonized on an EU level, this report will not delve into contractual liability. It will only consider liability for damage caused by a violation of EU law. In addition, because of the B2B context of WASABI, EU consumer protection rules such as the General Product Safety Regulation and the Sale of Goods Directive, are not applicable. They fall therefore outside the scope of this deliverable.

It is important to note that this report only represents the author's interpretation of the law. This report does therefore not claim to formulate definitive answers to the legal questions it raises. This is one of the key characteristics of legal research. Indeed, the law rarely has an objective meaning. Interpretation is always subjective to a certain extent. According to McCrudden, an applicable legal norm on anything but the most banal question is likely to be complex, nuanced and contested.[3] The outcome of interpreting and analyzing the law within a specific context will therefore inevitably depend on the expertise, views and methods of the researcher. It is therefore likely that other legal researchers will reach different conclusions based on the same facts.

[1] Liability applies to both natural and legal persons.
[2] Injury or 'damage' covers both physical harm, as well as material damage.
[3] C. McCrudden, "Legal Research and the Social Sciences", *The Law quarterly review* 2006, 648.

## 2.2 Relation to other WPs and Tasks

This deliverable is part of Task 3.3. It uses deliverable 1.2 as input and will serve as input itself for Tasks 1.1 and 5.4. It should be mentioned that this deliverable is the first version of the "report on contract and tort law for AI-based assistance solutions in manufacturing". There will be an important update in M39.

The purpose of this deliverable (D3.5) is to give a *general* overview of the EU regulatory framework that applies to digital assistance solutions in manufacturing. The follow-up deliverable (3.8) will provide a more in-depth analysis of *specific* legal questions that arise among the consortium partners based on D3.5. This means that D3.8 will rely on the so-called "regulating-by-debate" approach and will therefore require input from the different project partners.

## 2.3 Structure of the deliverable

This document consists of three main parts. The first part (3) provides a brief introduction to WASABI by giving an overview of the purpose and scope of the project. Next, we briefly discuss WASABI's use cases. The second part (4) maps and describes the EU legal framework applicable in the context of WASABI. It gives an overview of the EU Regulations and Directives most relevant for applying digital assistance solutions in manufacturing. These are: the AI Act, the proposal for an AI Liability Directive, the (revised) Product Liability Directive and the General Data Protection Regulation. We will discuss each of these EU laws in depth and apply them in the context of WASABI. Finally, the last part (5) concludes this deliverable by summarizing our main findings.

# 3. LIABILITY AND THE WASABI PROJECT

## 3.1 The WASABI project: purpose and scope

Before delving into the regulatory requirements for WASABI, it is essential to grasp the project's purpose and scope. The WASABI project holds substantial relevance within the liability framework discourse as it attempts to pioneer digital assistants tailored for manufacturing settings. These conversational agents, powered by machine learning, are designed to assist workers in the performance of monotonous and stressful tasks. These digital assistants therefore have the potential to enhance productivity and foster a more conducive work atmosphere. Recognizing the liability ramifications of deploying these digital assistants is imperative for the project's success.

The WASABI digital assistants are conversational agents. A conversational agent is an application that accepts user input in the form of voice or text and provides responses in natural language. There are two kinds of conversational agents: chatbots and voice-based assistants. Conversations with chatbots are in written text, while conversations with voice-based assistants happen through speech. The WASABI digital assistants are voice-based but support text input as well. The user can choose how to interact with the assistant.

The advantage of voice-based assistants over chatbots is that they can be used hands-free and are therefore faster. That is why voice-based assistants are better suited for manufacturing, where workers often have their hands full, and speed can be of the essence. However, voice-based assistants are also more prone to error than chatbots. If a WASABI digital assistant misunderstands a question from a worker and this leads to damage, the question is who can be held liable.

WASABI's focus on developing human-centered AI is a testament to its commitment to supporting, not replacing, workers. Its digital assistants are designed to help humans achieve their goals without marginalizing them. For

instance, one of WASABI's use cases is developing a digital assistant that trains new workers. This implementation of AI in the workplace not only offers workers the opportunity to learn more about this technology but also has the potential to increase their digital literacy, thereby enhancing their skills and capabilities.

The following section gives a brief overview of the WASABI use cases.

## 3.2 WASABI use cases

WASABI has three use cases in manufacturing. The first use case is augmented waste management and valorization. The second use case is workforce management. The third use case is product quality testing. These three use cases cover the entire product life cycle. The first use case covers production and recycling, while the second and third use cases focus on production and product quality testing.

The **first use case** is augmented waste management and valorization. This use case focuses on the management of inadmissible items in manufacturing with the aim of inventory management and minimization of items found to be suboptimal based on their specific manufacturing or tolerance criteria. If a production process cannot avoid generating non-conforming items for technical reasons, these items may still be reusable by other organizations, provided the characteristics of these items meet certain requirements.[4] Workers will describe and retrieve inadmissible items through a mobile conversational interface and rich-media records, such as images and videos of inadmissible items and relevant machinery. If users require specific expert-level entity descriptions, e.g., a laboratory analysis, they will receive suggestions on contacting local experts. WASABI will demonstrate its solution in this case by customizing and connecting the *COALA assistant* with the *rEUse platform*, as well as in two cases with target users, TRIMEK and CROMA. In case of TRIMEK, users can register artifacts in the rEUse platform via the assistant. They can also add calibration information for the registered artifacts. Finally, if an artifact is sold, the information of the buyer can be added by the user. Users can also edit this information via the rEUse platform. They can use the assistant to retrieve this info as well. Second, in recycling and revamping, surgical tools provider CROMA will check the instruments used after each surgery following SOPs (Standardized Operation Procedures): if they are still fit for use, they are sterilized (following another SOP) and used again, and if they are not, the information on the tool is published on the rEUse platform for it to be recycled.[5]

**The second use case** is workforce management. WASABI will develop a digital assistant to onboard and integrate new workers faster into the workforce of a manufacturing organization. Key characteristics of these solutions are multilingual conversational interfaces, customizable personas, and adaptable assistance based on learning progress. This use case aims to increase societal resilience after a crisis and increase agility by rapidly increasing and upskilling an organization's workforce. A second effect is that employers could integrate new workers faster and free up the time of the existing employees, resulting in productivity gains.[6]

In this use case, an onboarding assistant is developed for EPISCAN. EPISCAN is a Canarian-based company that produces personal protective equipment (PPE). The main products produced by EPISCAN are two types of masks, surgical and FFP2 without exhalation valves.[7]

[4] Deliverable 2.4.
[5] White-label shop for digital intelligent assistance and human-AI collaboration in manufacturing (WASABI), 149-150. (Hereafter: WASABI proposal).
[6] WASABI proposal, 150.
[7] Deliverable 2.4.

**The third use case** is assisted quality assurance for sustainable products. This use case aims to enhance product quality testing processes by leveraging a digital assistant that supports workers in executing validation protocols for safer and more sustainable products. This assistant integrates analytics and predictive modules to optimize testing, reduce energy consumption, and provide real-time guidance, fostering collaboration between the assistant and operators. WASABI aims to demonstrate this solution across the five business cases, i.e. REINOVA, TRIMEK, EPISCAN, CROMA, and SILK-BIO, spanning automotive battery testing, dimensional metrology, EPI material testing, and prosthetics quality testing, respectively, to improve overall product quality and worker efficiency.[8] For a detailed overview of this use case, we refer to deliverable 2.4.

In short, the WASABI project will develop AI systems that can perform specific manufacturing tasks. However, the question arises: if these systems malfunction and cause damage, **who can be held liable?**

The following sections attempt to answer this question by identifying the EU regulatory framework applicable to the WASABI digital assistants.

# 4. EU REGULATORY FRAMEWORK

In order to avoid liability, it is important that the WASABI project complies with its obligations under EU law. The most relevant EU legal instruments in this regard are: the AI Act, the proposal for an AI Liability Directive, the (revised) Product Liability Directive and the General Data Protection Regulation. The next sections provide a detailed overview of these legal acts in the context of applying digital assistance solutions in manufacturing.

## 4.1 EU liability rules concerning AI systems

This section provides an overview of the EU regulatory framework specifically tailored to AI systems. Relevant EU laws in this regard are the AI Act and the proposal for an AI Liability Directive. The AI Act imposes a series of obligations on providers and developers of high-risk AI systems. An infringement of these obligations could give rise to liability. In this regard, the proposal for an AI Liability Directive lowers the burden of proof for claimants when AI systems cause damage. This increases the liability risk of both the developers and the ends-users of the WASABI digital assistants. We will first give an overview of the AI Act in the context of applying digital assistance solutions in manufacturing. Afterward, we will discuss the proposal for an AI Liability Directive and apply it to the WASABI digital assistants.

### 4.1.1 AI Act

In April 2021, the European Commission issued its draft Regulation on AI. After nearly three years of intense negotiation between the EU Parliament, Council and Commission, an agreement on the text was finally reached in December 2023. The text was adopted by the Council on 2 February 2024 and approved by the Parliament a month later, on March 13th.

This part gives an overview of the provisions of the AI Act which are the most relevant in the context of WASABI. In the next paragraphs, we will discuss the scope of application of the AI Act, its risk-based approach, the mandatory requirements that apply to high-risk AI systems, the obligations of providers and deployers of high-risk AI systems, the transparency obligations that apply to limited-risk AI systems, and compliance with the AI Act through harmonized standards. Finally, it is also important to know when the AI Act enters into force.

[8] Deliverable 2.4.

Before starting our analysis, it is important to note that the AI Act is a relatively new piece of legislation and is not yet applicable. This means that there is still considerable uncertainty on how the AI Act will be applied in practice, and on how its provisions must be interpreted. Indeed, there are, for instance, no rulings by the Court of Justice of the EU on the interpretation of the AI Act. Therefore, it must be stressed that the following paragraphs represent the views of the author of this deliverable. It is possible that other researchers have a different interpretation of the AI Act and thus reach different conclusions based on the same facts.

**Scope of application**

The AI Act defines an AI system as "…a machine-based system, designed to operate with varying levels of autonomy, and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, or decisions, that can influence physical or virtual environments."[9] This definition is rather vague. For instance, it is unclear what "varying levels of autonomy" exactly means. According to recital 12 of the AI Act, AI systems exhibit autonomy if they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention.

In the current stage of the WASABI project, the digital assistants are reactive. This means that all interactions with the assistant are initiated by the user. Therefore, it could be argued that the digital assistants lack the required autonomy to qualify as 'AI' within the meaning of the AI Act. As a result, the digital assistants would fall outside the scope of the AI Act. **This would mean that the AI Act does not apply in the context of WASABI**.

Nevertheless, there are several reasons why this deliverable will apply the AI Act to the WASABI digital assistants. First, the meaning of 'autonomy' under the AI Act is unclear. It is therefore possible that the digital assistants are considered to be autonomous even though they are only reactive. Second, it is possible that the digital assistants become more proactive at a later stage of the project. If that is the case, it could be argued that the assistants exhibit autonomy and are therefore 'AI systems' within the meaning of the AI Act. Finally, Recital 12 of the AI Act clarifies that the definition of 'AI' includes machine learning approaches. Since the digital assistants rely on machine learning models, it could be argued that they qualify as 'AI systems' under the AI Act, even though they may not operate with "varying levels of autonomy".

The material scope of the AI Act is limited in several ways. For instance, the AI Act does not apply to AI systems developed and put into service for the sole purpose of scientific research and development. Also excluded is any research, testing, and development activity regarding AI systems prior to being placed on the market or put into service.[10] However, the AI Act applies as soon as an AI system developed through such research and development is placed on the market or put into service.[11]

It is unclear what exactly the phrase "for the sole purpose of scientific research" means. The WASABI digital assistants are mainly developed to become commercial or publicly available solutions.[12] As a result, they will probably not benefit from this exception. On the other hand, the exception related to product-oriented research,

[9] Article 3(1) Regulation of the European Parliament and of the Council of 19 April 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available: CO_TA (europa.eu). (hereafter: AI Act).

[10] According to Article 2 (8) AI Act, this exemption does not apply to testing in real world conditions.

[11] Recital 25 AI Act.

[12] Public means, for instance, that the source code is available.

testing and development will likely apply in the context of WASABI. This means that the AI Act will not apply to the WASABI digital assistants as long as they are not placed on the market or put into service. However, this exception may have little use in practice. If an AI system is developed with the goal of placing it on the EU market, then it is not recommended to wait until the system is finished to comply with the AI Act. It is important to take the AI Act into account during the research, development and testing phase. This will save both time and money.

The WASABI digital assistants are developed with a goal of placing them on the EU market. It is therefore important to take the AI Act into account during the research, development and testing phase of the WASABI project.

The scope of the AI Act is quite broad. It applies to operators of AI systems. The term 'operator' refers to a series of different actors. These are: providers, product manufacturers, deployers, authorized representatives, importers and distributors.[13] Each actor has a specific meaning and is subject to specific obligations under the AI Act. In the context of WASABI, providers and deployers are the most relevant actors. This deliverable will therefore mainly focus on these persons.

The AI Act applies to **providers** placing on the market or putting into service an AI system in the EU.[14] A 'provider' is a natural or legal person, public authority, agency, or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the system into service under its own name or trademark, whether for payment or free of charge.[15] To place an AI system on the market means to make it available on the EU market for the first time.[16] 'Making available' means any supply of an AI system for distribution or use on the EU market during a commercial activity, whether in return for payment or free of charge.[17] Lastly, 'putting into service' means supplying an AI system for first use directly to the deployer or for own use in the EU for its intended purpose.[18]

Recital 57 of the AI Act emphasizes that anyone who puts his or her trademark or name on an AI system already placed on the market or put into service should be considered a provider of that system and consequently assume all the relevant obligations. However, contractually, it is permitted to agree on a different allocation of obligations between the parties.

The AI Act also applies to **deployers** of AI systems.[19] A 'deployer' is any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of personal, non-professional activity.[20]

The developers of the WASABI digital assistants will qualify as providers of AI systems. They will therefore have to comply with the obligations the AI Act imposes on providers. The end-users who deploy the digital assistants in their factories will qualify as deployers of AI systems. They will have to comply with the obligations imposed by the AI Act on deployers.

[13] Article 3(8) AI Act.
[14] Article 2.1 (a) AI Act.
[15] Article 3(3) AI Act.
[16] Article 3(9) AI Act.
[17] Article 3(10) AI Act.
[18] Article 3(11) AI Act.
[19] Article 2.1 (b) AI Act.
[20] Article 3(4) AI Act.

