

D2.2: Ethics and legal Requirements

Revision: v.1.2

Work package	WP 2
Task	Task 2.2
Due date	30/05/2026
Submission date	30/05/2026
Deliverable lead	UGR
Version	1.2
Authors	Javier Valls Prieto, Henrik Larsen, Dimitris Katsaros
Reviewers	Patricia Saldaña Taboada
Abstract	The main objective of this deliverable is to carry out an ethical and legal assessment of the AI technologies implemented in Project X. A design-for-compliance analysis has been conducted from the earliest stages of the project to ensure that the risks are understood and that a plan is in place to address any negative impacts that may arise from their implementation.
Keywords	Impact, Fundamental Rights, Ethics, AI Act, Ethics assessment

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	27/02/2026	1st edit	Javier Valls Prieto (UGR) Henrik Larsen (LTA) Dimitris Katsaros (NEXUS)

V1.0	13/04/2026	Legal impact	Javier Valls Prieto (UGR)
V1.1	20/04/2026	Ethical assessment	Javier Valls Prieto (UGR)
V1.2	25/05/2026	Final version	Javier Valls Prieto (UGR)

DISCLAIMER



**Funded by
the European Union**

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

Funded by the European Union (BAG-INTEL, 101121309). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

COPYRIGHT NOTICE

© 2023 - 2026 BAG-INTEL

Project funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	ETHICS*	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)	✓
SEN	Sensitive, limited under the conditions of the Grant Agreement	
Classified R-UE/ EU-R	EU RESTRICTED under the Commission Decision No2015/ 444	
Classified C-UE/ EU-C	EU CONFIDENTIAL under the Commission Decision No2015/ 444	
Classified S-UE/ EU-S	EU SECRET under the Commission Decision No2015/ 444	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.



**Funded by
the European Union**

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI



EXECUTIVE SUMMARY

MOTIVATION AND CONTEXT

The rapid integration of artificial intelligence (AI) systems within border control and public safety operations demands a rigorous balance between security efficacy and strict compliance with European legal frameworks. The **BAG-INTEL** project develops an intelligent scanner system designed to detect smuggling and contraband within the luggage of travellers in airport environments. Given the evolving legislative landscape in the European Union, it is essential to determine whether these specific AI technologies are categorised as "high-risk" under the **EU AI Act** and to comprehensively evaluate their potential impact on the fundamental rights of citizens.

Artificial Intelligence (AI) systems deployed in high-stakes environments—such as border control and law enforcement—have a dual nature: they can significantly enhance public safety and operational efficiency, but they also pose inherent risks to fundamental human rights, data privacy, and personal autonomy. Establishing a robust framework for ethical compliance is critical for the BAG-INTEL project. Because the project operates entirely within a European context, it is essential to build public trust and ensure legal viability by aligning its technologies with democratic values and strict regulatory standards.

RESEARCH METHODOLOGY

Two different methodologies will be used in this analysis, depending on whether the section under consideration is legal or ethical.

The legal analysis methodology consists of a structured legal and jurisprudential assessment divided into three key phases:

- **Risk classification analysis:** The system's operational scope is evaluated against the criteria laid out in article 6 and annexe III of the EU AI Act to determine its exact regulatory tier.
- **Human Rights Impact Assessment (HRIA):** analysing the project's compatibility with the European Convention on Human Rights (ECHR) and the European Union Charter of Fundamental Rights, focusing particularly on the constitutional tension between security needs and data privacy.
- **Compliance Alignment:** Benchmarking the AI system's lifecycle development against the newly published *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (May 2026).

The ethical analysis of the BAG-INTEL AI components was conducted using the European Commission's High-Level Expert Group (HLEG) guidelines for Trustworthy AI as its baseline. The methodology focused on assessing the systems against four core ethical principles (Respect for human autonomy, Prevention of harm, Fairness, and Explicability) operationalised through seven key requirements.

A streamlined version of the HLEG Trustworthy AI Assessment Checklist was converted into a structured questionnaire to achieve a pragmatic, context-tailored assessment. This questionnaire was distributed to the technical partners responsible for developing the AI tools of the project. The compliance evaluation was further enriched through an ongoing, multilevel collaborative review

process involving engineers, law enforcement end-users, and a dedicated ethics and legal team throughout the system's lifecycle.

KEY FINDINGS AND CONCLUSIONS

We can highlight the following points as the most significant aspects of the work carried out in the ethical and legal assessment of the BAG-INTEL project:

- **Formal High-Risk Classification:** The BAG-INTEL project utilises at least three AI subsystems that are evaluated collectively as a single system. Although the technology purposefully avoids capturing biometric data or analysing individual personal behaviour (focusing strictly on luggage and objects) , **it is formally classified as a high-risk AI system**. This conclusion is triggered by section 57(b) of annex III (migration, asylum, and border control management) because automated scanning for illicit substances (such as drugs) directly addresses serious public health risks.
- **Fundamental Rights Impact and Justification:** The implementation primarily interacts with two core legal pillars of the EU Charter: article 6 (Right to liberty and security) and article 8 (Protection of personal data).
 - The assessment concludes that the scanner does not violate the absolute *essence* of these rights. Passenger detention resulting from potential false positives does not infringe on physical liberty, if it is strictly limited to the time required to fulfil standard custom formalities.
 - While data processing activities by definition constitute a technical interference with data protection rights , this use of data is legally permissible and justified for law enforcement authorities acting to safeguard Public security.
- **Adherence to 2026 Legal Standards:** The project's development pipeline aligns with the Council of Europe Framework Convention from May 2026. It explicitly integrates the newly emphasised principles of **reliability** (ensuring confidence in results to prevent discriminatory flight screening) and **safe innovation** (testing within controlled, supervised environments).
- **Human-in-the-Loop Supremacy:** The BAG-INTEL prototype successfully avoids fully automated decision-making. AI tools—specifically object recognition in x-ray scanner images (for detecting drugs, tobacco, and cash) and machine learning models for flight risk tracking—serve strictly as advisory alert mechanisms. The final decision-making authority regarding luggage inspections remains entirely in the hands of human law enforcement agencies (LEAs), mitigating risks related to system errors or false positives.
- **Success in Privacy and Data minimisation:** The project successfully navigated complex data privacy constraints by implementing strict data minimisation techniques. For luggage tracking through CCTV, passengers' faces and identifying features are systematically blurred to protect anonymity. To avoid the legally complex integration of real police databases or Passenger Name Record (PNR) data, the system was trained and evaluated using synthetic data modelled after real-world security requirements.
- **Robustness and Access Security:** While the prototype phase has not anticipated complex external hostile attacks, the system is deemed secure and non-vulnerable due to restricted, login-controlled access limited to a very small group of authorised users. Furthermore,

because of heavy human oversight, internal errors or "incorrect results" do not carry critical real-world consequences and can be easily reversed by personnel.

- **Transparency and Managing Trade-offs:** An inherent "black box" limitation exists within the complex machine learning models used, making it difficult to trace the exact decision-making logic. This explainability-versus-accuracy trade-off is successfully mitigated by increasing human oversight, training end-users on system limitations, and providing clear, interpretable outputs (e.g., risk levels and contributing indicators) to officers.
- **Societal and Environmental Well-being:** The design process intentionally reduced resource usage by eliminating unnecessary information from the data pipeline, lowering the overall operational energy consumption of the system. Societally, the system yields positive impacts by optimising customs wait times, enhancing crime detection, and improving state revenue collection.

RECOMMENDATIONS

Although it is very difficult to predict the actual use of the technologies applied to the project due to the scale issue, we can draw conclusions from the use cases in which the baggage control system has been tested.

Now that work on this deliverable has been completed, we would like to highlight the following recommendations regarding the use of this type of technology for baggage screening at airports

- **Formalize the Article 27 Impact Assessment:** The project consortium must formally complete and document a full Human Rights Impact Assessment (HRIA) prior to any operational deployment because the system meets the high-risk thresholds of the AI Act.
- **Establishment of Mitigation Protocols for System Errors:** Strict operational guidelines must be implemented to manage algorithmic errors. False positives must be processed rapidly to prevent arbitrary or disproportionate passenger delays (prohibited under Article 6) , while flight selection criteria must be continuously audited to eliminate any bias or discrimination based on destination.
- **Maintain unified governance:** The project should adhere to the conservative approach of treating all integrated AI components under the highest common denominator of compliance (high-risk status), ensuring that no regulatory gaps remain in any of its operative software modules.
- **Comprehensive External Communications:** While training and engagement of internal end-users (LEAs) have been highly active, future real-world deployments should focus on public-facing transparency. It is recommended to proactively display clear information regarding the use of AI in baggage screening on airport websites, mobile applications, and physical baggage claim areas.
- **Iterative Accuracy and Metrics Tracking:** The system's accuracy is heavily dependent on an expanding knowledge base, and performance metrics were still being assessed at the time of reporting. As the volume of machine learning training cases grows, the development teams must establish continuous evaluation pipelines to log and monitor real-world accuracy.

- **Preparation for Post-Prototype Scaling:** Any future international deployment or commercial scaling will require a completely separate, heavily adapted ethical and legal impact assessment because the prototype was explicitly customised for a European legislative framework (such as Directive 2016/680) and European cultural perceptions of fundamental rights. In addition, detailed explanations of design criteria should be integrated into the final market product documentation, as it fell outside the scope of this prototype phase.

TABLE OF CONTENTS

1 INTRODUCTION..... 11

2 LEGAL ISSUES: THE AI ACT 14

3 ETHICS 22

4 CONCLUSIONS..... 38

LIST OF FIGURES

FIGURE 1: EMPTY.....	26
FIGURE 2: COCAINE.....	26
FIGURE 3: BLISTERS.....	27
FIGURE 4: FALSE ALARM	28
FIGURE 5: FLIGHT TRACKING	28
FIGURE 6: FLIGHT ALERTS.....	29
FIGURE 7: APP ALERT FEEDBACK	32
FIGURE 8: LEAS' APP REVIEW AND SUBMISSION OF INFORMATION.....	33
FIGURE 9: PASSENGER ANONYMIZATION	34
FIGURE 10: PASSENGER FACE BLURRING	36

ABBREVIATIONS

AI	Artificial Intelligence
CCTV	Closed Circuit Television
DoA	Document of Action
DPIA	Data protection impact assessment
ELSIA	Ethic, legal and societal impact assessment
EC	European Community
ECHR	European Convention on human rights
EU	European Union
GDPR	General Data Protection Regulation
HLEG	High Level Expert Group
LEA	Law Enforcement Agency
NGO	non-Governmental Organization
PNR	Passenger Name Record
PU	Public
SIS	Schengen Information System

1 INTRODUCTION

BACKGROUND

The BAG-INTEL project addresses the problem of luggage control at airports by creating an intelligent scanner and baggage tracking system from baggage collection to airport customs control. The scanner detects substances considered as contraband using an image recognition system that will detect possible contraband objects. Once the object is detected in the baggage, it can be tracked by custom authorities to the checkpoint.

The original document was marked PU. However, it is recommended that the document remains confidential because it is intended to assist the consortium partners in the development and delivery of the BAG-INTEL tools. As such, it contains extensive references to the technology design and development, raising security risks for LEAs.

PURPOSE AND SCOPE

This deliverable focuses on assessing the impacts of the BAG-INTEL project on ethics, data protection, and other fundamental rights and the use of AI. It sets a comprehensive report on the activities that the consortium partners will conduct as part of task T2.2 and its findings. Considering the legal, ethical, and societal requirements and constraints for intelligence-led technologies, the partners answered an ethical privacy assessment, ethical, legal, and social impact assessment, and a trustworthy AI analysis of BAG-INTEL technologies.

Three artificial intelligence models are used in the development of the BAG-INTEL scanner to carry out risk analysis and to detect and track suitcases identified as containing any of the substances being analysed as part of the project.

Machine learning systems have been used in risk assessments to identify suitcases that require screening and to analyse future risks and predict smuggling. In baggage tracking, image recognition has been used to track luggage as it moves through the airport.

The ethical and legal analysis of AI systems will focus on these three tools, taking a comprehensive view of the system as required by the AI Act. In adopting this ethical approach from the outset, an 'ethics by design' model was chosen right from the start of the project. An initial analysis was carried out in the first deliverable to identify potential risks, culminating in this final analysis of the tools that have been implemented.

In line with the BAG-INTEL Description of Action (DoA), this report collects the partners' answers to the assessment of the BAG-INTEL project's impacts on data protection, other fundamental rights, and the Trustworthy AI and how the consortium will have an ethical and legal by design approach from the first steps.

Specifically, this deliverable:

1. Explain the concept of the tools used;
2. Describes the partners' knowledge of the risk they will face;
3. Provides key findings about the BAG-INTEL tools' trustworthy IA, ELSIA, and DPIA.

The methodological approach to legal and ethical analysis aims to bridge the gap [1] between the two fields to achieve the most comprehensive governance model possible, with the aim of protecting human rights, the rule of law, and democratic systems.

DOCUMENT STRUCTURE

This document is divided into four sections. The first section introduces the ethical and legal assessment of the artificial intelligence systems used in Project BAG-INTEL. This document outlines the work carried out, as well as the project's components, objectives, and aims.

The second section consists of a legal analysis of systems. This study examines compliance with the requirements of the AI Act, the impact assessment, and an analysis of the fundamental rights affected by this specific development.

The third part is an ethical analysis of the use of artificial intelligence in the project. To this end, we have drawn on the guidelines for trustworthy artificial intelligence produced by the European Commission's High Level Expert Group, setting out seven key points for the ethical use of this technology: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability [2].

Finally, in the fourth section, we discuss the conclusions and recommendations for the development of these artificial intelligence models within the context of luggage inspection.

APPLICABLE AND REFERENCE DOCUMENTS

Council of Europe:

- European Convention on Human Rights
- CETS 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

European Union:

- Charter of Fundamental Rights of the European Union
- 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, GDPR).
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the

field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006.

- Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts.
- European Commission, H2020 Programme Guidance: How to complete your ethics self-assessment, Version 6.1, 4 Feb 2019. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf
- European Commission, annexe 2: Ethics issues table – checklist, http://ec.europa.eu/research/participants/portal/doc/call/h2020/msca-rise-2014/1597696-ethics_issues_table_checklist_en.pdf

2 LEGAL ISSUES: THE AI ACT

2.1 HIGH-RISK SYSTEM ASSESSMENT

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised 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 (AI Act) defines, in its article 6.1, high-risk AI systems as these AI system that (a) 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 Union harmonisation legislation listed in annexe I; and (b) The product whose safety component pursuant to point (a) 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 placing that product on the market or putting it into service pursuant to the Union harmonisation legislation listed in annexe I. In the case of BAG-INTEL, point 1 does not apply to our case.

The second paragraph of Article 6 refers directly to annexe III of the Regulation, where we can find eight areas of use in which our project may be included. These eight areas are as follows:

1. Biometrics, insofar as their use is permitted under relevant Union or national law
2. Critical infrastructure: AI systems are intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or water, gas, heating, or electricity supply.
3. Education and vocational training.
4. Employment, workers' management, and self-employment access
5. Access to and enjoyment of essential Private and Public services and benefits.
6. Law enforcement, insofar as their use is permitted under relevant Union or national law.
7. Migration, asylum, and border control management insofar as their use is permitted under relevant Union or national law.
8. Administration of justice and democratic processes

From this list, we focus on three areas: critical infrastructure, law enforcement, and border control management. From this analysis, we will decide whether the AI technologies implemented in the BAG-INTEL can be considered as high risk.

Regarding the section on critical infrastructure, we cannot interpret border controls at airports as the use of AI for the management and operation of critical digital infrastructure. It is true that airports are classified as critical infrastructure under the Directive, but customs checks for contraband cannot be regarded as a threat to airport security.

With regard to law enforcement, the AI Act sets out five possible uses by the authorities. The first step is to assess the risk of a natural person becoming a victim of a criminal offense. In the case of BAG-INTEL, victims are not involved at any stage. The primary purpose of the scanner is to detect smuggling, with the scanner designed to focus on objects rather than people. In the second scenario, the artificial intelligence system acts as a support tool for authorities responsible for ensuring law enforcement, such as polygraphs or similar tools. In his case, the wording is so broad that it could be interpreted as referring to any tool used to enforce the law. There is not much further information, other than the fact that it is a tool like a polygraph. A scanner aims to help detect falsehoods in travellers' custom declarations. However, it is true that it is not a tool that captures a person's biometric data or analyses their behaviour. Indeed, in BAG-INTEL, this type of analysis has been avoided because it is considered disproportionate in the use of personal data, with the aim of finding a less intrusive alternative that

respects individuals. In this case, we cannot say for certain whether this is a high-risk AI system. However, it is true that it could be regarded as such due to the lack of clarity in the legislation. The third scenario concerns the examination of evidence during the investigation or prosecution of criminal offenses. In this case, BAG-INTEL Will focus on analysing items found in travellers' luggage. However, this is a stage before the investigation or prosecution of the offenses. It intends to detect contraband and not to assess the evidence obtained. We cannot consider this to fall within this category, as the primary objective is to assist in detecting offences rather than in the evidence relating to them, although the substances being sought are the main subject of these smuggling offences. Points (d) and (e) of Section 6 of annexe III would also not cover the activities carried out within BAG-INTEL, as they do not focus on individuals but on luggage. Hence, no risk assessments will be carried out regarding whether a person is likely to commit a crime or reoffend, nor will any assessment be made of personality traits or characteristics or past criminal behaviour. As natural persons are not the central focus of the scanner's operation, they would not fall within the scope of point (e), namely, the detection, investigation, or prosecution of offences, although the results of the scanner's use may be utilised in these phases of the fight against smuggling.

The final possibility for the use of AI systems in BAG-INTEL to be considered is that set out in section seven of annexe III. Point seven covers the use of high-risk systems in migration, asylum, and border management. This third point would fall squarely within the scope of the activities to be conducted at BAG-INTEL. The regulations identify four usage contexts that are considered high-risk: a) artificial intelligence systems intended to be used as polygraphs or similar tools; b) artificial intelligence systems intended to be used to assess risks, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State; c) AI systems intended to be used to assist competent public authorities for the examination of applications for asylum, visa, or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence; and d) AI systems intended to be used in the context of migration, asylum, or border control management, for the purpose of detecting, recognising, or identifying natural persons, with the exception of the verification of travel documents.

Regarding the first case, the issues raised by the 'similar tools' clause have already been highlighted. The scanner performs a function like that of a lie detector in detecting deception when passing through customs without any physical contact with the individual. It is not clear, but the scanner could be considered a high-risk system.

In the second case, where it is used to assess the risks posed by a person seeking to enter or having entered the territory of a Member State, smuggling could be considered a risk; however, in the case of cash or cigarettes, this would not constitute a serious risk but rather an administrative offence. In the case of drugs, the situation is different, as there would indeed be a serious risk to people's health. Therefore, we must consider that the artificial intelligence systems to be implemented within Project BAG-INTEL are indeed high-risk.