**Risk-based approach**

The AI Act follows **a risk-based approach**. This means that AI systems are regulated based on their risk. Risk means the severity of a harm multiplied by its probability of occurrence.[21] The AI Act has four risk categories: unacceptable risk, high risk, limited risk, and minimal risk. Each category is subject to a different regime.[22] First, AI systems that pose an unacceptable risk are prohibited. Second, high-risk AI systems are subject to several mandatory safety requirements. Third, certain transparency obligations apply to AI systems that pose a limited risk because they are intended to interact with natural persons or to generate content.[23] Fourth, minimal-risk AI systems are not subject to binding obligations. However, providers of such systems are encouraged to create codes of conduct based on the mandatory requirements that apply to high-risk systems.[24]

Certain AI systems are prohibited. They are deemed to pose an unacceptable risk to EU values of respect for human dignity, freedom, equality, democracy and the rule of law, and to EU fundamental rights, such as the right to non-discrimination, data protection and privacy and the rights of the child.[25] They have therefore no place on the EU market.

The following AI systems are **prohibited** within the EU: systems that use manipulative and subliminal techniques, systems that exploit specific vulnerabilities of a person or group of persons which are likely to cause that person or group significant harm, biometric categorization systems, social scoring systems, real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, systems that predict recidivism solely based on profiling, AI systems that perform untargeted scraping of facial images from the internet or CCTV footage with the specific purpose to create or expand facial recognition databases, and emotion recognition systems used in the workplace or education institutions.[26] It is not likely that the WASABI digital assistants will fall under this list of prohibited systems. Therefore, this category of AI systems will not be discussed further in this deliverable.

Chapter III of the AI Act imposes mandatory safety requirements on **high-risk** AI systems. Article 6 makes a distinction between two categories of high-risk AI systems. First, AI systems that are products or safety components of products already covered by certain EU health and safety harmonization legislation (such as toys, machinery, lifts, or medical devices) and required to undergo a third-party conformity assessment prior to being made available on the market.[27] The exact list can be found in Annex I of the AI Act. The second category are standalone AI systems that pose a high risk of harm to the health and safety or the fundamental rights of persons and are used in a number of specifically pre-defined areas specified in the AI Act.[28] These are listed in Annex III of the AI Act. In the next paragraphs, we will first consider whether the WASABI digital assistants fall under the first category of high-risk AI systems. Afterward, we will investigate whether the digital assistants fall under the second category of high-risk systems.

The first category of high-risk AI systems is defined in article 6.1 of the AI Act. According to this provision, an AI system is high-risk if two conditions are fulfilled. First, the AI system is intended to be used as a **safety component of a product**, or the AI system is itself a **product**, covered by the EU harmonization legislation listed in Annex I of

[21] Article 3 (2) AI Act.
[22] Recital 26 AI Act.
[23] Recital 132 AI Act.
[24] Recital 165 AI Act.
[25] Recital 28 AI Act.
[26] Article 5 AI Act.
[27] Article 6(1) AI Act.
[28] Article 6(2) AI Act and Recital 52 AI Act.

the AI Act. Second, the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a **third-party conformity assessment**, with a view to the placing on the market or putting into service of that product pursuant to the EU harmonization legislation listed in Annex I of the AI Act. It is irrelevant whether or not the AI system in question is placed on the market or put into service independently from the products covered by the EU harmonization legislation listed in Annex I.

This provision requires further clarification. A 'safety component of a product or system' means a component of a product or of a system which fulfils a **safety function** for that product or system or the failure or malfunctioning of which **endangers the health and safety** of persons or property.[29] Recital 47 of the AI Act emphasizes the importance of preventing and mitigating the safety risks that may be generated by a product as a whole due to its digital components, including AI systems. For instance, autonomous systems in the context of manufacturing should be able to safely operate and perform their functions in complex environments.

To reiterate, Annex I of the AI Act contains a list of EU harmonization legislation that regulates certain products. If an AI system qualifies as a product or as a safety component of a product that falls under one of these laws, it is high-risk and therefore subject to the mandatory safety requirements listed in chapter III of the AI Act. The most relevant piece of EU harmonization legislation listed in Annex I of the AI Act in the context of WASABI is Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery, or the '**Machinery Regulation**' for short.

The Machinery Regulation applies to machinery and related products.[30] Machinery is defined as "an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application."[31] The notion of 'related products' includes 'safety components' of machinery.[32] A 'safety component' refers to "…a physical or digital component, including software, of a product within the scope of the Machinery Regulation, which is designed or intended to fulfil a safety function and which is independently placed on the market, the **failure or malfunction of which endangers the safety of persons**, but which is not necessary in order for that product to function or for which normal components may be substituted in order for that product to function."[33] Lastly, 'safety function' means "a function that serves to fulfil a protective measure designed to eliminate, or, if that is not possible, to reduce, a risk, which, if it fails, could result in an increase of that risk."[34]

The Machinery Regulation applies to the WASABI digital assistants if the digital assistants qualify as 'safety components' of machinery. There are a number of reasons why this is the case. First, Annex II of the Machinery Regulation contains an indicative list of safety components. This list includes safety components with fully or partially self-evolving behavior using machine learning approaches ensuring safety functions.[35] Since the WASABI digital assistants rely on machine learning models, it could be argued that they fall under this category of safety components. However, the assistants do not learn after their deployment. They are only updated periodically. Nevertheless, it is possible that the prediction system of the digital assistant for product quality testing relies on an automated machine learning process. This may be considered as fully or partially self-evolving behavior.

[29] Article 3(14) AI Act.
[30] Article 2.1 Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (hereafter: Machinery Regulation). Available: Regulation - 2023/1230 - EN - EUR-Lex (europa.eu).
[31] Article 3 (1) (a) Machinery Regulation.
[32] Article 2 (1) (b) Machinery Regulation.
[33] Article 3 (3) Machinery Regulation.
[34] Article 3 (4) Machinery Regulation.
[35] Annex II (19) Machinery Regulation.

**Second, and most important, the WASABI digital assistants are used in a manufacturing context as part of machinery, where they fulfil a safety function**. For instance, the onboarding assistant will train new workers on how to operate machinery. If workers are not properly trained, they are not fit to operate potentially dangerous machines. Therefore, if the onboarding assistant malfunctions, workers' safety is at risk. Furthermore, the assisted quality assurance use case is specifically meant to increase product and worker safety. Lastly, it is also important that the WASABI Waste Inspector functions properly. For instance, it helps determine whether surgical instruments are still fit for use. A mistake in this regard could endanger people's health. In short, if the digital assistants malfunction, they endanger the safety of persons. It is therefore likely that they are a 'safety component' within the meaning of Article 3 (3) of the Machinery Regulation.

The third and last reason why the Machinery Regulation applies to the WASABI digital assistants, is that its recitals explicitly confirm that the regulation should cover the safety risks stemming from new digital technologies.[36]

In conclusion, the WASABI digital assistants will likely be considered as **safety components of machinery**. They therefore qualify as 'related products' within the meaning of the Machinery Regulation. As a result, the **Machinery Regulation is applicable**. This also means that the digital assistants are safety components of products covered by the EU harmonization legislation listed in Annex I of the AI Act. Consequently, **the digital assistants qualify as high-risk systems** under Article 6 (1) AI Act. This means that they will have to comply with the safety requirements imposed by the AI Act on such systems.

It is also possible that the WASABI digital assistants fall under the second category of high-risk AI systems.[37] These are standalone AI systems that pose a high risk of harm to the health and safety or the fundamental rights of persons and are used in a number of pre-defined areas specified in the AI Act.[38] These areas are listed in Annex III of the AI Act. The most relevant area in the context of WASABI is employment. According to Annex III (4) (b) of the AI Act, AI systems are high-risk if they are intended to be used to monitor or evaluate the performance and behavior of persons in a work-related relationship. In principle, the WASABI digital assistants are not used to make decisions about work-related relationships, nor to monitor and evaluate the performance of workers. The assistants are only meant to support workers when operating machinery. **However, while the assistants may not *directly* monitor workers, end-users could potentially rely on the assistants to *indirectly* evaluate the performance of their employees.** For example, manufacturing companies could evaluate their workers based on how well they are able to adapt to new technologies. This could potentially lead to discrimination against persons with disabilities or against certain age groups. This is all the more pertinent, since integrating workers with disabilities falls outside the scope of the WASABI project.[39] In addition, evaluating workers based on their ability to work with the WASABI digital assistants may undermine their fundamental rights to data protection and privacy.[40] Consequently, one could argue that the digital assistants qualify as high-risk AI systems within the meaning of Article 6 (2) of the AI Act.

It is possible that the WASABI digital assistants qualify as high-risk AI systems within the meaning of the AI Act. First, they likely function as **safety components of a product** covered by the EU harmonization legislation listed in Annex I of the AI Act. Specifically, the digital assistants probably qualify as safety components of machinery within the meaning of the Machinery Regulation. They therefore fall under the first category of high-risk AI systems

[36] Recital 12 Machinery Regulation.
[37] Article 6 (2) AI Act.
[38] Article 6 (2) AI Act and Recital 52 AI Act.
[39] WASABI proposal, 143.
[40] Recital 57 AI Act.

as stipulated in Article 6 (1) of the AI Act. In addition, the WASABI digital assistants can potentially be used to evaluate the performance of workers. It is therefore possible that they fall under the second category of high-risk AI systems. These are the AI-systems listed in Annex III of the AI Act. If the WASABI digital assistants are high-risk, they should comply with the safety requirements imposed by the AI Act on such systems.

**Safety requirements for high-risk AI systems**

High-risk AI systems are subject to a number of safety requirements listed in chapter III, section 2, of the AI Act. These requirements are: establishing a risk management system, applying appropriate data governance practices, drawing up technical documentation, keeping a record, and ensuring sufficient transparency and human oversight. Lastly, high-risk AI systems must achieve an appropriate level of accuracy, robustness and cybersecurity. It is the **obligation of the provider** to ensure that its high-risk AI system complies with these safety requirements.[41] The next paragraphs will go over each safety requirement, one by one.

First, Article 9 of the AI Act states that **a risk management system** shall be established, implemented, documented and maintained in relation to high-risk AI systems. This is an iterative process. The risk management system must be run throughout the entire life-cycle of a high-risk AI system. It therefore requires regular review and updating. The risk management system must comprise at least the following steps:

(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;
(b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;
(c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72 of the AI Act;
(d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).[42]

The risk management system must not address every risk posed by a high-risk AI system. It only concerns those risks which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.[43] Furthermore, the risk management measures referred to in point (d) shall give due consideration to the effects and possible interaction resulting from the combined application of the other safety requirements imposed on high-risk systems, with a view to minimizing risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.[44]

The aim of the risk management measures referred to in point (d) is to bring the risk associated with each hazard, as well as the overall residual risk of the high-risk AI system down to a level that is **acceptable**. In identifying the appropriate risk management measures, the following shall be ensured:

[41] Article 16 (a) AI Act.
[42] Article 9.2 AI Act.
[43] Article 9.3 AI Act.
[44] Article 9.4 AI Act.

(a) elimination or reduction of the identified risks as far as technically feasible through adequate design and development of the high-risk AI system;
(b) where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated;
(c) provision of information required pursuant to Article 13 of the AI Act and, where appropriate, training to deployers.[45]

With a view to eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, the training to be expected by the deployer, and the presumable context in which the system is intended to be used.[46]

The AI Act does not specify when a risk is 'acceptable'. **This is an assessment that has to be made by the provider of the high-risk AI system in question.** The provider has to demonstrate that all technically feasible measures were taken to either eliminate the identified risks, or reduce them as much as possible. Providers are free to choose how they will comply with the safety requirements of the AI Act. It is therefore up to them to decide when the risk posed by their high-risk systems is brought down to an acceptable level. However, providers will have to explain how they have addressed the risk posed by their high-risk systems, and why this risk can be considered acceptable. In other words, providers have to be able to tell a convincing story on their interpretation of the law. They need to show that they made deliberate choices in managing the risk of their high-risk systems, and provide arguments on why they did everything they could to eliminate or reduce these risks as much as possible.

The European Committee for Standardization (CEN) has already developed **a harmonized standard concerning risk management**.[47] It provides guidance on how providers can manage risk related to AI. It also aims to assist providers to integrate risk management into their AI-related activities and functions. It moreover describes processes for the effective implementation and integration of AI risk management. Compliance with such a harmonized standard entails a presumption of compliance with the law.[48] The role of harmonized standards in the AI Act will be detailed further below.

In addition, high-risk AI systems shall be **tested** for the purpose of identifying the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the safety requirements imposed by the AI Act.[49] Testing procedures may include testing in real-world conditions in accordance with Article 60 of the AI Act.[50] The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.[51]

[45] Article 9.5 AI Act.
[46] Article 9.5 AI Act.
[47] CEN, Information technology - Artificial intelligence - Guidance on risk management (ISO/IEC 23894:2023). Available: CEN - CEN/CLC/JTC 21 (cencenelec.eu).
[48] Article 40 (1) AI Act.
[49] Article 9.6 AI Act.
[50] Article 9.7 AI Act.
[51] Article 9.8 AI Act.

Lastly, when implementing the risk management system, providers must give due consideration to whether the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups.[52]

Article 10 of the AI Act concerns **data governance**. High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet certain quality criteria.[53] For the development of high-risk AI systems not using techniques involving the training of AI models, these criteria shall only apply to the testing data sets.[54]

First, training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

(a) the relevant design choices;
(b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;
(c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;
(d) the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;
(e) an assessment of the availability, quantity and suitability of the data sets that are needed;
(f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under EU law, especially where data outputs influence inputs for future operations;
(g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);
(h) the identification of relevant data gaps or shortcomings that prevent compliance with the AI Act, and how those gaps and shortcomings can be addressed.[55]

Furthermore, training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof.[56]

Finally, data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioral or functional setting within which the high-risk AI system is intended to be used.[57]

Article 11 of the AI Act requires that **technical documentation** of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date. The technical documentation shall be drawn up in such a way as to demonstrate that the high-risk AI system complies with the safety requirements imposed by the AI Act and to provide national competent authorities and notified bodies with the necessary information in a clear and comprehensive form to assess the compliance of the AI system with those

[52] Article 9.9 AI Act.
[53] Article 10.1 AI Act.
[54] Article 10.6 AI Act.
[55] Article 10.2 AI Act.
[56] Article 10.3 AI Act.
[57] Article 10.4 AI Act.

requirements. It shall contain, at a minimum, the elements set out in Annex IV of the AI Act. SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner. To that end, the EU Commission shall establish a simplified technical documentation form targeted at the needs of small and microenterprises. Where an SME, including a start-up, opts to provide the information required in Annex IV in a simplified manner, it shall use the form referred to in this paragraph.[58] **This is relevant for the WASABI project, since the intended end-users are primarily SME's**.

Article 12 of the AI Act stipulates that high-risk AI systems shall technically allow for the **automatic recording of events (logs)** over the lifetime of the system. In order to ensure a level of traceability of the functioning of a high-risk AI system that is appropriate to the intended purpose of the system, logging capabilities shall enable the recording of events relevant for:

(a) identifying situations that may result in the high-risk AI system presenting a risk within the meaning of Article 79(1) of the AI Act or in a substantial modification;
(b) facilitating the post-market monitoring referred to in Article 72 of the AI Act; and
(c) monitoring the operation of high-risk AI systems referred to in Article 26(5) of the AI Act.[59]

Article 13 of the AI Act imposes **transparency** requirements on high-risk AI systems. High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured with a view to achieving compliance with the relevant obligations of the provider and deployer.[60]

In addition, high-risk AI systems shall be accompanied by **instructions for use** in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers.[61] The instructions for use shall contain at least the following information:

(a) the identity and the contact details of the provider and, where applicable, of its authorized representative;
(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:
    i. its intended purpose;
    ii. the level of accuracy, including its metrics, robustness and cybersecurity referred to in Article 15 of the AI Act against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;
    iii. any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights referred to in Article 9(2) of the AI Act;
    iv. where applicable, the technical capabilities and characteristics of the high-risk AI system to provide information that is relevant to explain its output;
    v. when appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used

[58] Article 11.1 AI Act.
[59] Article 12.2 AI Act.
[60] Article 13.1 AI Act.
[61] Article 13.2 AI Act.

vi. when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system;
vii. where applicable, information to enable deployers to interpret the output of the high-risk AI system and use it appropriately;

(c) the changes to the high-risk AI system and its performance which have been predetermined by the provider at the moment of the initial conformity assessment, if any;
(d) the human oversight measures referred to in Article 14 of the AI Act, including the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI systems by the deployers;
(e) the computational and hardware resources needed, the expected lifetime of the high-risk AI system and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of that AI system, including as regards software updates;
(f) where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs in accordance with Article 12 of the AI Act.[62]

Article 14 of the AI Act requires **human oversight**. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.[63] Furthermore, human oversight shall aim to prevent or minimize the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular where such risks persist despite the application of other safety requirements imposed by the AI Act.[64]

The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system, and shall be ensured through either one or both of the following types of measures:

(a) measures identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;
(b) measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the deployer.[65]

In order to ensure effective human oversight, the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:

(a) to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance;
(b) to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;
(c) to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available;
(d) to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system;

[62] Article 13.3 AI Act.
[63] Article 14.1 AI Act.
[64] Article 14.2 AI Act.
[65] Article 14.3 AI Act.

(e) to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state.[66]

Finally, Article 15 of the AI Act requires high-risk AI systems to be designed and developed in such a way that they achieve an appropriate level of **accuracy, robustness, and cybersecurity**, and that they perform consistently in those respects throughout their lifecycle.[67] The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.[68] High-risk AI systems shall be as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. Technical and organizational measures shall be taken in this regard.

The **robustness** of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans. High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.[69]

Lastly, high-risk AI systems shall be resilient against attempts by unauthorized third parties to alter their use, outputs or performance by exploiting system vulnerabilities. The technical solutions aiming to ensure the **cybersecurity** of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.[70]

In short, high-risk AI systems are subject to a vast amount of safety requirements. These safety requirements correspond to a series of obligations imposed on providers and deployers of high-risk AI systems. These obligations will be discussed in the next section.

Under the AI Act, the WASABI digital assistants should comply with the following safety requirements: risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity.

| **Safety requirements for high-risk AI systems** |
|---|
| Risk management |
| Data governance |
| Technical documentation |
| Record-keeping |
| Transparency |
| Human oversight |
| Accuracy |

[66] Article 14.4 AI Act.
[67] Article 15.1 AI Act.
[68] Article 15.3 AI Act.
[69] Article 15.4 AI Act.
[70] Article 15.5 AI Act.

| |
|---|
| Robustness |
| Cybersecurity |

**Obligations of providers and deployers of high-risk AI systems**

The majority of the obligations imposed by the AI Act fall on the **provider** of high-risk AI systems. In the context of WASABI, this is the **developer of the digital assistants**. He or she should comply with the obligations listed in article 16 of the AI Act. The next paragraphs will go over these obligations one by one. Afterward, we will discuss the obligations of deployers of high-risk systems.

According to **Article 16 of the AI Act**, providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the safety requirements set out in the previous section of this deliverable;
(b) indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted;
(c) have a quality management system in place which complies with Article 17 of the AI Act;
(d) keep the documentation referred to in Article 18 of the AI Act;
(e) when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19 of the AI Act;
(f) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43 of the AI Act, prior to its being placed on the market or put into service;
(g) draw up an EU declaration of conformity in accordance with Article 47 of the AI Act;
(h) affix the CE marking to the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, to indicate conformity with the AI Act, in accordance with Article 48 of the AI Act;
(i) comply with the registration obligations referred to in Article 49(1) of the AI Act;
(j) take the necessary corrective actions and provide information as required in Article 20 of the AI Act;
(k) upon a reasoned request of a national competent authority, demonstrate the conformity of the high-risk AI system with the safety requirements set out in the previous section of this deliverable;
(l) ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

A number of these obligations require further clarification. For example, providers of high-risk AI systems must have a **quality management system** in place in accordance with Article 17 of the AI Act. The purpose of this quality management system is to ensure compliance with the AI Act. The quality management system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;
(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;
(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;
(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out

(e) technical specifications, including standards, to be applied and, where the relevant harmonized standards are not applied in full or do not cover all of the relevant safety requirements set out in the previous section of this deliverable, the means to be used to ensure that the high-risk AI system complies with those requirements
(f) systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems;
(g) the risk management system referred to in Article 9 of the AI Act;
(h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 72 of the AI Act;
(i) procedures related to the reporting of a serious incident in accordance with Article 73 of the AI Act;
(j) the handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;
(k) systems and procedures for record-keeping of all relevant documentation and information;
(l) resource management, including security-of-supply related measures;
(m) an accountability framework setting out the responsibilities of the management and other staff with regard to all the aspects listed above.

Furthermore, according to Article 18 of the AI Act, providers have to keep certain **documentation** on their high-risk AI systems:

(a) the technical documentation referred to in Article 11 of the AI Act;
(b) the documentation concerning the quality management system referred to in Article 17 of the AI Act;
(c) the documentation concerning the changes approved by notified bodies, where applicable;
(d) the decisions and other documents issued by the notified bodies, where applicable;
(e) the EU declaration of conformity referred to in Article 47 of the AI Act.

This documentation must be kept at the disposal of the national competent authorities for a period of 10 years after the high-risk AI system has been placed on the market or put into service.[71]

Article 19 of the AI Act requires providers of high-risk AI systems to **keep the logs** referred to in article 12(1) of the AI Act, automatically generated by their high-risk AI systems, to the extent such logs are under their control. These logs must be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in the applicable EU or national law, in particular in EU law on the protection of personal data.

Article 20 of the AI Act imposes a **duty to inform** on providers of high-risk AI systems. Providers that have reason to consider that a high-risk AI system that they have placed on the market or put into service is not in conformity with the AI Act shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it, to disable it, or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system concerned and, where applicable, the deployers, the authorized representative and importers accordingly.

Finally, providers of high-risk systems are required to **cooperate with competent authorities**. Upon a reasoned request by a competent authority, providers shall provide that authority all the information and documentation

[71] Article 18.1 AI Act.

necessary to demonstrate the conformity of the high-risk AI system with the safety requirements detailed in the previous section of this deliverable. Furthermore, upon a reasoned request by a competent authority, providers shall also give the requesting competent authority, as applicable, access to the automatically generated logs of the high-risk AI system referred to in Article 12(1) of the AI Act, to the extent such logs are under their control.

The **obligations of deployers** of high-risk AI systems are listed in Article 26 of the AI Act. In the context of WASABI, complying with these obligations will be the **responsibility of the end-users** who purchase a digital assistant from the WASABI white-label shop, and deploy it in their factories. In essence, deployers of a high-risk system must closely monitor the operation of their system and use it according to the instructions for use which have been drawn up by the provider of the system. The next few paragraphs give a detailed overview of the obligations that apply to deployers of high-risk systems.

First, deployers of high-risk AI systems shall take appropriate technical and organizational measures to ensure they **use such systems in accordance with the instructions for use** accompanying the systems.[72] Second, deployers shall assign **human oversight** to natural persons who have the necessary competence, training and authority, as well as the necessary support.[73] Third, to the extent the deployer exercises control over the input data, the deployer shall ensure that the **input data is relevant and sufficiently representative** in view of the intended purpose of the high-risk AI system.[74] Fourth, deployers shall **monitor the operation** of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72 of the AI Act.[75]

Where deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system **presenting a risk** within the meaning of Article 79(1) of the AI Act, they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall **suspend the use** of that system.[76] An AI system 'presents a risk' within the meaning of Article 79(1) of the AI Act, if it presents a risk to the health, safety or fundamental rights of persons.[77] Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident.[78]

In addition, deployers of high-risk AI systems shall **keep the logs** automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in applicable EU or national law, in particular in EU law on the protection of personal data.[79]

Before putting into service or using a high-risk AI system at the workplace, **deployers who are employers** shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. This information shall be provided, where applicable, in accordance with the rules and procedures laid down in EU and national law and practice on information of workers and their representatives. **This obligation is especially relevant in the context of WASABI, where deployers are manufacturing companies that will**

[72] Article 26 (1) AI Act.
[73] Article 26 (2) AI Act.
[74] Article 26 (4) AI Act.
[75] Article 26 (5) AI Act.
[76] Article 26 (5) AI Act.
[77] Article 79 (1) AI Act.
[78] Article 26 (5) AI Act.
[79] Article 26 (6) AI Act.

**integrate high-risk AI systems in the workplace.** The end-users should therefore comply with this obligation, before deploying a digital assistant in their factories.

Furthermore, where applicable, deployers of high-risk AI systems shall use the information provided on the basis of the transparency requirement laid down in Article 13 of the AI Act, to comply with their obligation to carry out a **data protection impact assessment** under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680.[80]

Lastly, Article 4 of the AI Act requires both providers and deployers of AI systems to take measures to ensure, to their best extent, a sufficient level of **AI literacy** of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used. The notion of 'AI literacy' means the skills, knowledge and understanding that allow someone to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause.[81]

In the context of WASABI, this obligation will mainly fall on the end-users**. The end-users must ensure that their employees have a sufficient level of AI literacy.** This means that they must receive training to obtain the skills, knowledge and understanding necessary to use the WASABI digital assistants in a safe way. In addition, they must be made aware of the risks associated with using digital assistants, as well as the possible harm the assistants may cause should they malfunction.

The AI Act imposes a series of obligations on both the developers and the end-users of the WASABI digital assistants. The developers of the digital assistants should comply with the obligations of providers of high-risk AI systems. These obligations include: having a quality management system in place, keeping certain documentation and the logs automatically generated by high-risk AI systems, a duty to inform the deployer in case of lack of conformity with the AI Act, and a duty to cooperate with competent authorities. The end-users of the WASABI digital assistants should comply with the obligations of deployers of high-risk AI systems. These obligations include: using high-risk systems according to the instructions for use, monitoring the operation of high-risk systems, ensuring human oversight, and suspending the use of high-risk systems that present too high of a risk. Furthermore, before deploying a WASABI digital assistant at the workplace, the end-users should inform workers' representatives and the affected workers that they will be subject to the use of a high-risk AI system. Finally, the end-users should also ensure that their workers have a sufficient level of AI literacy, such that they can safely use the WASABI digital assistants.

| **Obligations of providers (developers)** | **Obligations of deployers (end-users)** |
|---|---|
| Ensure compliance with the safety requirements stipulated in chapter III, section 2, of the AI Act. | Use the high-risk AI system according to the instructions for use. |
| Have a quality management system in place. | Monitor the operation of the high-risk AI system |
| Keep documentation and the logs automatically generated by the high-risk AI system. | Ensure human oversight |
| Inform the deployer in case of a lack of conformity of the high-risk system with the AI Act. | Suspend the use of the high-risk system if it presents too high of a risk. |

[80] Article 26 (9) AI Act.
[81] Article 3 (56) AI Act.

| | |
|---|---|
| Cooperate with the competent authorities. | Inform workers' representatives and affected workers that they will be subject to the use of a high-risk AI system. |
| | Ensure that the workers have a sufficient level of AI literacy. |

**Transparency obligations for limited-risk AI systems**

The WASABI digital assistants are conversational agents, intended to interact with workers in a manufacturing context. They are therefore subject to specific **transparency obligations**. According to Article 50 of the AI Act, providers must ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.[82] This information must be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure.[83] It is doubtful whether this transparency obligation applies to the WASABI digital assistants. Indeed, it will be rather obvious for the workers using the digital assistants that they are conversing with a chatbot, and not with a real person. Nevertheless, it is recommended that the WASABI chatbots clearly indicate their artificial nature to the workers. That way, compliance with the AI Act is assured.

Workers using the WASABI digital assistants should be made aware that they are conversing with an AI system. While this will be fairly obvious from the context of use, it is recommended that the digital assistants disclose their artificial nature to the workers at the time of the first interaction or exposure.

**Harmonized standards**

The obligations of deployers and providers of high-risk AI systems as stipulated in the AI Act are often rather vague. They will be further refined by standardization bodies. There are two recognized EU standardization organizations that are relevant for the AI Act: The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC).[84] These organizations create harmonized standards following a request from the EU Commission. If these organizations adopt standards relating to the AI Act, providers and deployers can follow these standards rather than interpreting the safety requirements as they are stipulated in the AI Act. **By following standards, providers and deployers enjoy a presumption of conformity with the AI Act**.[85]

The use of standards remains voluntary. Providers and deployers are free to interpret the obligations laid down in AI Act themselves. However, using standards is both cheaper and safer. It is the easiest way to demonstrate compliance with the law. Consequently, standards are not as voluntary as the EU Commission maintains. Therefore, some scholars claim that standardization is where the real rule-making in the AI Act will occur.[86]

[82] Article 50 (1) AI Act.
[83] Article 50 (4) AI Act.
[84] M. VEALE and F. Z. BORGESIUS, "Demystifying the Draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach", *CRi* 2021, (97) 104-105.
[85] Article 40 AI Act.
[86] M. VEALE and F. Z. BORGESIUS, "Demystifying the Draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach", *CRi* 2021, (97) 105.

An overview of the harmonized standards relating to AI that are currently under development can be found on the website of the European Committee for Standardization.[87]

**Entry into force and application**

The AI Act enters into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall start to apply 24 months after the date of entry into force.

**Key takeaways**

It is possible that the WASABI digital assistants qualify as high-risk AI systems within the meaning of the AI Act. If that is the case, they must comply with a series of **safety requirements**. These include: risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity. In order to ensure that these requirements are met, the AI Act imposes a number of obligations on providers and deployers of high-risk AI systems. In the context of WASABI, the developers of the digital assistants should comply with the obligations of providers, while the end-users should comply with the obligations of deployers. The easiest way to comply with these obligations is by following harmonized standards. High-risk AI systems that comply with harmonized standards enjoy a presumption of compliance with the safety requirements of the AI Act.