The next provision, point (c), would apply to cases where the authorities use the systems to grant asylum, visas, or residence permits. This does not apply to the use of the AI systems employed at BAG-INTEL.

Finally, intelligent systems used in the context of migration, asylum, or border management for the purpose of detecting, identifying, or recognising individuals would not fall within the scope of BAG-INTEL either, since the entire evaluation system implemented in BAG-INTEL relates to objects and luggage.

Therefore, we can conclude that the systems used in BAG-INTEL are indeed considered high-risk because they fall under section 7(b) of annexe III. BAG-INTEL uses at least three AI systems to operate. Although not all of them may be considered high risk, we will treat them all as a single system. Considering this criterion, we focus on the impact assessment requirements from article 27 of the AI Act. Thus, a human rights impact assessment Will be conducted.

2.2 HUMAN RIGHTS IMPACT ASSESSMENT

To analyse the impact on human rights, we will focus on the European Convention on Human Rights as a framework applicable at the European level, where the project is being conducted and its operations are concentrated [3]. Within this list of rights, two articles regulate the two rights most affected by the project's implementation.

In a commercial application of the scanner, the impact on fundamental rights would be more far-reaching. On initial examination of the impact, we can see how the misuse of the AI systems implemented in the scanner could affect rights such as freedom of movement, health, property rights, privacy, the principle of equality, and the right to security. Eg, a false positive may result in a person being wrongly detained for inspection, causing them to miss a connecting flight due to the delay. A false negative undermines the right to security. The process may discriminate against flights arriving from certain destinations when selecting aircraft for inspection. The impact on fundamental rights in these cases is not so significant, given that, in principle, travellers must be prepared for customs inspections; however, this may affect certain sections of the population in a way that restricts their fundamental rights.

The two fundamental rights that will be affected are the right to security and the right to privacy, which are enshrined in Articles 5 and 8 of the European Convention on Human Rights. The other key document on human rights at the European level is the Charter of Fundamental Rights of the European Union. This document sets out the right to security and privacy (Article 6, which, as in the Convention, is linked to the right to liberty, and Article 8, which concerns the protection of personal data).

Articles 6 and 8 of the Charter of Fundamental Rights of the European Union constitute two key legal pillars within the Union's constitutional architecture. The first guarantees the right to Liberty and security; the second guarantees the right to the protection of personal data. Although they belong to the same Title II on Freedoms, their relationship is far from harmonious: these two rights are frequently in tension in the fields of electronic surveillance, data retention, or the control of digital identities. Understanding their substantive content, their limits, and the way in which the Court of Justice of the European Union (CJEU) has interpreted them is essential for any analysis of the European system for the protection of fundamental rights.

2.2.1 Article 6: Physical liberty as a prerequisite for all rights

Article 6 of the Charter states in a single sentence that 'everyone has the right to Liberty and security. This concise wording is deliberate and contrasts with the length of Article 5 of the European Convention on Human Rights (ECHR), from which it derives directly. As José Martín y Pérez de Nanclares explains in the article-by-article commentary edited by Araceli Mangas Martín, 'the right to liberty, understood in the sense of physical liberty, is one of the most basic and fundamental rights of the individual'. It constitutes, in fact, a prerequisite for the exercise of all other individual rights and freedoms, alongside the equally fundamental right to life [4].

2.2.1.1 Freedom's scope: prohibition of arbitrary detention

Article 6's core substance lies in protection against arbitrary deprivation of liberty. the broad concept of Liberty has been defined by the ECHR as the individual's physical Liberty and, specifically, as the corresponding protection against arbitrary or unjustified arrests or imprisonment [...]. The aim of this provision is, therefore, to ensure that no one can be deprived of their Liberty in an arbitrary manner'

[4]. This protection extends to all persons without distinction: ‘it covers both adults and minors [...] and both those who are at liberty and those who are already detained’ [4].

It is crucial to distinguish the right recognised in Article 6 from the right to freedom of movement: this right refers to the prohibition of arbitrary arrests or those without the requisite safeguards; therefore, it has no bearing on restrictions on freedom of movement or limitations on the freedom of movement of certain persons (for example, members of the military), which would rather derive from Article 2 of Protocol No. 4 [5]. Within the European Union, it is equally important to draw a clear distinction between the right to Liberty and the right to freedom of movement and residence as an integral part of citizenship.

The safeguards surrounding this right are not limited to the mere prohibition of arbitrary deprivation of Liberty. Article 5 of the ECHR, fully incorporated by reference to Article 6 of the Charter, provides for a range of procedural rights that form part of the provision’s substantive content. Thus, every person arrested must be informed of the reasons for his arrest as soon as possible and in a language he understands, and every person arrested or deprived of liberty [...] shall be brought without delay before a judge or other authority empowered by law to exercise judicial powers [4]. The right to habeas corpus is also enshrined: every person deprived of their liberty through detention shall have the right to bring an application before a judicial body, so that it may rule within a short period on the lawfulness of their deprivation of liberty and order their release if it is unlawful.

security reasons, passengers may be detained at security checkpoints for a limited time. This has been established in the case law of the European Court of Human Rights, which permits individuals to be detained, provided that the detention is strictly limited to the time necessary to complete the relevant formalities [6]. The length of detention varies depending on the circumstances; in some cases, an 11-hour detention may be permitted¹, whereas in others, five hours is considered too long².

2.2.1.2 The security dimension: a concept that is difficult to define

The second term in the statement—security—raises interpretative issues that were the subject of debate within the Convention that drafted the Charter. As the commentary notes, ‘there were certainly some voices within the Convention, such as those of Friedrich (representative of the European Parliament) or Rodríguez Bereijo, who advocated the removal of the security dimension from this provision on the grounds that it was unclear what specific guarantees this (apparent) right entailed in practice’ [4]. The established legal conclusion is that security has no specific normative content distinct from the element of freedom. It merely highlights its indissoluble link with freedom and requires protection against arbitrary freedom restrictions.

The European Court of Human Rights has extended the protection afforded by Article 6 beyond the borders of the State where the deprivation of liberty takes place: ‘an arrest carried out by the authorities of one State on the territory of another State without the latter’s consent is capable of affecting the right to liberty and security of the individual concerned’. However, it must be proven that the authorities of the State acted in violation of the sovereignty of the State in which the person concerned was located and in violation of the rules of international law.³

The case law of the European Court of Human Rights has emphasised with particular firmness the superior status of this right: ‘we are dealing with a right which, from its earliest case law, has been

¹ECHR 18603/12 Case of O.M. and d.s. v. Ukraine.

²ECHR 53659/17 Case of Kasparov v. Russia

³ 2003, Öcalan, paragraph 88 et seq., upheld in 2005 by the Grand Chamber

regarded by the European Court of Human Rights as an inalienable right in a democratic society [...] which today continues to retain full relevance of the first order.’ This is particularly true at a time such as the present, when a dangerous, restrictive conception of the right to liberty is spreading in some States—including within the European Union—in favour of supposedly necessary security measures to combat the real risks posed by international terrorism and organised crime’ [7].

2.2.2 III. Article 8: Data Protection as an Autonomous Fundamental Right

Article 8 of the Charter establishes that every person has the right to the protection of their personal data, that such data must be processed fairly, for specific purposes and on the basis of the consent of the data subject or on another legitimate ground provided for by law, that everyone has the right to access and rectify their data, and that compliance with these rules shall be subject to the supervision of an independent authority. The enshrinement of the right to data protection as an autonomous fundamental right, distinct from the right to privacy under Article 7 [8], constituted a novelty in international law [9], given that no previous international instrument had conferred upon it independent constitutional status at the supranational level. As from this development, the inclusion of a specific article on data protection (which has its roots in the 1978 Spanish Constitution) demonstrates the importance that European institutions attach to data protection. A Data Protection Directive was already in place, followed by the General Data Protection Regulation (GDPR) and Directive 2016/680 on the use of police data for law enforcement purposes.

The distinction between Articles 7 and 8—privacy and data protection—has been the subject of intense academic debate. Vogiatzoglou and Valcke note that ‘the two rights can also be seen as distinct, with one being broader than the other. The right to respect for private and family life encompasses the protection of aspects of the private sphere that are irrelevant to data processing, whereas the right to the protection of personal data concerns all information relating to an identified or identifiable person, whether or not it relates to their private life’. Despite this distinction’s theoretical clarity, the Court of Justice of the European Union’s practice has often been confusing: ‘through its increasingly extensive case law, the Court of Justice of the European Union continues to examine measures that interfere with the rights to privacy and data protection by referring to both rights together’ [9].

One of the most fruitful doctrinal debates surrounding pits the prohibitive conception against the permissive conception of the right to data protection. According to the prohibitive interpretation, data protection as a prohibitive right provides a general prohibition on the processing of personal data laid down in Article 8(1) of the Charter, while the provisions that follow under Article 8(2) and (3) of the Charter provide the exceptions to this prohibition [9]. The permissive approach, by contrast, considers that the processing of personal data is permitted in principle and that the right guarantees a system of control and transparency over such processing. Given the subsequent development of the relevant legislation, the use of data is permitted in many cases, except in a few specific instances. In our case, the use of data is permitted by law enforcement authorities to safeguard public security.