### 4.1.2 Proposal for an AI Liability Directive

If the developers and end-users of the WASABI digital assistants violate their obligations under the AI Act, they can be held liable if certain conditions are fulfilled. While fault liability is not harmonized by the EU, most Member States' legal regimes require **proof of three things in order to hold someone liable: fault, damage and causality**. First, fault refers to wrongful behavior. Most legal systems recognize two types of faults: negligence and the violation of a specific rule of conduct. A rule of conduct is a legal rule that either prescribes or prohibits certain behavior.[88] The obligations imposed by the AI Act on providers and deployers of high-risk AI systems are rules of conduct. Violating these obligations is therefore a fault. The second condition is relatively straightforward. If there is no damage, there is nothing to compensate. The third condition, however, is less evident. There must be a causal link between fault and damage. This means that the damage would not have occurred had the fault in question not been committed. In the context of WASABI, this means that the claimant will have to prove that his or her damage was caused by a lack of compliance with the AI Act on the part of the developer or the end-user of the digital assistants. For instance, the claimant may have to demonstrate that he or she would not have suffered harm if the developer of the WASABI digital assistants had taken appropriate data governance measures. This may be difficult to prove in practice. In order to alleviate the burden of proof for claimants when AI systems cause damage, the EU has recently adopted a proposal for an AI Liability Directive.

The **proposal for an EU AI Liability Directive** lays down uniform requirements for certain aspects of non-contractual civil liability for damage caused with the involvement of an AI system. Article 1 defines the scope of the AI Liability Directive. It stipulates two sets of rules. On the one hand, the AI Liability Directive lays down common rules on the **disclosure of evidence** on high-risk AI systems to enable a claimant to substantiate a non-contractual fault-based civil law claim for damages. These rules can be found in Article 3. On the other hand, the

[87] CEN - CEN/CLC/JTC 21 (cencenelec.eu).
[88] See, for instance, Article 6.6 §1 New Belgian Civil Code (NBCC).

AI Liability Directive creates common rules on the **burden of proof** in the case of non-contractual fault-based civil law claims brought before national courts for damages caused by an AI system. These rules are stipulated in Article 4.

According to Article 3 of the AI Liability Directive, a court may order the **disclosure of relevant evidence** about a specific high-risk AI system that is suspected of having caused damage. Either a claimant or a potential claimant can request the disclosure of evidence. A claimant is a person bringing a claim for damages.[89] A potential claimant is a person who is considering but has not yet brought a claim for damages.[90] Certain conditions have to be met before a court can order the disclosure of evidence. The potential claimant must present facts and evidence sufficient to support the plausibility of a claim for damages. The claimant, on the other hand, must merely undertake all proportionate attempts at gathering the relevant evidence from the defendant. Requests for evidence may be addressed to the provider of an AI system, a person subject to the provider's obligations or the deployer.[91]

A disclosure of evidence is a far-reaching measure. The AI Liability Directive contains several provisions aimed at ensuring proportionality and protecting the defendant's interests. For instance, national courts must limit the disclosure of evidence to what is necessary and proportionate to support a claim for damages.[92] In addition, the Directive contains a rebuttable presumption of non-compliance. Where a defendant fails to comply with an order by a national court in a claim for damages to disclose or to preserve evidence at its disposal, the court shall presume the defendant's non-compliance with a relevant duty of care. However, the defendant can rebut that presumption by submitting evidence to the contrary.[93]

Article 4 of the AI Liability Directive goes one step further than Article 3. It introduces a **rebuttable presumption of causality**. More precisely, according to Article 4(1), national courts shall presume the causal link between the fault of the defendant and the output produced by the AI system or the failure of the AI system to produce an output. However, this presumption only applies if three conditions are met.

(a) First, the claimant proves that the defendant has committed a fault according to applicable EU law or national rules. However, a fault can also be presumed by the court. This will be the case if the defendant fails to comply with a court order to disclose or preserve evidence;

(b) Second, it can be considered reasonably likely that the fault has influenced the output produced by the AI system or the failure of the AI system to produce an output;

(c) Third, the claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage.

According to Article 4(7), the defendant has a right to **rebut** the presumption of causality.

Article 4(1) applies to defendants in general. Articles 4(2) and 4(3), on the other hand, have a more specific scope of application. Article 4(2) applies to claims brought against the **provider** of a high-risk AI system or against a person subject to the provider's obligations under the AI Act. Article 4(3) applies to claims brought against the

[89] Article 2 (6) Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). Available: EUR-Lex - 52022PC0496 - EN - EUR-Lex (europa.eu).
[90] Article 2 (7) AI Liability Directive.
[91] Article 3 (1) AI Liability Directive.
[92] Article 3 (4) AI Liability Directive.
[93] Article 3 (5) AI Liability Directive.

**deployer** of a high-risk AI system. For these categories of defendants, the presumption of causality only applies when the fault consists of a **failure to comply with certain obligations imposed by the AI Act**. These obligations are listed in Article 4(2) and 4(3) of the AI Liability Directive.

According to Article 4(2), in the case of a claim for damages against a provider of a high-risk AI system, Article 4(1)(a) shall be met only where the claimant has demonstrated that the provider failed to comply with any of the following requirements of the AI Act:

(a) the AI system is a system which makes use of techniques involving the training of models with data and which was not developed on the basis of training, validation and testing **data sets that meet the quality criteria** referred to in Article 10 (2) to (4) of the AI Act;
(b) the AI system was not designed and developed in a way that meets the **transparency** requirements laid down in Article 13 of the AI Act;
(c) the AI system was not designed and developed in a way that allows for an **effective oversight** by natural persons during the period in which the AI system is in use pursuant to Article 14 of the AI Act;
(d) the AI system was not designed and developed so as to achieve, in the light of its intended purpose, an appropriate level of **accuracy, robustness and cybersecurity** pursuant to Article 15 of the AI Act; or
(e) the necessary **corrective actions** were not immediately taken to bring the AI system in conformity with the safety requirements laid down in Chapter III, section 2 of the AI Act or to withdraw or recall the system, as appropriate, pursuant to Article 16, point (j), and Article 20 of the AI Act.

According to Article 4(3), in the case of a claim for damages against a deployer of a high-risk AI system, Article 4(1)(a) shall be met where the claimant proves that the deployer:

(a) did not comply with its obligations to use or monitor the AI system in accordance with the accompanying instructions of use or, where appropriate, suspend or interrupt its use pursuant to Article 26(5) of the AI Act; or
(b) exposed the AI system to input data under its control which is not relevant in view of the system's intended purpose pursuant to Article 26(4) of the Act.

Article 4(4) contains an **exception** to the presumption of causality. This exception only applies to high-risk AI systems. If the defendant demonstrates that sufficient evidence and expertise is reasonably accessible for the claimant to prove the causal link, the court shall not apply the presumption of causality. This exception may induce defendants to comply with an order to disclose relevant evidence. In addition, it is an incentive to comply with the transparency and documenting obligations of the AI Act. Indeed, documentation and logging can provide the claimant with the necessary evidence and expertise. In such situations, the court should not apply the presumption of causality.[94]

In short, **if a WASABI digital assistant produces an output that causes harm**, and the developer or end-user of the assistant violated one of its obligations under the AI Act, national courts shall **presume the causal link** between this violation and the output of the digital assistant, if the claimant can prove three things. First, he or she needs to prove that the developer or end-user committed a fault. As mentioned, this condition will be met if the developer violated one of the obligations listed in Article 4(2) of the AI Liability Directive, and if the end-user violated one of the obligations listed in Article 4(3) of the AI Liability Directive. Second, the claimant has to prove that it can be considered reasonably likely that this violation has influenced the output of the WASABI digital assistant. For instance, if the developer of the assistant did not follow appropriate data management practices, it

[94] Recital 27 AI Liability Directive.

can be argued that it is reasonable that this has influenced the output of the digital assistant. Indeed, an AI system is only as good as its training data. If the training data are flawed, the AI system will not produce accurate outputs.[95] Third, the claimant has to prove that the output of the digital assistant caused damage. If these three conditions are met, causality will be presumed and the developer or end-user of the digital assistant will be held liable. Of course, the developer or end-user can rebut this presumption.

**Key takeaways**

The proposal for an AI Liability Directive increases the liability risk for the developers and end-users of the WASABI digital assistants. It does so by requiring a disclosure of evidence and introducing a rebuttable presumption of causality if certain conditions are met.

## 4.2 EU product liablity regime

Applying fault liability to AI can be challenging. Victims may need alternative grounds of tort liability to recover damage caused by AI systems. One such option is product liability. The product liability regime provides a layer of protection that national fault-based liability alone does not provide. **It introduces a system of strict liability of producers for damage caused by defects in their products.** The liability of the producer is strict because it is based on putting a defective product into circulation and not on committing wrongful acts. Four elements require particular attention in the context of WASABI. First, the question is whether software is a product. Second, the product must be defective. Third, the concept of 'producer' requires clarification in an AI context. Fourth, the defect needs to exist at the moment when the product is put into circulation.[96] Before discussing these four elements, we first give a brief overview of the applicable legislation.

The current EU product liability regime is laid down in the Directive on Liability for Defective Products (Product Liability Directive).[97] This Directive was adopted in 1985. The world has changed since then. The current EU product liability regime is not adapted to the digital age. That is why in September 2022, the EU Commission published a proposal to revise the Product Liability Directive.[98] The proposal introduces new provisions to address liability for products such as software (including AI systems) and digital services that affect how the product works (e.g. navigation services in autonomous vehicles). It also alleviates the burden of proof for victims under certain circumstances.[99] The EU Parliament and Council are currently working towards a compromise text. Because there is no agreement yet, we will discuss both the current and the revised Product Liability Directive in relation to the WASABI digital assistants.

---

[95] D. BERGSTROM and J. WEST, *Calling Bullshit: The Art of Skepticism in a Data-driven World*, New York, Random House, New York, 2021, 43 and 183.

[96] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 376-377.

[97] Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) (hereafter: Product Liability Directive). Available: Directive - 85/374 - EN - Product Liability Directive - EUR-Lex (europa.eu).

[98] For the most recent version of the proposal for a new Product Liability Directive, see: European Parliament legislative resolution of 12 March 2024 on the proposal for a directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD). Available: TA (europa.eu). Future references to the revised Product Liability Directive refer to this document.

[99] EUROPEAN PARLIAMENT, "New Product Liability Directive", *Briefing: EU Legislation in Progress* 2023, 1. Available: New Product Liability Directive (europa.eu).

### 4.2.1 The notion of 'product'

The Product Liability Directive only applies to **products**. It is unclear whether this includes software. There are two main arguments against qualifying software as a product. First, some consider software a service. Second, others argue that software is intangible.

The Product Liability Directive only applies to products, not services. However, the difference between products and services is not clear. In the Krone case, the European Court of Justice found that health advice in a newspaper is a service. Some scholars conclude from this decision that mere information is excluded from the scope of the Product Liability Directive. The question is whether the analogy can be drawn to software. Because software is a collection of instructions, one could argue that it qualifies as information. Consequently, it would be a service instead of a product. However, others argue that software is more than simply a piece of information. Software is essential to the functioning of many products and affects their safety. Therefore, it would make sense to include software in the scope of the Product Liability Directive.[100]

It is not because software is not a service that it is automatically a product. According to Article 2 of the Product Liability Directive, a 'product' means all movables, whether or not integrated into another movable or an immovable. This definition is rather vague. It is unclear whether 'movable' is restricted to tangible goods or whether it also includes intangible goods. The answer to this question differs from Member State to Member State. For instance, in Belgium, only tangible goods qualify as products. Intangible goods are excluded. This can be problematic for software. There is debate on whether software is tangible or intangible. The European Court of Justice has not yet ruled on the matter. Some scholars argue that software is part of our physical world and is therefore tangible.[101] However, nothing exists outside our physical world. As a result, there would no longer be a difference between tangible and intangible goods. Everything would become tangible. In principle, software is intangible because one cannot touch it. Consequently, software would be excluded from the scope of the Belgian product liability rules.

Scholars argue that it no longer makes sense to differentiate between tangible and intangible goods in the digital age. Software plays a necessary part in the functioning of certain products today, and it should therefore be considered part of such products.[102] Following a teleological interpretation of the Product Liability Directive, software could qualify as a product even if it is intangible.[103] After all, electricity is explicitly considered a product despite its intangible nature. The Product Liability Directive was originally designed to prevent and compensate for the rising safety risks resulting from industrial production and mass distribution of increasingly complex consumer goods.[104] If the purpose of the Product Liability Directive is to protect consumers against complex technology, then excluding software is difficult to justify. Personal computers were not commercially widespread

[100] E. VAN GOOL, "Case C-65/20 Krone: Offering (some) clarity relating to product liability, information and software", *European Law Blog* 2022. Available: Case C-65/20 Krone: Offering (some) clarity relating to product liability, information and software – European Law Blog; J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 377.

[101] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 378-379.

[102] T. S. CABRAL, "Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive", *Maastricht Journal of European and Comparative Law* 2020, (615) 619; EUROPEAN PARLIAMENT, "New Product Liability Directive", *Briefing: EU Legislation in Progress* 2023, 9. Available: New Product Liability Directive (europa.eu).

[103] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 379.

[104] E. VAN GOOL, "Case C-65/20 Krone: Offering (some) clarity relating to product liability, information and software", *European Law Blog* 2022. Available: Case C-65/20 Krone: Offering (some) clarity relating to product liability, information and software – European Law Blog.

when the Product Liability Directive was adopted in the early 80s. Legislators simply did not think to include software in the definition of a product. But the world has changed since then. Today, the software is a commercial product, just like any other product that may entail risks for users and third parties. Including it in the Product Liability Directive would reflect the current economic reality.[105]

As it turns out, EU policymakers hold the same view. **The revised Product Liability Directive explicitly includes software in its definition of a product**.[106] According to Recital 12, software is a product for the purposes of applying no-fault liability, irrespective of the mode of its supply or usage, and therefore, irrespective of whether the software is stored on a device, accessed through cloud technologies, or supplied through a software-as-a-service model. However, information is not a product. The content of digital files, such as the mere source code of software, is therefore excluded. Recital 13 states that the Directive does not apply to free and open-source software developed or supplied outside the course of a commercial activity. However, where software is supplied in exchange for a price or personal data is provided in the course of a commercial activity (*i.e.* for purposes other than exclusively improving the security, compatibility, or interoperability of the software), the revised Product Liability Directive should apply.

The WASABI digital assistants are software and thus qualify as 'products'. As a result, the revised EU Product Liability Directive applies.

### 4.2.2 The notion of 'defect'

Liability under the Product Liability Directive requires a **defect** in the product. A product is defective if it is unsafe.[107] The safety of a product is determined based on the so-called 'consumer-expectations test'. A product is defective if it does not provide the safety that the public at large is entitled to expect, taking all circumstances into account.[108] This is a normative evaluation. The question is not what expectations consumers actually have, but what expectations they are legitimately entitled to have.[109] The revised Product Liability Directive defines the notion of defect similarly to the currently applicable Directive. However, it adds that a product shall be considered defective if it does not provide the safety that is required under EU or national law.[110]

The **consumer expectations** test is carried out on a case-by-case basis. The current Product Liability Directive contains a non-exhaustive list of considerations that must be taken into account. These include the presentation of the product, the instructions for use, the reasonably foreseeable use of the product and the moment the product was put into circulation.[111] The revised Directive expands this list to address the risks of inter-connected products and AI.[112] It now also includes the reasonably foreseeable effect on the product of other products that can be expected to be used together with the product, the ability of the product to continue to learn after it is placed on the market, and the level of cybersecurity of the product.[113] These considerations are particularly

[105] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 379.
[106] Article 4 (1) revised Product Liability Directive.
[107] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 568.
[108] Article 6 (1) Product Liability Directive.
[109] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 380-381.
[110] Article 7 (1) revised Product Liability Directive.
[111] Article 6 (1) Product Liability Directive.
[112] Recital (23) revised Product Liability Directive.
[113] Article 7 (2) (c), (d) and (f) revised Product Liability Directive.

relevant for the WASABI digital assistants. Furthermore, due consideration should be given to the needs of the group of users for whom the product is intended.[114] Some products entail an especially high risk of damage to people and therefore give rise to particularly high safety expectations.[115] Finally, compliance with product safety requirements is also relevant in the assessment of whether a product is defective.[116] It is therefore important that the **WASABI digital assistants comply with the safety requirements of the AI Act**. Otherwise, they could be considered defective under the Product Liability Directive.

In order not to be considered defective, the WASABI digital assistants should comply with product safety requirements, such as the safety requirements stipulated in the AI Act.

Despite all these clarifications, the consumer-expectations test remains vague. Judges therefore have a wide margin of appreciation.[117] This flexibility is often used to the benefit of the victim. In practice, courts sometimes hold the defendant liable, even if it is not proven that the product in question is defective.[118] The consumer-expectations test is therefore **victim-friendly**. It gives courts the freedom to demand a high level of safety, thereby allowing victims to get compensation for their damages.[119]

Because the consumer-expectations test is so vague, there are two obstacles in applying it to AI. First, it is unclear when an AI system can be considered defective. Second, it can be difficult to prove both defect and causality.

While it remains to be seen how judges will apply the consumer-expectations test to AI, product liability law has several tools at its disposal that can help judges in their assessment. First, as mentioned, a product is defective if it is unsafe. The safety of an AI system depends to a large extent on its accuracy. The more accurate a system's predictions are, the safer it is. Therefore, one could argue that an AI system is defective if it falls below a certain threshold of accuracy. This threshold will be determined by the consumer-expectations test. An AI system should reach the level of accuracy that the public at large is entitled to expect. In practice, much will depend on what the AI system is used for. Safety expectations will be very high in high-risk contexts.[120] One such context is manufacturing. Indeed, as we have seen, the WASABI digital assistants are a safety component of machinery. If they malfunction, they could endanger people's safety. For example, if the onboarding assistant is not sufficiently accurate, new workers may not be adequately trained to operate potentially dangerous machinery. It is therefore reasonable to expect that the WASABI digital assistants achieve a high level of accuracy.

**A complication in the context of WASABI is that the digital assistants make predictions, but also provide human-made content in the form of learning material**. This content will be provided by the end-user or a third party. It is therefore possible that the assistant makes accurate predictions, but that the content is wrong. The question rises who can be held liable in this case.

[114] Article 7 (2) (h) revised Product Liability Directive.
[115] Recital (30) revised Product Liability Directive.
[116] Article 7 (2) (f) revised Product Liability Directive.
[117] T. VANSWEEVELT and B. WEYTS, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, Antwerp, Intersentia, 2009, 515.
[118] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 562-568.
[119] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 572.
[120] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 381.

It is possible that the third-party content qualifies as a 'component' of the digital assistants. A 'component' means any item, whether tangible or intangible, or raw material or any related service, that is integrated into, or inter-connected with, a product.[121] This notion is very broad. It is therefore likely that third-party content, such as learning material, falls under its scope. If damage is caused by a defective component of a product, the manufacturer of the product can be held liable. However, there is one precondition: the component must be within the manufacturer's control.[122] A component is within the manufacturer's control if it is integrated into, or inter-connected with, a product, or supplied by the manufacturer or where the manufacturer authorizes or consents to its integration, inter-connection or supply by a third party.[123] In the context of WASABI, the developer of the digital assistant authorizes the integration of the learning material by third parties into the assistant. The learning material is therefore within the control of the developer of the digital assistant. Thus, if damage is caused by such third-party content, the developer of the assistant can be held liable. In addition, the third-party or end-user who supplied the learning material can also be held liable as the manufacturer of a defective component.[124] In short, the developer and the end-user or third party will be held jointly and severally liable.[125] This means that the claimant can ask for full compensation of the damage from either party. Of course, the party that has provided compensation has a right of recourse against the other liable party.[126]

Another way to assess the safety of an AI system is the **risk-utility test**. If the benefits of increasing the accuracy of an AI system outweigh the costs, then the system can be considered defective. The question is whether the producer should have taken more precautions to avoid the damage.[127] One advantage of the risk-utility test over the consumer-expectations test is its precision. It gives judges a useful tool to evaluate the defectiveness of a product by comparing the costs and benefits of increasing safety. However, the EU product liability framework is a regime of strict liability. The liability of the producer does not depend on negligence. It only depends on placing a defective product on the market. That is why most scholars agree that the risk-utility test has no place in EU product liability law. However, a minority of authors argues that the risk-utility test can complement the consumer-expectations test. They emphasize that EU Member States' courts already apply variations of the risk-utility test in practice.[128] We should therefore recognise that it is part of the EU product liability framework. The risk-utility test is indeed a useful tool in assessing the defectiveness of a product. Because AI is such a complex and opaque technology, we should use every tool at our disposal to help victims get compensation for their damages.

A specific application of the risk-utility test is the '**reasonable design alternative**' test. This test can be found in the US Third Products Liability Restatement.[129] The question is whether the foreseeable risk of harm posed by the product could have been avoided if the product had an alternative, safer, design. In practice, this means comparing the AI system that caused damage to a functionally comparable reference AI system placed in the same

[121] Article 4(4) revised Product Liability Directive.
[122] Article 8(1) revised Product Liability Directive.
[123] Article 4(5) and Recital 18 revised Product Liability Directive.
[124] Article 8(1)(b) revised Product Liability Directive.
[125] Article 12(1) revised Product Liability Directive.
[126] Article 14 revised Product Liability Directive.
[127] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 633-634.
[128] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 633.
[129] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 628.

circumstances.[130] One advantage of determining an AI system's safety on the basis of its accuracy is that accuracy can be measured. Measures allow for making objective comparisons. Computer scientists use a wide variety of accuracy metrics to evaluate the performance of their AI models. For example, the test error of a model reflects the difference between the model and reality. It is therefore a good indication of how the model will perform in practice. Judges can apply the 'reasonable design alternative' criterion to AI by comparing the test error of different AI systems. For instance, suppose that the AI system that caused damage has a test error of 20%. If there are similar AI systems on the market that only have a test error of 10%, it could be argued that there was a reasonable alternative design that could have avoided the damage. However, it is not because a better AI system is available on the market that all other AI systems are automatically defective.[131] Judges must therefore be careful in applying this test. Nevertheless, looking at the accuracy of reference AI systems can help judges determine the level of safety that consumers are entitled to expect.

The Product Liability Directive places the **burden of proof on the claimant**. He or she must prove the defectiveness of the product, the damage suffered and the causal link between defect and damage.[132] This can be difficult in practice. Product liability is characterised by an inequality between parties. The manufacturer knows the intricate details of his product, while the victim might not even know the product exists.[133] This information asymmetry is even more prevalent in the context of AI. The average person has no idea how AI works. Claimants will therefore often lack the necessary expertise and evidence to prove that an AI system is defective. In order to balance the scale, courts have systematically lowered the standard of proof for claimants.[134] Moreover, the revised Product Liability Directive requires the disclosure of evidence and establishes a presumption of defect and/or causality under certain conditions.

Against the wording of the Product Liability Directive, both Member States' courts and the European Court of Justice have **systematically lowered the standard of proof for the claimant**. For instance, judges sometimes accept that a product is defective if it causes harm under normal use.[135] As a result, the claimant does not have to demonstrate precisely how the product is defective. In other words, direct proof of a defect is not always required. Indirect proof can be sufficient. In the US, this is called the 'malfunction doctrine'.[136] This doctrine can be particularly helpful when damage is caused by AI. Because claimants lack the necessary expertise and evidence, it can be very challenging to prove how an AI system is defective. Under the malfunction doctrine, however, the claimant only has to prove that the AI system malfunctioned under normal use. If, for instance, a WASABI digital assistant makes a wrong prediction which causes damage, courts could decide to hold the developer liable without requiring further proof of what exactly is wrong with the digital assistant. The assistant malfunctioned and is therefore unsafe.[137] That is sufficient to hold the developer liable.

---

[130] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 383.

[131] Article 7 (3) revised Product Liability Directive.

[132] Article 4 Product Liability Directive

[133] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 562.

[134] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 562.

[135] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 565.

[136] C. BEGLINGER, "A broken Theory: The Malfunction Theory of Strict Products Liability and the Need for a new Doctrine in the Field of Surgical Robotics Note", *Minnesota Law Review* 2019, (1041) 1053-1057.

[137] T. VERHEYEN, *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 562.

Claimants are further aided by article 9 of the revised Product Liability Directive. Article 9 allows Member States' courts to require the defendant to **disclose relevant evidence** to the claimant. The latter must, however, present facts and evidence sufficient to support the plausibility of the claim for compensation.[138] This provision will be particularly relevant when damage is caused by AI. Claimants will often lack access to the information necessary to prove defect. For instance, an important piece of evidence is the training data of an AI system. An AI system is only as good as the data it is trained on. If the data set is flawed, the system will not be accurate. Having access to the data set can therefore help claimants build a case against the defendant. In addition, as mentioned, the test error of an AI system is a measure of its safety. This information will therefore also likely qualify as 'relevant evidence'. However, the defendant is not left without protection. The disclosure of evidence should be limited to what is necessary and proportionate.[139] In particular, due consideration must be given to the protection of trade secrets. It is likely that an AI system's training set is a trade secret. In order to protect the interests of the defendant, the court may take specific measures to preserve the confidentiality of information that is a trade secret when it is used or referred to in the course of the legal proceedings.[140]

Article 10 of the revised Product Liability Directive goes one step further. It contains two presumptions, one of the **product's defectiveness and one of causality between defect and damage**. Of course, the defendant has a right to rebut any of these presumptions.[141]

First, according to article 10 (2), the **defectiveness of the product shall be presumed** if any of the following conditions are met:

(a) The defendant failed to disclose relevant evidence pursuant to Article 9 of the revised Product Liability Directive;
(b) The claimant demonstrates that the product does not comply with mandatory safety requirements set in EU or national law; or
(c) The claimant demonstrates that the damage was caused by an obvious malfunction of the product during reasonably foreseeable use or under ordinary circumstances.

The last condition is almost an exact articulation of the malfunction doctrine. The meaning of 'obvious malfunction', 'reasonably foreseeable use' and 'ordinary circumstances' will have to be clarified and further refined by judges and/or policymakers. Especially relevant in the context of WASABI, however, is condition (b). **If the WASABI digital assistants do not comply with the safety requirements of the AI Act, they will be presumed to be defective**.

Second, article 10 (3) introduces a **presumption of causality**. The causal link between the defectiveness of the product and the damage shall be presumed, where it has been established that the product is defective and the damage caused is of a kind typically consistent with the defect in question.

Lastly, article 10 (4) contains a more general presumption. A national court shall presume the defectiveness of the product or the causal link between its defectiveness and the damage, or both, where:

[138] Article 9 (1) revised Product Liability Directive.
[139] Article 9 (3) revised Product Liability Directive.
[140] Article 9 (4) and (5) revised Product Liability Directive.
[141] Article 10 (5) revised Product Liability Directive.

(a) the claimant faces excessive difficulties, in particular due to technical or scientific complexity, to prove the defectiveness of the product or the causal link between its defectiveness and the damage, or both; and
(b) the claimant demonstrates that it is likely that the product is defective or that there is a causal link between the defectiveness and the damage, or both.

'Technical or scientific complexity' should be determined by national courts on a case-by-case basis, taking into account various factors. Those factors include, among others, the complex nature of the technology used, such as **machine learning.** Another factor that should be taken into account is the complex nature of the causal link, such as a link that, in order to be proven, would require the claimant to explain the inner workings of an AI system. While a claimant should provide arguments to demonstrate excessive difficulties, proof of such difficulties should not be required. For example, in a claim concerning an AI system, the claimant should, for the court to decide that excessive difficulties exist, neither be required to explain the AI system's specific characteristics nor how these characteristics make it harder to establish the causal link.[142]

**If a WASABI digital assistant causes damage, it is likely that a judge will presume both defectiveness and causality in accordance with article 10 (4) of the revised Product Liability Directive**. Indeed, because the digital assistant is a machine learning algorithm, the claimant will probably be successful in arguing that he or she faces excessive difficulties in proving both defectiveness and causality due to the technical complexity of the digital assistant. Consequently, the claimant will only need to prove that it is likely that the digital assistant is defective and that there is a causal link between defect and damage.[143] In order to prove this, it may be sufficient to simply demonstrate that the digital assistant made a wrong prediction which caused harm. In other words, judges no longer have to rely on the controversial malfunction doctrine to help claimants get compensation. The revised Product Liability Directive now provides an explicit legal basis for them to do so.

According to the revised Product Liability Directive, if the WASABI digital assistants do not comply with the safety requirements imposed by the AI Act on high-risk systems, they will be presumed to be defective if they cause damage. In addition, because of the technical complexity of the WASABI digital assistants, both their defectiveness and the causal link between their defectiveness and the damage will be presumed.

### 4.2.3 The notions of 'producer' and 'manufacturer'

Under the current Product Liability Directive, liability rests with the **producer** of the product. A producer is the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part, and any person who presents himself as its producer by putting his name, trademark, or other distinguishing feature on the product.[144] Furthermore, the term 'producer' also includes any person who imports a product into the EU for sale, hire, lease or any form of distribution during his or her business.[145] If the producer (or importer) cannot be identified, each product supplier will bear this liability unless he or she informs the victim within a reasonable time of the identity of the producer (or importer) or of the person who supplied him or her with the product.[146]

[142] Recital 48 revised Product Liability Directive.
[143] Of course, as mentioned, if the digital assistant does not comply with the safety requirements high-risk systems stipulated in the AI Act, the defectiveness of the assistant will be presumed. See Article 10 (2) (b) revised Product Liability Directive.
[144] Article 3 (1) Product Liability Directive.
[145] Article 3 (2) Product Liability Directive.
[146] Article 3 (3) Product Liability Directive.