It must be acknowledged that this controversy has direct practical consequences regarding when an interference with the right occurs and when such interference may be justified. ‘defining data protection as a prohibitive or permissive right leads to divergent determinations of what constitutes an interference with the right to data protection, and of how the conditions set out in the Charter regarding its justifiable interference are applicable’ [9], especially when we’re talking about metadata

In practice, the Court of Justice of the European Union has adopted an approach that is closer to a restrictive interpretation of the law. It considers that ‘an interference with the right arises as soon as

the measure under scrutiny falls within the scope of the processing of personal data'. The Court of Justice of the European Union consistently points out that data processing activities, such as the storage, access, or use of data, fall within the scope of Article 8 of the Charter regardless of the nature of the information contained therein and must therefore comply with the requirements set out therein⁴. However, the Court frequently resorts to a joint analysis of Articles 7 and 8 when examining the justifiability of interferences, which does not allow the right to data protection to reach its full potential as an autonomous right.

2.2.3 IV. The core of rights: The Essence of Article 52(1) of the Charter

2.2.3.1 1. The 'essence' clause as a limit on the limits

Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms recognised therein 'must be provided by law and respect the essence of those rights and freedoms'. This provision is directly linked to Articles 6 and 8 because it sets the maximum threshold of permissible interference in both Articles. The Court's statements show that, as legal norms, the fundamental rights protected by the Charter must not only be treated as principles capable of being weighed and balanced against other competing principles. Furthermore, these rights can generate rules that must be applied in a binary manner (all or nothing)⁵.

The codification of the essence in the Charter represented a significant contribution by EU law to European and international fundamental and human rights law^[10], precisely because other instruments such as the European Court of Human Rights do not expressly include it and it has remained a jurisprudential construct. By contrast, the Charter elevates it to the highest rank of a positive text.

With regard to Article 6, the European Court of Human Rights had already recognised the existence of the very essence of Article 5(4) of the ECHR in the context of the deprivation of liberty of a person with a mental disability, noting that although mental illness may restrict or alter the exercise of that right, 'it cannot justify undermining the very essence of the right'⁶. This approach will prove decisive: the essence acts as an absolute barrier that cannot be breached by even the most compelling reasons of Public interest.

For Ojanen, the Court of Justice has adopted a position analogous to that of the German Federal Constitutional Court in its most significant judgments—Digital Rights Ireland and Schrems—that 'not even public interests of the utmost importance can justify a limitation of the absolutely protected core of private life; the balancing of interests under the principle of proportionality is not at issue'^[10].

The Court of Justice's case law on the essence of Article 7 began with the Digital Rights Ireland judgment, in which the Court held that the Data Retention Directive did not undermine the essence of the right to privacy 'because the directive does not permit the acquisition of knowledge of the content of electronic communications as such'⁷. This distinction between content and metadata as a criterion for determining whether the essence is affected was the subject of strong doctrinal criticism. Maja Brkan notes that 'the Court appears to perceive intrusion into the essence as the most serious of all

⁴ Joined Cases C-293/12 and C594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI: EU:C:2014:238, para 53; Opinion 1/15 [2017] ECLI:EU:C:2016:656, paras 133, 149; Case C-207/16 Ministerio Fiscal [2018] ECLI:EU:C:2018:788, para 133.

⁵ ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner

⁶ ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner

⁷ ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner

possible intrusions and access to the content of data as an expression of such intrusion, but unfortunately does not explain why the acquisition of knowledge of the content could not also be classified as a particularly serious interference’[11].

The Schrems judgment marked a qualitative turning point. The Court declared that ‘legislation which allows public authorities to have generalised access to the content of electronic communications must be regarded as compromising the very essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter’.

Ojanen emphasises that this statement ‘brings the concept of the essence of fundamental rights to life, in the clearest possible terms from a judicial body’[10]. This implies that the essence functions as a rule, not as a principle: it precludes any balancing of interests, however relevant the objective pursued may be.

However, Brkan points to a methodological inconsistency in Schrems: the Court concludes that there is an interference with the essence after having already determined that the measure does not pass the proportionality test. According to the author, ‘the application of the principle of proportionality excludes the possibility of interference with the essence and only allows one to conclude that the measure constitutes a justified or unjustified (dis)proportionate interference’ [11]. The essence and proportionality operate on different levels: the former is a preliminary categorical test, and the latter is a judgement of degree that is only applicable if the essence has not been undermined.

2.2.3.2 The essence of the right to data protection: a poorly conceived minimum standard for data protection

The Court of Justice’s caselaw construction of Article 8’s essence has proved, if anything, more problematic than that of Article 7. In Digital Rights Ireland, the Court held that the essence of the right to data protection was not affected because the Directive required compliance with ‘certain principles of data protection and data security’ [11]. Brkan strongly criticises this approach: ‘the Court narrows the core of the fundamental right to data protection down to minimum standards of data protection and data security [...]. This approach turns the essence of this right into a minimum rather than a maximum standard and sets a low threshold for compliance with the Essence [11]. The author concludes that ‘viewing the essence of a fundamental right as a minimum standard deprives this concept of its purpose and misinterprets its role in the landscape of fundamental rights protection’ [11].

Vogiatzoglou and Valcke share this criticism and propose an alternative approach: ‘We suggest that the essence of the right to the protection of personal data should not be defined by reference to the elements of Article 8(2) and (3) of the Charter as organisational measures in accordance with the case law of the Court of Justice, but rather by virtue of the higher values that the law seeks to serve, such as human dignity and autonomy’. They added that “when an individual is rendered completely powerless or deprived of their autonomy, the essence of the fundamental right to the protection of personal data is violated” [9].

2.2.4 V. Articles 6 and 8 in the context of mass surveillance: an unresolved dialectic

The area where the tension between Articles 6 and 8 is most evident is that of electronic surveillance and the widespread retention of communications data. By protecting liberty, Article 6 implicitly guarantees that the State cannot subject individuals to controls and surveillance which, without physically depriving them of their liberty, produce an equivalent inhibitory effect on the exercise of their rights. Article 8 adds specific protection against data processing that allows the creation of individual profiles or the mapping of people’s private lives.

Brkan warns that the distinction between content and metadata as a criterion for defining the essence of privacy is becoming increasingly artificial: ‘Advocate General Saugmandsgaard Øe rightly demonstrates that access to metadata can sometimes have the same or even a greater impact on the privacy of users of electronic communications than content data’ [11]. Metadata can reveal political affiliation, religious beliefs, health status, or behaviour with the same or greater precision than content. For this reason, the Court of Justice in *Tele2 Sverige* recognised that metadata-based profiling ‘is no less sensitive, from the point of view of the right to privacy, than the actual content of communications’ [11]. Consistency would require drawing the relevant constitutional conclusions from this finding: If metadata is as sensitive as the content, its mass retention should also be capable of undermining the very essence of the right.

2.2.5 Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law

Recently (May 2026), the Council of Europe published the Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, which will ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law [12].

The general obligations of this legal framework include the protection of human rights, respect for the rule of law, and the integrity of democratic processes. Although this is not a new concept, given their position in the text and the emphasis placed on them, these elements have become key to the development of artificial intelligence systems in Europe.

It then sets out a series of principles that must be observed in the lifecycle of artificial intelligence systems, namely: human dignity and individual autonomy, Transparency and oversight, Accountability and responsibility, Equality and non-discrimination, Privacy and personal data protection, Reliability and Safe innovation.

Except for the last two, all of these are already covered by the ethical guidelines on trustworthy artificial intelligence, which we have set out in the section on ethics in this document. The last two are not explicitly addressed in the ethics section, but it is certainly in the spirit of the entire process of developing the artificial intelligence systems of the BAG-INTEL project. Reliability refers to the implementation of measures that promote the reliability of artificial intelligence systems and confidence in the results they produce, as well as security and quality measures, whereas ‘safe innovation’ refers to the establishment of safe environments for development, testing, and experimentation under the supervision of competent authorities.

Both principles are addressed through the project’s activities and the analysis of its ethical and legal frameworks. This is achieved through the active collaboration of all parties and end users.

3 ETHICS

From the outset, we have incorporated an ethical assessment into Project BAG-INTEL. This evaluation by design [13] enabled us to design the entire scanner while considering its ethical implications, thereby establishing various strategies to minimise any negative impacts.

To conduct an ethical analysis of the AI components of BAG-INTEL, we will use the ethical guidelines for Trustworthy AI of the European Commission as the basis for our assessment [2]. This document is regarded as a precursor and benchmark for many other ethical guidelines in the field of practice. Furthermore, the project is limited to the European context, both in terms of the participating partners and the location of the use cases. Therefore, we will focus on the following four principles: Respect for human autonomy, Prevention of harm, Fairness, and Explicability. These four principles can be ensured with seven key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability.

The guidelines consider the respect of human autonomy in three main areas. The artificial intelligence system must respect fundamental rights. I.e., AI has a dual nature: it can protect and infringe on people's fundamental rights. On the one hand, it can be a powerful tool that helps citizens manage their personal data or improves access to education. However, given its enormous scope and capacity, it can also pose a threat to those very same rights. Therefore, before developing any AI system that may pose a risk, its impact on fundamental rights must be assessed. This assessment must determine whether such risks can be mitigated or justified within a democratic society, and to receive external feedback on potential infringements, channels must be established. In the second area, human autonomy, users must be able to make informed and autonomous decisions regarding AI systems. This means that they must have the necessary knowledge and tools to understand how these systems work and, ideally, be able to question them. However, the text warns that AI can influence human behaviour in subtle and difficult-to-detect ways, using mechanisms such as manipulation, deception, or conditioning. Therefore, user autonomy must be a central principle in the design of any system. A key right in this area is the right not to be legally affected by fully automated decisions without human intervention. Finally, human oversight means maintaining human control over AI is essential to prevent adverse effects. Three models of oversight are proposed: human in the loop, which allows intervention in every decision; human on the loop, which oversees the design and overall operation; and human in command, which assesses the overall impact of the system. As a general rule, the less scope there is for human oversight, the more comprehensive the testing and the stricter the governance.