The revised Product Liability Directive expands the list of potentially liable persons. Instead of using the term 'producer', the new Directive relies on the notion of 'economic operator'. The term 'economic operator' means the manufacturer of a product or component, the provider of a related service, the authorised representative, the importer, the fulfilment service provider, the distributor, or the provider of an online platform allowing consumers to conclude distance contracts with traders.[147]

The revised Product Liability Directive introduces a layered approach to liability. The manufacturer is liable for damage caused by a defect in his or her product or components.[148] If the manufacturer is established outside the EU, the revised Product Liability Directive attributes liability to the importer and the authorised representative in the EU. As a last resort, the fulfilment service provider (offering at least two of: warehousing, packaging, addressing and dispatching of a product, without having ownership of the product), will be held liable when there is no importer or authorised representative established within the EU.[149] In addition, distributors of a defective product (offline and online sellers) can also be held liable upon request by a claimant and when the distributor fails to identify any of the above economic operators.[150] Online platforms should be liable in respect of a defective product on the same terms as such economic operators when performing the role of manufacturer, importer or distributor.[151]

In sum, the term 'economic operator' is very broad. The goal is to make sure that at least one person involved in the product supply chain can be held liable. This gives victims the biggest possible chance to get compensation. Moreover, if two or more economic operators are liable for the same damage, the victim can claim full compensation from any one of them.[152] This ensures maximum consumer protection.

Manufacturers are first in line in the liability chain. A 'manufacturer' is any natural or legal person who develops, manufactures or produces a product or has a product designed or manufactured, or who, by putting its name, trademark or other distinguishing features on that product, presents itself as its manufacturer, or who develops, manufactures or produces a product for its own use.[153] **In the context of WASABI, those who develop the digital assistants will qualify as their 'manufacturers'**. Consequently, if a digital assistant is defective and causes harm, its developer can be held liable under the revised Product Liability Directive. In addition, any entity that supplies a 'component' to the assistant, will qualify as the manufacturer of this component. If this component is defective and causes damage, both the manufacturer of the assistant as a whole and the manufacturer of the component can be held liable. However, this is under the precondition that the component was integrated into the assistant with the main manufacturer's consent.[154]

The developers of the WASABI digital assistants qualify as manufacturers under the revised Product Liability Directive. They can therefore be held liable if the assistants are defective and cause damage.

[147] Article 4 (15) revised Product Liability Directive.
[148] Article 8 (1) (a) and (b) revised Product Liability Directive.
[149] Article 8 (1) (c) revised Product Liability Directive.
[150] Article 8 (3) revised Product Liability Directive.
[151] Article 8 (4) revised Product Liability Directive; EUROPEAN PARLIAMENT, "New Product Liability Directive", *Briefing: EU Legislation in Progress* 2023, 5. Available: New Product Liability Directive (europa.eu).
[152] Article 12 (1) revised Product Liability Directive.
[153] Article 4 (10) (b) revised Product Liability Directive.
[154] Article 8(1) revised Product Liability Directive.

### 4.2.4 The defenses of the producer/manufacturer

The manufacturer is liable if the claimant proves damage, defect, and causality.[155] However, the Product Liability Directive contains several exemptions from liability. For instance, manufacturers are not liable for damage caused by defects that did not exist when the product was placed on the market or put into service.[156] Whatever happens to the product after that moment is out of the manufacturer's control. This defense, however, can be problematic in the context of AI. Digital technologies allow manufacturers to exercise control beyond the moment of placing the product on the market.[157] That is why the revised Product Liability Directive limits this liability exemption in several ways. A manufacturer will not escape liability if the defectiveness of the product is due to any of the following, provided that it is within the manufacturer's control:

(a) a related service;

(b) software, including software updates or upgrades;

(c) the lack of software updates or upgrades necessary to maintain safety; or

(d) a substantial modification.[158]

Such software, related services or modifications should be considered within the manufacturer's control where they are supplied by that manufacturer or where that manufacturer authorises them or otherwise consents to their supply by a third party.[159]

In the context of WASABI, a digital assistant has a number of skills. It is possible that a new skill is added to the assistant by the end-user or a third-party, after the assistant is placed on the market. **If this new skill is defective and causes damage, the question is whether the developer (manufacturer) of the assistant can be held liable**. In principle, the developer is exempt from liability because the defect came into being after the assistant was placed on the market. However, the developer cannot invoke this liability exemption if the defectiveness is due to software, such as skills, which is within the developer's control. This is the case if the developer authorizes or consents to the integration of the skill by the end-user or a third-party.[160] However, the developer of the digital assistant should not be considered to have consented to the integration of a skill, merely by providing for the technical possibility of integration. An important question in the context of WASABI will thus be whether or not the developers of the digital assistants exercise control over the skills added by end-users or third-parties. The answer to this question determines whether the developers can be held liable for damage caused by a defective skill integrated into the assistant after the assistant was placed on the market.

Another liability exemption that may be relevant in the context of AI is the development risk defense. Manufacturers should not be liable if the state of scientific and technical knowledge did not allow them to discover the defect.[161] Judges interpret this exemption in a very restrictive way. What matters is the most advanced level of objective knowledge accessible, not the actual knowledge of the manufacturer in question. However, the relevant

[155] Article 4 Product Liability directive and Article 10 (1) revised Product Liability Directive.
[156] Article 11 (1) (c) revised Product Liability Directive.
[157] Recital 50 revised Product Liability Directive.
[158] Article 11 (2) revised Product Liability Directive.
[159] Recital 50 revised Product Liability Directive.
[160] Article 4(5) revised Product Liability Directive.
[161] Article 11 (1) (e) revised Product Liability Directive.

scientific and technical knowledge must have been accessible at the time when the product was put into service.[162]

The development risk defense is assessed over the period when the product is within the manufacturer's control. Suppose a defective product is placed on the market, but that science is not advanced enough to notice something wrong. Over time, however, our scientific knowledge progresses. It might become possible to discover the defect within a couple of years. If the product is still within the manufacturer's control at that moment, he or she will not be able to escape liability by invoking the development risk defense. This is particularly relevant in the context of AI. An AI system remains within the control of its manufacturer as long as the latter as the ability to supply software updates or upgrades.[163] The manufacturer must stay in touch with the latest scientific and technical developments during this period.

Technologies such as the WASABI digital assistants allow manufacturers to exercise control beyond the moment of placing the product on the market. It will therefore be difficult for the developers of the digital assistants to rely on some of the defenses against liability listed in Article 10 of the revised Product Liability Directive.

**Key takeaways**

The WASABI digital assistants qualify as 'products' within the meaning of the revised Product Liability Directive, while the developers of the digital assistants qualify as 'manufacturers' under this Directive. The developers can therefore be held liable if the digital assistants are defective and cause damage to natural persons. Because of the technical complexity of the digital assistants, both defectiveness and causality will likely be presumed. In any case, if the digital assistants do not comply with the safety requirements for high-risk AI systems imposed by the AI Act, they are presumed to be defective. Finally, because the developers may be able to exercise control over the digital assistants after they are placed on the market, their defenses against liability are limited.

## 4.3 General Data Protection Regulation

According to Article 82 of the General Data Protection Regulation (GDPR), any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered. In addition, violating the GDPR can give rise to administrative fines and penalties.[164] Compliance with the GDPR is therefore important in the context of WASABI.

This part gives an overview of the provisions of the GDPR which are the most relevant in the context of WASABI. In the next paragraphs, we will discuss the scope of application of the GDPR, the principles relating to the processing of personal data, special categories of personal data, the rights of data subjects, the obligations of data controllers and processors, and the requirements of carrying out a data protection impact assessment and appointing a data protection officer. In addition, we will briefly consider the special case of processing personal data for the

[162] J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems" in J. DE BRUYNE and C. VANLEENHOVE (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, (359) 387-388.

[163] Article 4 (5) (b) revised Product Liability Directive.

[164] Article 83 and 84 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available: Regulation - 2016/679 - EN - gdpr - EUR-Lex (europa.eu). (Hereafter : GDPR).

purposes of scientific research. Finally, we will discuss liability for damage as a result of an infringement of the GDPR.

**Scope of application**

The GDPR lays down rules relating to the protection of **natural persons** with regard to the processing of personal data.[165] It applies to the **processing of personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[166] The territorial scope of the GDPR is limited. It only applies to the processing of personal data in the context of the **activities of an establishment of a controller or a processor in the EU**, regardless of whether the processing takes place in the EU or not.[167]

The GDPR applies to the **processing of personal data**. **The terms 'personal data' and 'processing' are defined very broadly**. 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[168] 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[169]

The GDPR imposes obligations on **data controllers and processors**. A '**controller'** is the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**.[170] A '**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[171]

There are several reasons why the GDPR applies in the context of WASABI. First, **training the digital assistants inevitably requires processing personal data**. As mentioned, the term 'processing' is extremely broad. It refers to any operation which is performed on personal data. It therefore also includes training a machine learning model. In addition, it is very likely that the training data sets of the WASABI digital assistants contain 'personal data', since this notion is also very broad. It includes any piece of information that relates to an individual. This means that this piece of information could be used, either individually or in combination with other pieces of information, to identify an individual.[172] For example, in WASABI, the onboarding assistant is trained on data relating to workers. This data could be used to re-identify individual workers in the data set, and qualifies therefore as 'personal data'. Second, conversations between workers and the digital assistants will be stored for as long as necessary to continue a specific conversation. Such conversations also qualify as personal data. Indeed, each utterance of a worker to the assistant may contain personal information and the conversation as a whole

[165] Article 1 (1) GDPR.
[166] Article 2 (1) GDPR.
[167] Article 3 (1) GDPR.
[168] Article 4 (1) GDPR.
[169] Article 4 (2) GDPR.
[170] Article 4 (7) GDPR.
[171] Article 4 (8) GDPR.
[172] EUROPEAN DATA PROTECTION SUPERVISOR, "AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation", 2021. Available: 21-04-27_aepd-edps_anonymisation_en_5.pdf (europa.eu).

can be used to identify the worker. Third, **personal data will also be processed when testing the WASABI digital assistants**. For instance, as part of providing AI-enhanced training to workers in manufacturing, the WASABI consortium shall collect workers' primary information with which the WASABI partners will evaluate the AI services.[173] Finally, the digital assistants benefit from a continuous feedback loop.[174] Therefore, **when deploying the digital assistants, end-users will collect workers' personal data to improve the training data of the assistants**. Indeed, creating successful skills requires a continuous improvement of the training data.[175] This is only possible by collecting new personal data during deployment of the WASABI digital assistants.

In the context of WASABI, the developers and end-users of the digital assistants should comply with the GDPR every time they qualify as the 'controller' or 'processor' of a processing activity. For instance, the **developers of the WASABI digital assistants will likely qualify as 'controllers'** when training the digital assistants. Indeed, the developers collect personal data to train machine learning models, and therefore determine the purpose and means of this processing activity. The **end-users will also qualify as 'controllers'** when training the assistants, since the end-users are often involved in designing training data. In addition, end-users will deploy the WASABI digital assistants in their factories, and collect data relating to their workers. Specifically, end-users will store workers' conversations with the digital assistants for as long as necessary to continue a conversation. For this processing operation, the end-users will qualify as 'controllers', since they determine the purpose of the data collection. However, during the testing phase of the WASABI digital assistants, the end-users may collect workers' data under the instructions of the developers of the assistants. For this processing operation, it is possible that **the end-users qualify as 'processors'** instead of 'controllers'. However, if the end-users determine which data is collected together with the developers, they will be joint controllers.

The WASABI project involves processing of personal data. Each time personal data is processed, it must be determined who qualifies as the 'controller' and/or 'processor' of that processing operation. This person will then be required to comply with the GDPR. For example, training the WASABI digital assistants requires processing of personal data. The developers of the digital assistants qualify as 'controllers' of this processing operation. They should therefore comply with the obligations of controllers stipulated in the GDPR. Most importantly, the end-users qualify as 'controllers' when processing conversations between workers and the digital assistants. Each utterance of a worker to the assistant may contain personal information and the conversation as a whole can be used to identify the worker. In addition, during the testing phase, it is possible that end-users collect personal data on behalf of the developers of the WASABI digital assistants. If that is the case, then the end-users qualify as 'processors'. However, if the end-users determine which data is collected together with the developers, they will be joint controllers. In short, depending on the processing activity, the end-users should comply with the obligations of 'controllers' or 'processors' imposed by the GDPR.

**Data protection principles**

Personal data must be processed in accordance with a number of key principles: **lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability**. These principles are stipulated in Article 5 GDPR. According to this provision, personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

[173] WASABI proposal, 183.
[174] WASABI proposal, 150.
[175] WASABI proposal, 144 and 169.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR, not be considered to be incompatible with the initial purposes ('purpose limitation');
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');
(d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation');
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with the these principles ('accountability').[176]

The principle of '**lawfulness'** requires further clarification. According to **Article 6 GDPR**, processing of personal data is only lawful if at least one of the following legal grounds applies:

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;
(d) processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[177]

[176] Article 5 (2) GDPR.
[177] Article 6 (1) GDPR.

In the context of WASABI, 'consent' will be the most relevant legal basis for data processing. Indeed, before conducting training activities with workers, the WASABI consortium partners will ask participants' consent via an informed consent form.[178] In order to qualify as 'consent' within the meaning of the GDPR, participants must give a free, specific, informed and unambiguous indication of their wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.[179]

**If processing is based on consent, the controller must fulfil a number of conditions**. First, the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.[180] Second, if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of the GDPR shall not be binding.[181] Third, the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.[182] Last, when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[183]

It is possible that controllers lawfully collect personal data for one purpose, but afterward, want to **process it for another purpose**. This is only allowed if certain conditions are met. According to Article 6 (4) GDPR, where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a EU or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) GDPR, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 GDPR, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10 GDPR;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymization

**Special categories of personal data**

Additional safeguards apply when **special categories of personal data** are processed. In principle, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union

[178] WASABI proposal, 184.
[179] Article 4 (11) GDPR.
[180] Article 7 (1) GDPR
[181] Article 7 (2) GDPR.
[182] Article 7 (3) GDPR.
[183] Article 7 (4) GDPR.

membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be **prohibited**.[184] However, processing of these categories of data is allowed if one the conditions listed in Article 9(2) GDPR is met.

For the WASABI project, the most relevant legal basis for processing special category personal data is **explicit consent**. Indeed, it is allowed to process special category personal data if the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.[185] The difference between 'consent' and 'explicit consent' is unclear. In principle, an informed consent form should be sufficient to amount to 'explicit consent'. However, ticking a box may not be enough. Instead, it could be required for the data subject to explicitly write "hereby, I am consenting to…" on the informed consent form.