The second requirement is technical robustness and safety. As described in the HLEG guidelines, five points must be considered as robust and reliable. Technical robustness is the foundation of reliable AI. Systems must be designed with a risk-preventive approach, operating predictably and minimising unintended harm, including changes to their environment or interactions with hostile external agents. Attack resilience and security are understood to mean that AI systems must be protected against vulnerabilities and attacks that may target the data (data poisoning), the model (model leakage), or the infrastructure. A successful attack can alter the behaviour of the system or render it inoperable. Potential malicious or unintended uses of the system must also be considered. The third is the contingency plan and general security. Systems must have fail-back mechanisms, such as switching to rule-based procedures or requesting human intervention. Minimising unintended consequences and assessing risks according to the system's capabilities are essential. The greater the anticipated risk, the more rigorous the security measures. Accuracy is considered when an artificial intelligent system is capable of making accurate classifications, predictions, and recommendations. A well-defined development and evaluation process helps minimise errors. Where errors are unavoidable, the system

must be able to indicate their likelihood. Accuracy is particularly critical when the system directly affects people's lives. Finally, reliability and reproducibility are consistent and reproducible under the same conditions. This enables researchers and policymakers to verify its behaviour, detect faults, and prevent unintended harm.

The third point to be addressed is privacy and data management as essential elements of ethical AI, structured around three aspects: privacy and data protection. Artificial intelligent systems must guarantee privacy throughout their entire lifecycle, both for the data initially provided by the user and for that generated during their interaction with the system. Given that AI can infer sensitive information, such as sexual orientation, religion, or political ideology, the data collected should not be used to discriminate against people in an unfair or unlawful manner. The quality and integrity of data are crucial to the proper functioning of AI. Data may contain biases, errors, and inaccuracies that must be corrected before training the system. Furthermore, data integrity must be protected, as introducing malicious data can alter the behaviour of the system. The entire process—from planning to deployment—must be documented and tested, even when the system has been procured externally. Access to data is crucial for the use of AI. Organisations handling personal data must establish clear protocols governing who can access it and under what conditions. Only suitably qualified staff with a legitimate need must be authorised to access individual data.

As a fundamental requirement in artificial intelligence systems, the requirement for transparency is closely linked to the principle of explainability. It revolves around three key aspects. Traceability: For an artificial intelligent system to be truly transparent, all the elements involved in its operation must be properly documented. This includes the datasets used, data collection and labelling processes, algorithms employed, and system decisions. Comprehensive documentation enables the identification of the causes behind erroneous decisions and, consequently, prevents future failures. Furthermore, traceability is an essential prerequisite for both external auditing of the system and explaining its behaviour in an understandable manner. Explainability encompasses two dimensions: technical and human. On the one hand, automated decisions must be understandable and traceable by people. Human decisions associated with the system must also be explained, such as the chosen areas of application or the reasons for deploying it. The text acknowledges an inherent tension between explainability and accuracy: improving one may involve sacrificing the other; thus, it is necessary to strike a balance depending on the context. When an AI system has a significant impact on people's lives, a clear and timely explanation of how it reached its decision must be possible. Such an explanation must be tailored to the recipient's level of knowledge, whether they are a member of the Public without technical training, a regulator, or a specialist researcher. Furthermore, the business model must be transparent, explaining how the system influences organisational processes and why it has been chosen for use. Communication artificial intelligence systems must identify themselves to users, who have a fundamental right to know that they are not interacting with a human being. Users must be given the option to choose human interaction. Where necessary to ensure that fundamental rights are respected. Finally, the system's capabilities and limitations must be communicated clearly, honestly, and in a manner that is appropriate to the type of user and the context of use.

Integrating inclusion and diversity into every stage of the AI systems' lifecycle is essential to achieve trustworthy AI. This principle is closely linked to equity value and revolves around three key pillars.

The first step is to eliminate unfair biases. The datasets used to train and operate artificial intelligence systems contain historical biases, incomplete data, or flawed governance models. Perpetuating these biases can lead to discrimination—direct or indirect—against certain groups, worsening social marginalisation. The intentional exploitation of consumer biases or anticompetitive practices, such as price homogenisation through collusion, can also cause harm. To combat this, it is necessary to identify and eliminate biases during the data collection phase, establish transparent oversight processes for

algorithmic development, and promote the hiring of individuals with diverse backgrounds in terms of origin, culture, and discipline.

Accessibility and universal design artificial intelligent systems, especially in the consumer services sector, must be user-centred and accessible to everyone regardless of age, gender, abilities, or personal characteristics. Special attention must be paid to accessibility for people with disabilities. Rather than adopting one-size-fits-all, inflexible solutions, systems should follow the principles of Universal Design, adapting to the widest possible range of users and complying with current accessibility standards. This ensures equitable participation in technology-mediated activities.

Finalise with stakeholder participation. To develop truly trustworthy AI systems, all stakeholders who may be affected—directly or indirectly—throughout the entire system lifecycle should be consulted. It is important to regularly gather feedback, even after implementation, and to establish stable mechanisms for long-term participation. This includes ensuring that workers are informed and can actively participate in AI adoption processes within organisations. In conclusion, building trustworthy AI requires a proactive approach that combats algorithmic bias, makes technology accessible to all, and maintains an ongoing dialogue with society.

The sixth key point is the social elements of AI use. The text addresses the responsibility of AI systems towards society as a whole, living beings, and the environment, beyond just their direct users. Sustainable and eco-friendly AI. Although AI can help solve major social challenges, its development and use must be environmentally friendly. It is necessary to assess resource and energy consumption throughout the system's entire life cycle—including its supply chain—and always opt for less polluting alternatives.

Social Impact. The widespread presence of AI in areas such as education, work, and entertainment can transform our perception of social relationships and affect people's physical and mental well-being. Its positive and negative effects must be closely monitored.

Society and democracy. The impact of AI must also be assessed at the institutional and democratic levels. Its use in political and electoral processes requires careful consideration to protect democratic values.

Ultimately, truly trustworthy AI must be geared towards the benefit of all humanity, including future generations, while respecting the environment and social structures.

Accountability is a fundamental requirement for ensuring trustworthy AI and serves as an essential C to fairness principles. It involves establishing clear mechanisms to ensure that both AI systems and their outputs can be monitored and evaluated at every stage of their lifecycle.

Auditability. Artificial intelligent systems must be able to be evaluated in terms of their algorithms, data, and design processes. This does not mean that all commercial or intellectual property information must be publicly available, but it does mean that internal and external auditors can conduct evaluations and publish their reports. Independent auditing is essential in applications that affect fundamental rights or security to ensure trust in the technology.

Minimisation and reporting of the negative impacts It is essential to identify, document, and reduce the potential negative impacts of AI systems, especially for those directly or indirectly affected. Channels must exist to report unintended consequences, along with mechanisms to address them. Furthermore, those who report legitimate issues—such as whistleblowers, nongovernmental

organisations (NGOs), or labour unions—must be afforded adequate protection. Impact assessments, such as red teaming or Algorithmic Impact Assessments, are valuable tools both before and during the development and use of these systems, and they must be proportionate to the risk they pose.

Managing compromises and conflicts the simultaneous application of all ethical requirements can produce tensions and conflicts. These must be addressed in a reasonable and methodical manner by identifying the values at stake and explicitly assessing each decision's ethical risks. If no ethically acceptable solution exists, the development or use of the system should not proceed in that form. Any decision on how to resolve these tensions must be duly reasoned, documented, and subject to the responsible party's ongoing review.

Redress mechanisms. Accessible mechanisms must be in place to ensure adequate redress when unjust Harm occurs. The possibility of obtaining redress when something goes wrong is key to building trust in AI. Special attention must be paid to vulnerable individuals and groups to ensure that they can access these mechanisms.

In conclusion, AI accountability requires transparency, protection against harm, and clear avenues for redress—elements that are indispensable for building truly trustworthy systems.

Within this framework, we will conduct an ethical analysis of the use of artificial intelligent systems using the same tool as in deliverable 2.1. Always from a pragmatic perspective [14] and tailored to the context in which the project will be carried out. On this occasion, and in line with the philosophy of the Digital Omnibus on AI Regulation Proposal, we will provide stakeholders with a more concise and easier-to-complete questionnaire based on the one proposed by the HLEG [2]. The Trustworthy AI Assessment Checklist is a comprehensive document designed for AI systems that are currently on the market or are about to be launched, which is not the case for the BAG-INTEL prototype.

The questionnaire was sent to the partners involved in the develop of artificial intelligence systems in BAG-INTEL. No particular adaptation of the list was needed to GenAI because none of the partners has used these artificial intelligence systems to develop the tools.

The final version of the questionnaire can be found in Appendix A.