**It is possible that special category personal data will be processed in the WASABI project**. For instance, WASABI uses voice-enabled digital assistants. This technology uses Automated Speech Recognition (ASR) in two cases. First, it processes audio signals continuously to identify the so-called wake word. This operation takes place in the Android App on the user's mobile device. Second, it transcribes human utterances. The current App version uses Google's Speech-to-Text service available on most Android mobile devices. It communicates with a Google server via the Internet to process the audio and return the transcript. This raises data protection issues. Organizations could process the audio signal to recognize biometric information, such as an individual's voice.[186] Under the GDPR, biometric data is special category data.[187] In order to process this data, it is necessary to obtain data subjects' explicit consent.

It can, however, also be argued that **no special category data is processed** when deploying the digital assistants. Even though the digital assistants process audio continuously to recognize keywords, no audio is stored and no biometric markers are extracted. In addition, the digital assistants do not have the capability of uniquely identifying workers based on their voice.[188] Since biometric data is not processed for the purpose of uniquely identifying a natural person, it can be argued that deploying the WASABI digital assistants does not involve processing special category data within the meaning of Article 9(1) GDPR.

While the WASABI digital assistants process audio signals continuously to recognize wake words, they do not store audio data, nor do they extract biometric markers. In addition, the digital assistants cannot identify workers based on their voice. Since biometric data is not processed for the purpose of uniquely identifying a natural person, it can be argued that deploying the WASABI digital assistants does not involve processing of special category data within the meaning of Article 9(1) GDPR.

**Rights of the data subjects**

The GDPR gives data subjects a number of **rights**. They include: a right to information, a right to access, a right to rectification, a right to erasure, a right to restriction of processing, a right to data portability, a right to object and a right not to be subject to automated decision-making. The purpose of these rights is to ensure that the data

[184] Article 9 (1) GDPR.
[185] Article 9 (2) (a) GDPR.
[186] WASABI, proposal, 183.
[187] According to Article 4 (14) GDPR, 'biometric data' refers to personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
[188] European Data Protection Board (EDPB), *Guidelines 02/2021 on virtual voice assistants*, version 2.0, 2021, 30.

protection principles laid down in Article 5 GDPR are respected. The rights of data subjects are contained in Articles 12-22 GDPR. The next paragraphs will go over these provisions, one by one.

Article 12 GDPR stipulates the **modalities for the exercise of the rights of data subjects**. It stipulates the rules controllers must adhere to when communicating with data subjects. In short, controllers must communicate with data subjects in a clear and plain language. Communication must happen in writing or, at the request of the data subject, orally. Furthermore, controllers may use standardized icons in their communication with data subjects. Lastly, the controller must provide information to the data subject free of charge. The next paragraphs contain a detailed exposition of these modalities.

First, the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 GDPR, and any communication under Articles 15 to 22 and 34 GDPR relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.[189]

Furthermore, the controller shall facilitate the exercise of data subject rights under Articles 15 to 22 GDPR.[190] The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.[191] If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.[192]

Information provided under Articles 13 and 14 GDPR and any communication and any actions taken under Articles 15 to 22 and 34 GDPR shall be provided free of charge.[193] Lastly, the information to be provided to data subjects pursuant to Articles 13 and 14 GDPR may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.[194]

Article 13 GDPR gives data subjects a **right to information**. Where personal data relating to a data subject **are collected from the data subject**, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

[189] Article 12 (1) GDPR.
[190] Article 12 (2) GDPR.
[191] Article 12 (3) GDPR.
[192] Article 12 (4) GDPR.
[193] Article 12 (5) GDPR.
[194] Article 12 (7) GDPR.

(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1) GDPR, the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47 GDPR, or the second subparagraph of Article 49(1) GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.[195]

In addition to the aforementioned information, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) GDPR or point (a) of Article 9(2) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[196]

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in Article 13 (2) GDPR.[197]

Article 14 GDPR contains a right to information **were personal data have not been obtained from the data subjects**. In this case, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

[195] Article 13 (1) GDPR.
[196] Article 13 (2) GDPR.
[197] Article 13 (3) GDPR.

(d) the categories of personal data concerned;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47 GDPR, or the second subparagraph of Article 49(1) GDPR, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.[198]

In addition to the aforementioned information, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) where the processing is based on point (f) of Article 6(1) GDPR, the legitimate interests pursued by the controller or by a third party;
(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
(d) where processing is based on point (a) of Article 6(1) GDPR or point (a) of Article 9(2) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(e) the right to lodge a complaint with a supervisory authority;
(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[199]

The controller has to provide the information required by Article 14 (1) and (2) GDPR:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.[200]

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in Article 14 (2) GDPR.[201]

There is an exception to the information requirements imposed by Article 14 GDPR. This provision shall not apply where:

[198] Article 14 (1) GDPR.
[199] Article 14 (2) GDPR.
[200] Article 14 (3) GDPR.
[201] Article 14 (4) GDPR.

(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, **scientific** or historical **research** purposes or **statistical purposes**, subject to the conditions and safeguards referred to in Article 89(1) GDPR or in so far as the obligation referred to in Article 14 (1) GDPR is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
(c) obtaining or disclosure is expressly laid down by EU or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law, including a statutory obligation of secrecy.[202]

It is possible that the **'scientific research' exception applies in the context of WASABI**. This will be considered in depth below.

Article 15 GDPR grants data subjects **a right to access**. According to this provision, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[203]

Article 16 GDPR provides data subjects a right to obtain from the controller without undue delay the **rectification** of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

In addition, according to Article 17 GDPR, the data subject shall have the right to obtain from the controller the **erasure** of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

[202] Article 14 (5) GDPR.
[203] Article 15 (1) GDPR.

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) GDPR, or point (a) of Article 9(2) GDPR, and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) GDPR;
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) GDPR.

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.[204] **This provision may be relevant in the context of WASABI, since training data sets will be published with an Open Source License**.

Article 17 GDPR shall not apply to the extent that processing is necessary:

(…)
(d) for archiving purposes in the public interest, **scientific** or historical **research** purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing;[205]
(…)

As mentioned, it is possible that the **WASABI project falls under the 'scientific research' exception**. If that is the case, data subjects cannot exercise their right to erasure if exercising this right is likely to render impossible or seriously impair the achievement of the objectives of the processing for scientific research purposes.

Article 18 GDPR gives data subjects a **right to restriction** of processing. Specifically, the data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
(d) the data subject has objected to processing pursuant to Article 21(1) GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.[206]

[204] Article 15 (2) GDPR.
[205] Article 17 (3) (d) GDPR.
[206] Article 18 (1) GDPR.

Article 20 GDPR establishes a **right to data portability**. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) GDPR or point (a) of Article 9(2) GDPR or on a contract pursuant to point (b) of Article 6(1) GDPR; and
(b) the processing is carried out by automated means.[207]

Article 21 GDPR gives data subjects the **right to object**. In this regard, the most relevant provision for WASABI is stipulated in Article 21 (6) GDPR. According to this provision, where personal data are processed for **scientific** or historical **research** purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest. In addition, as mentioned, if processing is based on consent, the data subjects have a right to withdraw their consent at any time.[208]

Article 22 GDPR gives the data subject the right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Since the WASABI digital assistants are not used to make decisions regarding the workers whose data is collected, this provision is not relevant for the purposes of this deliverable.

The GDPR gives data subjects a series of rights. These include: a right to access, a right to rectification, a right to erasure, a right to restriction, a right to data portability, a right to object and a right not to be subject to automated decision-making. In the context of WASABI, it will be the task of the controller to enable data subjects to exercise these rights whenever personal data is processed.

**Obligations of the controller and the processor**

The **obligations of the controller and the processor** are stipulated in chapter IV GDPR. Controllers have the responsibility to make sure that processing is performed in compliance with the GDPR. In addition, controllers must ensure data protection by design and by default. Under certain conditions, controllers must carry out a data protection impact assessment and appoint a data protection officer. In case of a personal data breach, the controller must notify the supervisory authority and, under certain conditions, the data subject. Moreover, the controller can only use processors who provide sufficient guarantees of compliance with the GDPR. Processors, on their part, must process personal data in accordance with the instructions from the controller. Finally, there are also certain obligations that apply both to controllers and processors. These are: maintaining a record of processing activities, cooperating with the supervisory authority and ensuring an appropriate level of data security. The next paragraphs give a detailed exposition of the obligations of controllers and processors under the GDPR.

According to Article 24 GDPR, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate **technical and organizational measures to ensure and to be able to demonstrate that**

[207] Article 20 (1) GDPR.
[208] Article 7 (3) GDPR.

**processing is performed in accordance with the GDPR**.[209] Those measures shall be reviewed and updated where necessary. Where appropriate, those measures shall include the implementation of appropriate data protection policies by the controller.[210] Adherence to approved codes of conduct as referred to in Article 40 GDPR or approved certification mechanisms as referred to in Article 42 GDPR may be used as an element by which to demonstrate compliance with the obligations of the controller.[211]

Article 25 requires data controllers to ensure **data protection by design and by default**. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate **technical and organizational measures**, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.[212]

In addition, the controller shall implement appropriate **technical and organizational measures** for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.[213]

An approved certification mechanism pursuant to Article 42 GDPR may be used as an element to demonstrate compliance with the obligations stipulated in Article 25 GDPR.[214]

Where two or more controllers jointly determine the purposes and means of processing, they shall be **joint controllers**. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 GDPR, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by EU or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.[215] The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.[216] Irrespective of the terms of the arrangement, the data subject may exercise his or her rights under the GDPR in respect of and against each of the controllers.[217]

According to Article 28 GDPR, a controller cannot simply use anybody as a processor. On the contrary, the controller shall **use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR** and

[209] Article 24 (1) GDPR.
[210] Article 24 (2) GDPR.
[211] Article 24 (3) GDPR.
[212] Article 25 (1) GDPR.
[213] Article 25 (2) GDPR.
[214] Article 25 (3) GDPR.
[215] Article 26 (1) GDPR.
[216] Article 26 (1) GDPR.
[217] Article 26 (3) GDPR.

ensure the protection of the rights of the data subject.[218] Moreover, processors are not allowed to engage another processor without prior specific or general written authorization of the controller.[219]

**Processing by a processor shall be governed by a contract** or other legal act under EU or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by EU or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to Article 32 GDPR;
(d) respects the aforementioned conditions for engaging another processor;
(e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR;
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless EU or Member State law requires storage of the personal data;
(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.[220]

In addition, according to Article 29 GDPR, the processor must **process the personal data according to the instructions from the controller**, unless required otherwise by EU or Member State Law.

Article 30 requires both controllers and processors to keep a record of processing activities. Controllers must maintain a record that contains all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
(e) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;

[218] Article 28 (1) GDPR.
[219] Article 28 (2) GDPR.
[220] Article 28 (3) GDPR.

(f) where possible, the envisaged time limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.[221]

Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;
(d) where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.[222]

Article 31 GDPR requires controllers and processors to **cooperate**, on request, **with the supervisory authority** in the performance of its tasks.

Article 32 GDPR obliges controllers and processors to ensure **data security**. More precisely, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor **shall implement appropriate technical and organizational measures to ensure a level of security** appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymization and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[223]

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.[224] Once again, adherence to an approved code of conduct as referred to in Article 40 GDPR or an approved certification mechanism as referred to in Article 42 GDPR may be used as an element by which to demonstrate compliance with the data security requirements set out Article 32 GDPR.[225]

[221] Article 30 (1) GDPR.
[222] Article 30 (2) GDPR.
[223] Article 32 (1) GDPR.
[224] Article 32 (2) GDPR.
[225] Article 32 (3) GDPR.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, **notify the personal data breach to the supervisory authority** competent in accordance with Article 55 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[226] The processor shall **notify the controller** without undue delay after becoming aware of a personal data breach.[227] The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with Article 33 GDPR.[228] If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.[229]

In conclusion, the GDPR imposes a large number of obligations on controllers and processors. In the context of WASABI, the developers and/or end-users should comply with these obligations, depending on whether they qualify as 'controller' or 'processor' of a specific processing activity.

**Data protection impact assessment**

Under certain conditions, controllers must carry out a **data protection impact assessment** (DPIA). Specifically, 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.[230] When carrying out a DPIA, the controller shall seek the advice of the data protection officer, where designated.[231]

The WASABI digital assistants are machine learning models, and can thus be considered as a 'new technology' within the meaning of Article 35(1) GDPR. These assistants store conversations with workers to allow the continuation of the conversation at a later stage. Such conversations qualify as workers' personal data. As mentioned above, this data can be used to evaluate the performance of workers. Such a processing operation is likely to result in a high risk to the rights and freedoms of those workers, since it could lead to a discrimination of persons with disabilities or certain age groups. Therefore, it is possible that a DPIA is required when the WASABI digital assistants collect workers' personal data.

In addition, a DPIA shall in particular be required in the case of:

(a) a 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;
(b) processing on a large scale of special categories of data referred to in Article 9(1) GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 GDPR; or

[226] Article 33 (1) GDPR.
[227] Article 33 (2) GDPR.
[228] Article 33 (5) GDPR.
[229] Article 34 (1) GDPR.
[230] Article 35 (1) GDPR.
[231] Article 35 (2) GDPR.

(c) a systematic monitoring of a publicly accessible area on a large scale.[232]

As mentioned, the digital assistants continuously process audio to recognize wake words. Since voice data is biometric data, it could be argued that a DPIA is required when processing workers' voices. However, the assistants are not able to identify workers based on their voice. Therefore, no biometric data is processed for the purpose of uniquely identifying natural persons. Since no special category data is processed, it is unlikely that a DPIA is required when the assistants process audio to recognize wake words.

A DPIA assessment must contain at least:

(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;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects; and
(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 the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.[233]

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.[234]

**Data protection officer**

Under certain circumstances, Article 37 GDPR requires controllers and processors to designate **a data protection officer** (DPO). A DPO must be appointed in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 GDPR and personal data relating to criminal convictions and offences referred to in Article 10 GDPR.[235]

In other cases it is not mandatory to appoint a DPO. Nevertheless, the controller and the processor are allowed to do so.[236] The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 GDPR.[237] The DPO

[232] Article 35 (3) GDPR.
[233] Article 35 (7) GDPR.
[234] Article 35 (9) GDPR.
[235] Article 37 (1) GDPR.
[236] Article 37 (4) GDPR.
[237] Article 37 (5) GDPR.

may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.[238] The controller or the processor shall publish the contact details of the DPO and communicate them to the supervisory authority.[239]

In the context of WASABI, **the question is whether end-users need to appoint a DPO when deploying a digital assistant in their factories**. As mentioned, the end-users collect and store conversations between the digital assistants and the workers. This amounts to processing of personal data. However, the question is whether this processing operation crosses the threshold of Article 37(b) GDPR. This is the case if the core activities of the end-users require regular and systematic monitoring of workers on a large scale.

First, the 'core activities' of a controller relate to primary activities and do not relate to the processing of personal data as ancillary activities.[240] 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals. However, 'core activities' should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity.[241] Thus, while the core activity of end-users of the digital assistants is manufacturing, the end-users cannot fulfil this activity effectively without processing the conversations between workers and the digital assistants, since such processing is necessary to allow the assistants to function. Without such processing, the digital assistants do not work, which affects the manufacturing activities of the end-users. In other words, processing conversations between workers and the digital assistants can be considered to be part of the end-users' core activities. [242]

Second, the question is whether storing conversations between workers and the digital assistants amounts to regular and systematic monitoring. The notion of 'regular and systematic monitoring' is not defined in the GDPR. However, recital 24 states that 'monitoring the behavior of data subjects' includes all forms of tracking and profiling on the internet. [243] In principle, the WASABI digital assistants are not used to monitor the behavior of workers. However, it is possible that end-users rely on the conversations stored by the assistants to evaluate their workers. Even though this scenario is unlikely, it cannot be excluded that deploying the digital assistants can lead to monitoring of data subjects.

According to the WP29 'regular' monitoring means one or more of the following:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times
- Constantly or periodically taking place[244]

In addition, 'systematic monitoring' means one or more of the following:

- Occurring according to a system
- Pre-arranged, organized or methodical
- Taking place as part of a general plan for data collection

[238] Article 37 (6) GDPR.
[239] Article 37 (7) GDPR.
[240] Recital 97 GDPR.
[241] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 7.
[242] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 7.
[243] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 8.
[244] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 8-9.

- Carried out as part of a strategy[245]

While it cannot be excluded that end-users will rely on conversation data to monitor workers, it is unlikely that such monitoring will take place on a systematic level. However, if this is the case, end-users will have to appoint a DPO.

Third, a DPO must only be appointed if personal data is processed on a 'large scale'. The GDPR does not define what amounts to large-scale processing. It is not possible to give a precise number relating to the amount of data processed or the number of data subjects concerned.[246] Nevertheless, the WP29 recommends that the following factors should be taken into account when assessing whether processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity[247]

Some Member States have issued guidance on what amounts to 'large scale' processing. For instance, the Polish data protection authority has given a number of examples of data processing operations that should be considered to be large scale. The most interesting example in the context of WASABI is employee documentation.[248] Thus, it is possible that the collection of workers' personal data is in itself sufficient to amount to large scale processing, regardless of the amount of data processed or the number of individuals concerned.

In conclusion, end-users of the WASABI digital assistants will have to appoint a DPO when deploying the assistants if the core activities of the end-users require regular and systematic monitoring of workers on a large scale. As mentioned, it cannot be excluded that end-users will rely on conversation data to monitor and evaluate their employees. However, it is unlikely that this will happen on a systematic level. Therefore, it could be argued that appointing a DPO is not mandatory when deploying the WASABI digital assistants in end-users' factories.

In any event, it is not obvious that end-users are not required to appoint a DPO when deploying the digital assistants in their factories. Therefore, the WP29 recommends that end-users, being controllers, document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly. This analysis is part of the documentation under the accountability principle stipulated in Article 5(2) GDPR. It may be required by the supervisory authority and should be updated when necessary, for example if the end-users undertake new activities or provide new services that might fall within the cases listed in Article 37(1).[249]

When an end-user designates a DPO on a voluntary basis, the requirements under Articles 37 to 39 GDPR will apply to his or her designation, position and tasks as if the designation had been mandatory.[250]

[245] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 9.
[246] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 7.
[247] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 7-8.
[248] P. Breithbarth, "On large-scale processing and GDPR compliance", 2018. Available: On large-scale data processing and GDPR compliance | IAPP.
[249] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 5.
[250] Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 5.

The **position of the DPO** is detailed in Article 38 GDPR. The controller and the processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.[251] The controller and processor shall support the DPO in performing the tasks referred to in Article 39 GDPR by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.[252] In addition, the controller and processor shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The DPO shall directly report to the highest management level of the controller or the processor.[253] Furthermore, data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR.[254] The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with EU or Member State law.[255] Finally, the DPO may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.[256]

Article 39 GDPR contains the **tasks of the DPO**. The DPO shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other EU or Member State data protection provisions;
(b) to monitor compliance with the GDPR, with other EU or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 GDPR;
(d) to cooperate with the supervisory authority;
(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 GDPR, and to consult, where appropriate, with regard to any other matter.[257]

The DPO shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.[258]

**Processing for scientific research purposes**

Article 5(1)(b) contains an **exception to the purpose limitation principle**. According to this principle, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. However, **further processing for scientific research** purposes shall not be considered to be incompatible with the initial purposes. This is the so-called 'research exemption'.

[251] Article 38 (1) GDPR.
[252] Article 38 (2) GDPR.
[253] Article 38 (3) GDPR.
[254] Article 38 (4) GDPR.
[255] Article 38 (5) GDPR.
[256] Article 38 (6) GDPR.
[257] Article 39 (1) GDPR.
[258] Article 39 (2) GDPR.

Simply put, every processing operation with a distinct purpose needs to have a separate legal ground. Thus, if data is collected for one purpose, and is then processed for another purpose, it is necessary to obtain a new legal ground for that second processing operation. For instance, the controller needs the data subjects' consent in order to process their personal data for another purpose than for the purpose it was originally collected. However, if the second purpose is scientific research, it is not necessary to have a new legal ground. This means that if data is collected for one purpose and is then used for scientific research purposes, it is not necessary to obtain the consent of the relevant data subjects within the meaning of Article 6(1)(a) GDPR, for regular personal data, and within the meaning of Article 9(2)(a) GDPR, for special category data.

The GDPR does not define the term 'research'. What is clear, however, is that it is a broad concept. According to Recital 159 GDPR, it includes technological development and demonstration, fundamental research, applied research and privately funded research. In order to qualify as research, it is important that the research results are published. Indeed, the purpose of research is to gain new knowledge and to share this knowledge with society.

WASABI is a research project funded by the EU that will make its results public through a detailed communication and dissemination plan. It can therefore be argued that data processing in the context of WASABI qualifies as processing for scientific research purposes. **As a result, WASABI may benefit from the 'research exemption'**. This would mean that WASABI is allowed to process personal data that was originally collected for another purpose, without requiring a new legal ground, such as consent, to do so. Of course, the collection of new personal data must have a legal ground. For instance, if personal data of workers using the digital assistants is collected, it is necessary to obtain, for example, the consent of those workers.

It is not because the 'research exemption' applies that the provisions of the GDPR no longer play a role. Data subjects must still be able to enjoy their rights and controllers and processers still have to comply with their obligations under the GDPR. However, the GDPR contains a number of exceptions to the rights of data subjects in case of processing for scientific research purposes. For example, a data subject cannot exercise his or her right to erasure if exercising this right is likely to render impossible or seriously impair the achievement of the objectives of that processing.[259] Furthermore, the right to information under Article 14 GDPR does not apply if the provision of such information would prove a disproportionate effort.[260]

In order to protect data subjects, the GDPR requires taking appropriate safeguards when processing for research purposes. According to Article 89 GDPR, processing for archiving purposes in the public interest, **scientific** or historical **research** purposes or statistical purposes, shall be subject to **appropriate safeguards**, in accordance with the GDPR, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. Those measures may include pseudonymization provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.[261]

WASABI may be able to benefit from the 'research exemption' under Article 5(1)(b) GDPR.

[259] Article 17 (3) (d) GDPR.
[260] Article 14 (5) (b) GDPR.
[261] Article 89 (1) GDPR.

**Right to compensation and liability**

Article 82 gives data subjects a **right to compensation and regulates the liability of controllers and processors** for infringements of the GDPR.

According to Article 82 GDPR, any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the **right to receive compensation** from the controller or processor for the damage suffered.[262] Any **controller** involved in processing shall be **liable** for the damage caused by processing which infringes the GDPR. A **processor** shall be **liable** for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.[263] A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.[264]

Where **more than one controller or processor**, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.[265] Where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage. [266]

**Key takeaways**

The WASABI project requires processing personal data. As a result, the GDPR is applicable. This means that every processing operation with a distinct purpose requires a distinct legal ground. For the processing activities in the context of WASABI, 'consent' will likely be the most relevant legal ground. In addition, processing must comply with the data protection principles of Article 5 GDPR. For every processing operation, it must be determined who the controller and, where applicable, who the processor of that operation is. For instance, when training the digital assistants, the developers of the assistants will qualify as the controllers of that processing operation. Controllers must ensure that the data subjects are able to exercise their rights. Moreover, controllers and processors have to comply with their obligations under the GDPR. Otherwise, they risk incurring liability. One of these obligations is carrying out a DPIA. This will likely be required when collecting workers' personal data, such as conversations with the digital assistants. When carrying out a DPIA, the controller and/processor can rely on the advice of the DPO, where appointed.

# 5. CONCLUSIONS

This deliverable mapped and described the EU regulatory framework applicable in the context of WASABI, and discussed liability for lack of compliance with EU law. Specifically, this deliverable focused on the following EU Regulations and Directives: the AI Act, the proposal for an AI Liability Directive, the Product Liability Directive, and the General Data Protection Regulation. We provided an in depth exposition of the content of these legal acts, and applied them in the context of digital assistance solutions in manufacturing.

[262] Article 82 (1) GDPR.
[263] Article 82 (2) GDPR.
[264] Article 82 (3) GDPR.
[265] Article 82 (4) GDPR.
[266] Article 82 (5) GDPR.

After a thorough analysis, we give a final recap of our main findings under each of the discussed EU legal acts.

**AI Act**

It is possible that the WASABI digital assistants qualify as high-risk AI systems within the meaning of the AI Act. If that is the case, they must comply with a series of **safety requirements**. These include: risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity. In order to ensure that these requirements are met, the AI Act imposes a number of obligations on providers and deployers of high-risk AI systems. In the context of WASABI, the developers of the digital assistants should comply with the obligations of providers, while the end-users should comply with the obligations of deployers. The easiest way to comply with these obligations is by following harmonized standards. High-risk AI systems that comply with harmonized standards enjoy a presumption of compliance with the safety requirements of the AI Act.

**Proposal for an AI Liability Directive**

The proposal for an AI Liability Directive increases the liability risk for the developers and end-users of the WASABI digital assistants. It does so by requiring a disclosure of evidence and introducing a rebuttable presumption of causality if certain conditions are met.

**(revised) Product Liability Directive**

The WASABI digital assistants qualify as 'products' within the meaning of the revised Product Liability Directive, while the developers of the digital assistants qualify as 'manufacturers' under this Directive. The developers can therefore be held liable if the digital assistants are defective and cause damage to natural persons. Because of the technical complexity of the digital assistants, both defectiveness and causality will likely be presumed. In any case, if the digital assistants do not comply with the safety requirements for high-risk AI systems imposed by the AI Act, they are presumed to be defective. Finally, because the developers may be able to exercise control over the digital assistants after they are placed on the market, their defenses against liability are limited.

**GDPR**

The WASABI project requires processing personal data. As a result, the GDPR is applicable. This means that every processing operation with a distinct purpose requires a distinct legal ground. For the processing activities in the context of WASABI, 'consent' will likely be the most relevant legal ground. In addition, processing must comply with the data protection principles of Article 5 GDPR. For every processing operation, it must be determined who the controller and, where applicable, who the processor of that operation is. For instance, when training the digital assistants, the developers of the assistants will qualify as the controllers of that processing operation. Controllers must ensure that the data subjects are able to exercise their rights. Moreover, controllers and processors have to comply with their obligations under the GDPR. Otherwise, they risk incurring liability. One of these obligations is carrying out a DPIA. This will likely be required when collecting workers' personal data, such as conversations with the digital assistants. When carrying out a DPIA, the controller and/processor can rely on the advice of the DPO, where appointed.

# 6. BIBLIOGRAPHY


**EU legislation**

- Regulation of the European Parliament and of the Council of 19 April 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
- Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (hereafter: Machinery Regulation).
- Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).
- Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) (Product Liability Directive).
- European Parliament legislative resolution of 12 March 2024 on the proposal for a directive of the European Parliament and of the Council on liability for defective products (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD) (revised Product Liability Directive).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

**National legislation**

- New Belgian Civil Code.

**Legal doctrine**

- VEALE, M. and BORGESIUS, F. Z., "Demystifying the Draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach", *CRi* 2021, 97-112.
- DE BRUYNE, J., VAN GOOL, E. and GILS, T., "Tort Law and Damage Caused by AI Systems" in DE BRUYNE J. and VANLEENHOVE, C., (eds.) *Artificial Intelligence and the Law*, Cambridge, Intersentia, 2021, 520 p.
- VAN GOOL, E., "Case C-65/20 Krone: Offering (some) clarity relating to product liability, information and software", *European Law Blog* 2022.
- VERHEYEN, T., *Eenzijdige beheersing van het aansprakelijkheidsrisico: Over waarschuwingen, instructies, disclaimers en andere technieken tot eenzijdige exoneratie,* Antwerp, Intersentia, 2021, 717 p.
- CABRAL, T. S., "Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive", *Maastricht Journal of European and Comparative Law* 2020, 615-635.
- VANSWEEVELT, T. and WEYTS, B., *Handboek Buitencontractueel Aansprakelijkheidsrecht*, Antwerp, Intersentia, 2009, 935 p.
- BEGLINGER, C., "A broken Theory: The Malfunction Theory of Strict Products Liability and the Need for a new Doctrine in the Field of Surgical Robotics Note", *Minnesota Law Review* 2019, 1041-1093.
- P. Breithbarth, "On large-scale processing and GDPR compliance", 2018. Available: On large-scale data processing and GDPR compliance | IAPP.
- C. McCrudden, "Legal Research and the Social Sciences", *The Law quarterly review* 2006, 632-650.

**Other**


- BERGSTROM D. and WEST, J., *Calling Bullshit: The Art of Skepticism in a Data-driven World*, New York, Random House, New York, 2021, 318 p.
- EUROPEAN DATA PROTECTION SUPERVISOR, "AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation", 2021.
- CEN, Information technology - Artificial intelligence - Guidance on risk management (ISO/IEC 23894:2023). Available: CEN - CEN/CLC/JTC 21 (cencenelec.eu).
- EUROPEAN PARLIAMENT, "New Product Liability Directive", *Briefing: EU Legislation in Progress* 2023, 12 p.
- European Data Protection Board (EDPB), *Guidelines 02/2021 on virtual voice assistants*, version 2.0, 2021, 39 p.
- Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers (DPO's)", 2017, 25 p.
- White-label shop for digital intelligent assistance and human-AI collaboration in manufacturing (WASABI proposal), 187 p.