3.1 ETHICS ASSESSMENT

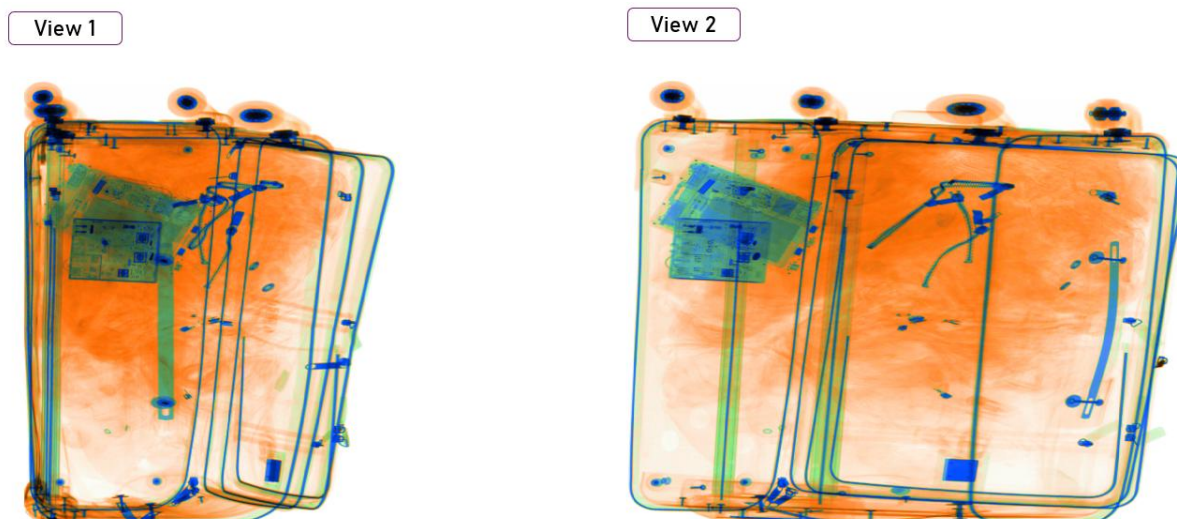
Using our analysis and partners' feedback, we will assess compliance with each of the HLEG's ethical principles.

3.1.1 Human agency and oversight

At BAG-INTEL, given the risks associated with the use of AI systems at borders, we have taken great care to ensure that decision-making is not automated, [15]. To avoid such situations, AI analyses predicting smuggling scenarios will serve solely as a basis for law enforcement agencies (LEAs) to improve their operations, providing an alert system. This alert system will be used to carry out an initial luggage screening, with the final decision on whether or not to inspect the luggage remaining in the hands of the LEAs.

Therefore, the x-ray images will be analysed by an object recognition system (in this case, for drugs, tobacco, and money), thereby improving the examination of the X-ray images and issuing an alert regarding the likelihood that these objects are among those sought by the LEAs. Next, we look at some examples of images captured by x-ray machines.

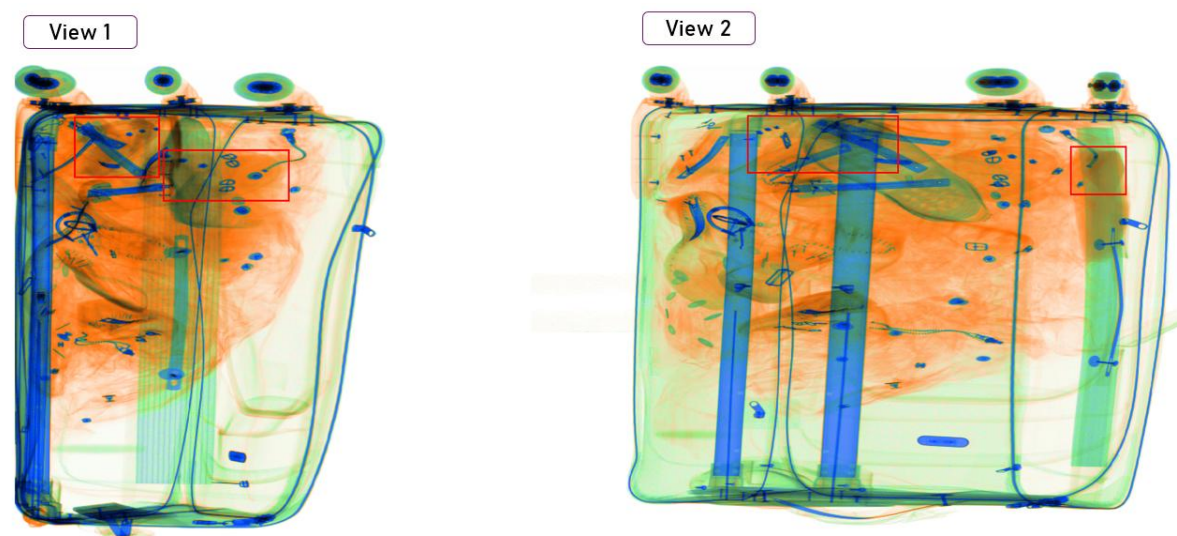
Figure 1: Empty



These are the images from the scanner that the LEAs will have to analyse. In this case, the system considered it as a low risk.

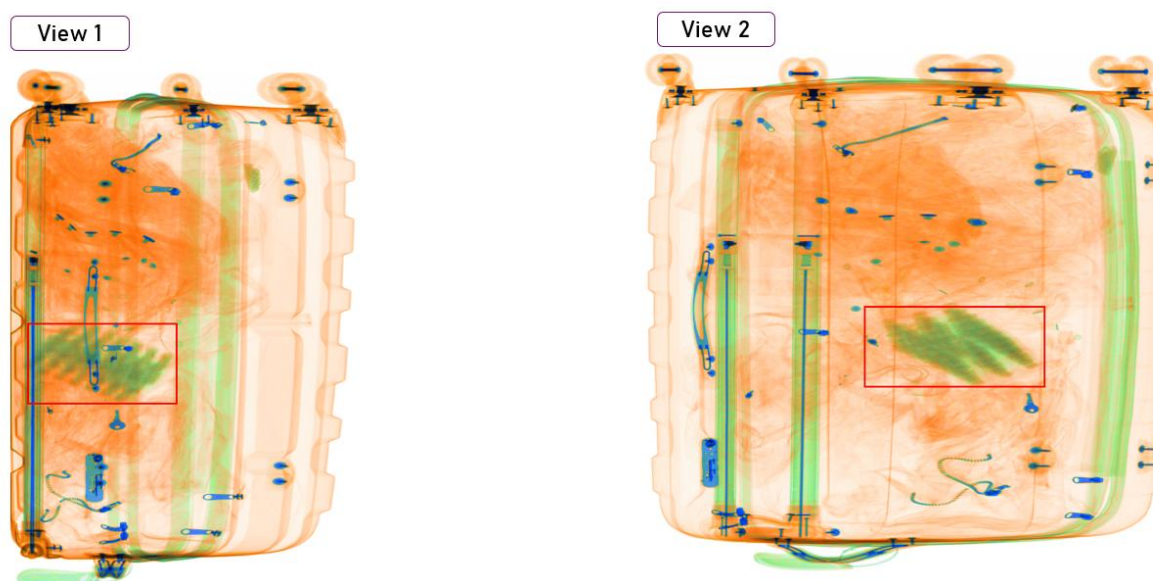
The next figure shows a case in which the artificial intelligence system detects small packets of cocaine. The system signal is shown with a red square, where is the possible trafficking, giving LEAs information where they must focus, increasing the detection task and saving time. This is only a signal. The person is the one to analyse the results and make the final decision.

Figure 2: Cocaine



The same applies to blister packs, which the AI system flags as a potential smuggling alert and then examines by the LEAs.

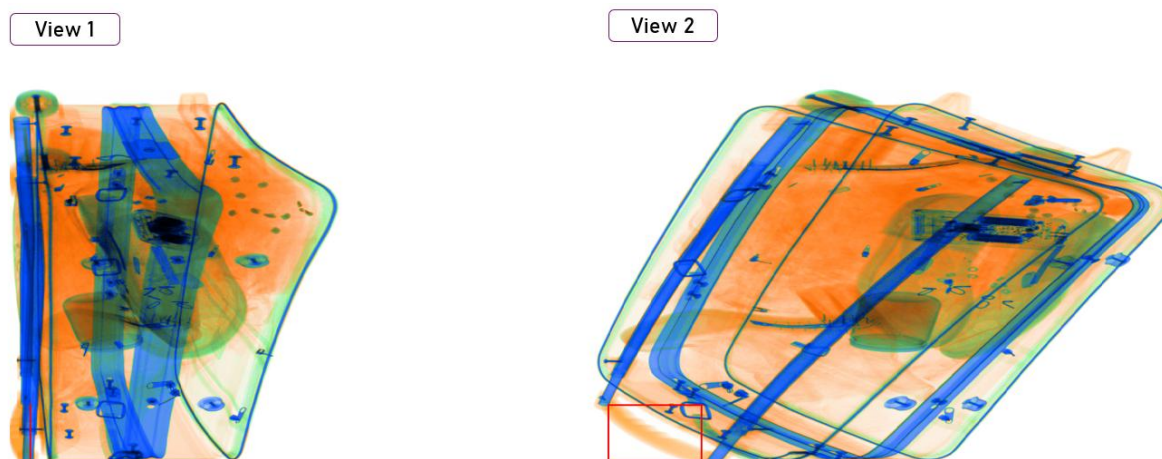
Figure 3: Blisters



The alert system is not immune to false positives. This possibility must be considered because the frequency of false positives can disrupt the work of the authorities, causing significant delays in inspections. The tool has been designed with this situation in mind, always upholding the principle of human oversight while striking a balance between effectiveness and practicality.

Fig 4 identifies a suitcase's handle is identified as a contraband item. The customs officer can quickly spot the AI analysis error in the image displayed on the app and make the appropriate decision without having a significant impact on their work.

Figure 4: False alarm



The second application of AI in the project is risk analysis to predict which customs inspections flights should focus on. This machine learning model uses flight data and intelligence information to perform an initial screening of flights of interest. A similar situation arises here. The LEAs receive the information from the system and are the final decision-makers regarding which flights are targeted for smuggling prevention.

Figure 5: Flight tracking

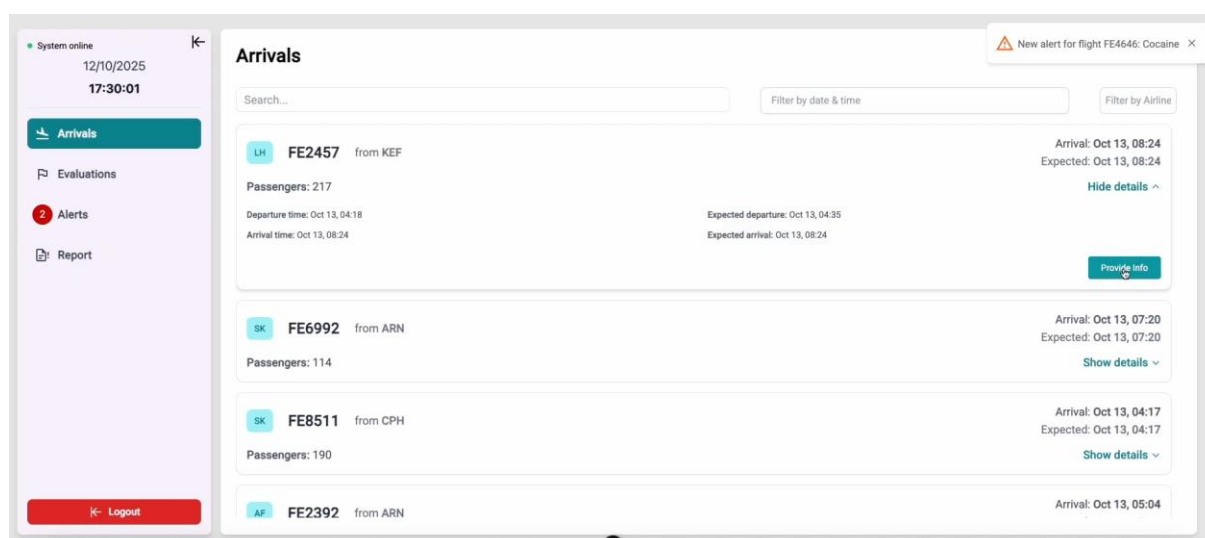
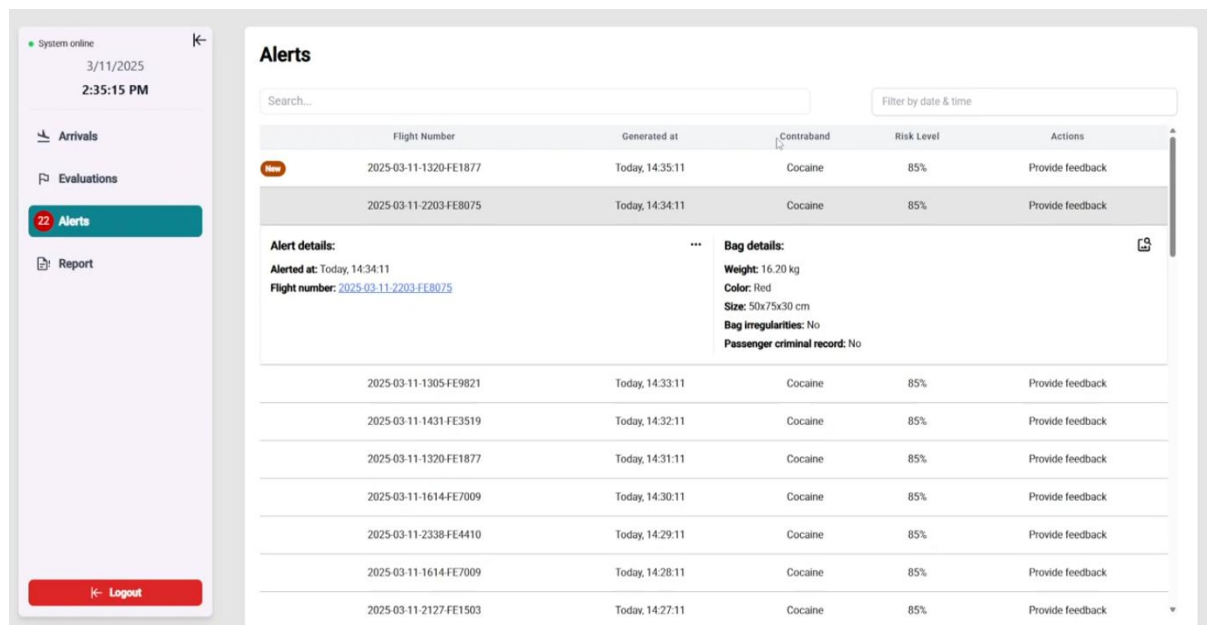


Figure 6: Flight Alerts



Flight Number	Generated at	Contraband	Risk Level	Actions
2025-03-11-1320-FE1877	Today, 14:35:11	Cocaine	85%	Provide feedback
2025-03-11-2203-FE8075	Today, 14:34:11	Cocaine	85%	Provide feedback

Alert details:
 Alerted at: Today, 14:34:11
 Flight number: [2025-03-11-2203-FE8075](#)

Bag details:
 Weight: 16.20 kg
 Color: Red
 Size: 50x75x30 cm
 Bag irregularities: No
 Passenger criminal record: No

The app contains all flight details and receives alerts for items detected by the AI analysis, along with information on the luggage being tracked. In this way, law enforcement officers are ultimately able to decide which luggage is screened and which is not, retaining control over the final decision at all times while taking the AI analysis into account.

3.1.2 Technical robustness and safety

In the specific case of project BAG-INTEL, there are no major issues regarding the principles of robustness and security. The project has not anticipated any potential external attacks on the system. Access to the AI systems and the application is restricted to a very small group of users through a login process. We cannot consider it a vulnerable system.

The databases that feed the system also have restricted access, with login controls in place.

Focusing on internal security, we can point out that any errors that may arise from the use of the prototype are not of particular significance. Any 'incorrect results' can always be easily reversed by authorised personnel should they prove to be insufficiently valid.

The system's accuracy will be improved using machine learning, which learns from positive and negative results. As this model is still under development, it has been trained on a limited number of cases. It will improve as the knowledge base grows through use. The system's accuracy (the number of positive cases out of the total number of suitcases inspected) and performance metrics are assessed at the time of submitting this deliverable.

In any case, as noted in the first principle, human oversight of the results is very high, and errors are easily rectified through LEA intervention.

3.1.3 Privacy and Data Governance

The BAG-INTEL project uses data in three distinct parts: luggage identification, baggage risk analysis, and, finally, future risk analysis. The first part uses photographs of suitcases and passengers taken from the airport's CCTV cameras. To avoid privacy issues, travellers' faces, if they appear, will be blurred to prevent identification. The use of data for analysing the probability of the presence of contraband items and for preassessing flights requiring special attention does not involve the use of personal data.

Although the system can be fed with police data from actual investigations, this option has not been chosen in the use cases. The databases of the police have not been integrated into the system for the purposes of BAG-INTEL's activities. The project has successfully addressed a long-standing issue relating to the differing applicable regulations, which the European legislator should resolve in the future [16].

In the case of PNR data, the decision was made to use synthetic data. To this end, the categories of data collected under the PNR regulations were analysed, selecting only those categories relevant to the project; from there, synthetic data were generated to feed into the system.

Data governance is covered in D.1.3. Please refer to this document for information about data governance about AI.

3.1.4 Transparency

The principle of transparency is often difficult to implement and has several dimensions, including technological and sociologic dimensions. The technological aspect presents two main challenges. The first relates to the traceability of the results produced by the artificial intelligence system and the decision-making traceability—known as the black box dilemma. Decision-making with machine learning is so complex that according to experts, it is impossible to determine why the system makes a particular decision. Human oversight in the decision-making process outlined in the first principle can address this challenge. Certain outcomes of machine learning and neural networks may be difficult—or even impossible—to explain. Therefore, project BAG-INTEL has sought to minimise this effect through more intensive human oversight and by designing a system with built-in human oversight from the outset.

The next issue regarding transparency—also from a technological standpoint—is the difficulty in accessing the source code underlying decision-making since intellectual property rights protect the development of these tools. Trade secrets pose a challenge when investigating them to ensure that this principle is upheld.

It differs in terms of the human agents. Thus, a key aspect of transparency is providing information [17] about the use of artificial intelligence in baggage screening. There are various ways to provide this information. If available, it can be posted on the airport's website and in its app. It can also be displayed at baggage claim carousels, in baggage claim areas, etc.

Specifically, in project BAG-INTEL, AI developers have focused on four key areas: 1) measures to ensure traceability, 2) evaluating why the result can be understood, 3) informing end users of the criteria and reasoning behind the artificial intelligence system's decision, and 4) clearly communicating the characteristics, limitations, and potential shortcuts taken by the AI system to end users. Therefore, a great deal of effort has been made to ensure prospective transparency, which we can consider to be assured by the decisions implemented within the project and the measures taken regarding the

provision of information to participants, as well as retrospective transparency, which can be seen to be guaranteed through the monitoring of decision-making, although traceability in the case of machine learning systems can be more complicated [18].

Understanding the outcomes is not too complicated. The system provides interpretable outputs, such as risk levels and key indicators contributing to recommendations. The officer makes the final decision because it is only an assessment of risk, ensuring that the output from the artificial intelligence system is reliable. The end user engaged actively. LEAs have helped in the selection of risk indicators and contributed to the design of the scanner with their knowledge. As the officer makes the final decision, they understand how the system works and how it makes the decisions based on the risk assessment and the officer's observation. Regarding the reason and criteria behind the BAG-INTEL design, officers can see the main sources of bag risk assessment. More detailed information can/should be provided in the final version of the product, but it is not within the scope of the project to provide this information. BAG-INTEL has several use cases, and the officers had end-user training, and they were informed about the characteristics, limitations, and potential shortcomings of the artificial intelligence systems in those meetings. They were also aware of the limitations of data use and the risks associated with artificial intelligence systems.

3.1.5 Diversity, non-discrimination, and fairness

According to the ethical guidelines for trustworthy AI, these principles have three main objectives: 1) avoidance of unfair bias, 2) accessibility and universal design, and 3) stakeholder participation.

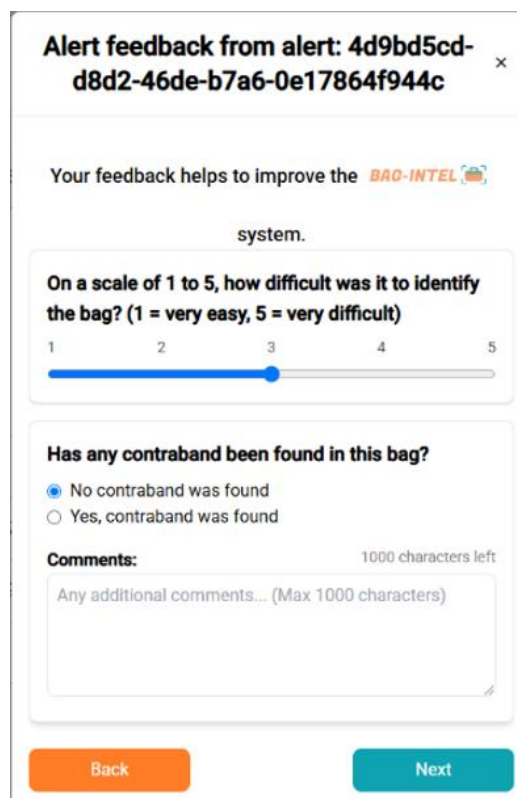
Preventing unfair discrimination is an objective of BAG-INTEL. Particular care has been taken with the databases used to prevent algorithmic discrimination and unfair treatment [19]. To this end, the experience of end-users has been taken into account to minimise data and prevent excessive noise in the datasets, thereby avoiding discrimination; the use of reliable sources of information; and the application of their expert knowledge in decision-making.

Accessibility and universal design focus on consumer products. This is not the case with Project BAG-INTEL, where the system is used exclusively by law enforcement agencies.

Although its use is strictly limited to end-users, its design has taken into account the wide range of security personnel who may be involved in its operation, from private security services to law enforcement agencies.

The design of the app is very basic and user-friendly, ensuring that it is easy and straightforward to use. Training courses have also been provided to ensure that there are no issues with its use, whether in terms of inputting information into the system—including alerts and the detection of false positives—or tracking the suitcase.

Figure 7: App Alert Feedback



Alert feedback from alert: 4d9bd5cd-d8d2-46de-b7a6-0e17864f944c

Your feedback helps to improve the **BAG-INTEL** system.

On a scale of 1 to 5, how difficult was it to identify the bag? (1 = very easy, 5 = very difficult)

1 2 3 4 5

Has any contraband been found in this bag?

☒ No contraband was found

☐ Yes, contraband was found

Comments: 1000 characters left

Any additional comments... (Max 1000 characters)

Back Next

Fig 7 shows an example of how the system learns using information provided by an expert, who simultaneously monitors the artificial intelligence system's output, assessing its accuracy and reliability. In this case, the drug test result was negative.

Figure 8: LEAs' app review and submission of information

Alert feedback from alert: cabb962d-2ca4-4403-be61-3c9e84d894f6 ×

Review & Submit

Identification Difficulty: 3

Contraband Found: Yes

Contraband Details:

- **Category:** Drugs
- **Substance:** cocaine
- **Amount:** 2kg
- **Packed in:** baggage
- **Concealing Method:** hidden

Comments:

Suspect detained

Name this Feedback:

Enter a name for this feedback

Back

Submit

Figure 8 shows an example of a positive drug test result and the summary received by security personnel, including an assessment of the difficulty, details of the positive test result, and further information on the smuggling method. As in the previous case, the result can be assessed and additional information provided to the system for processing, with the final assessment always being performed by a human, as required by the first ethical principle of the guidelines on trustworthy AI.

Figure 9: Passenger Anonymization

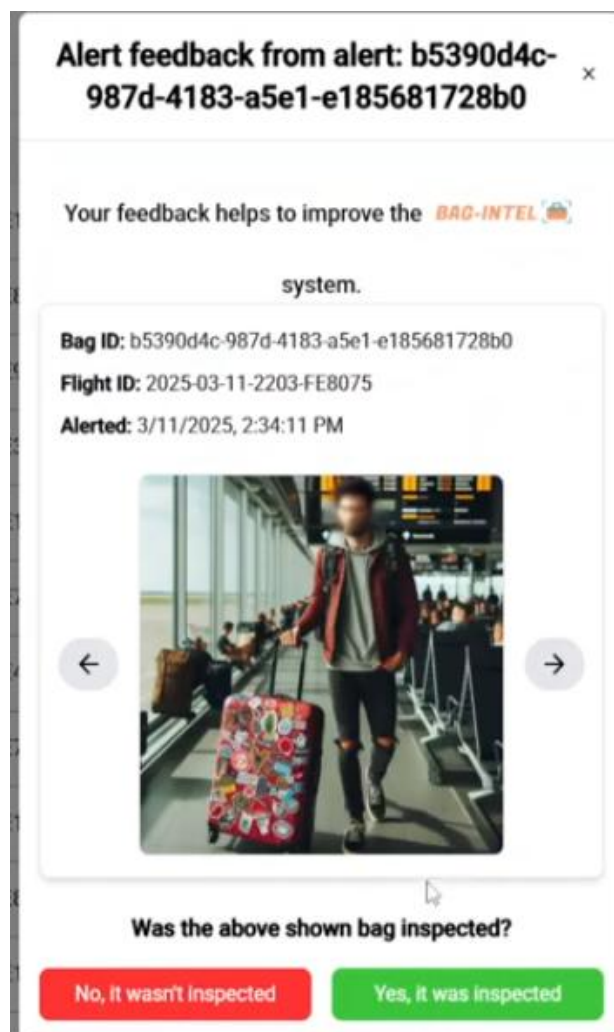


Fig 9 shows an example of luggage tracking within the app. As the aim is to focus solely on the suitcase, the subject's face and identifying features are blurred to remove irrelevant information. The final decision on whether to inspect the luggage rests with the customs control authority.

BAG-INTEL has placed great emphasis on ensuring that the design is intuitive and always facilitates the use of the system, bringing together the various stakeholders who may be involved in its use.

Finally, partners from law enforcement agencies have played an active role in designing the scanner. First, they have been involved in analysing the scenarios we might encounter when designing the scanner, including the methods they use to detect contraband, and the key factors involved in its detection.

In the creation of synthetic data, they have been instrumental in selecting the important data categories and in using data that closely resembles the reality they encounter in their security work.

They have also been involved in the development and testing of the artificial intelligence system's results.

3.1.6 Societal and environmental well-being

The most difficult ethical principle to achieve is that of societal and environmental well-being. We would like to highlight three points of interest from our project.

BAG-INTEL reduces resource usage by removing unnecessary information from the system, thereby improving operational performance and lowering energy consumption in an environmentally conscious manner [20].

The expected social impact is significant. Improvements to baggage screening systems result in shorter customs waiting times and enhance the detection of contraband, thereby reducing crime, increasing public safety, and creating a less intrusive baggage screening system. This improves the working conditions of law enforcement officers, reduces risks, and ensures that airports and aircraft are safer.

The reduction in crime relating to drug trafficking, cigarette smuggling, or the uncontrolled movement of money improves customs control and state revenue collection, enabling a more efficient collection system and more effective funding of control systems.

As we have seen, we can improve security and freedom of movement and reduce discriminatory decision-making based on arbitrary judgments in terms of the impact on citizens' fundamental rights. The impact on privacy may be debatable, as data usage may increase and the tool could be used for profiling individuals; however, this impact can be mitigated through proper use under Directive 2016/680.

3.1.7 Accountability

Accountability complements the above requirements and is closely linked to the principle of fairness. The main goal is to implement mechanisms to ensure responsibility and accountability for artificial intelligent systems and their outcomes.

Auditability

Auditability refers to the ability to evaluate algorithms, data, and design processes. At X, this process has been conducted through a collaborative effort between engineers, end users, and the ethics and legal team for each use case.

It has been a multi-level process, with the goal of achieving ethical design by default. In the first phase, the potential risks and issues posed by the use of AI were analysed with all stakeholders. This provided us with a map of the affected fundamental rights and identified where we encountered implementation challenges (see D2.1)

The second phase involved selecting the data that would be fed into the system. Photographs of the luggage used for tracking sometimes showed the passenger's face. To address this, the faces were blurred out so that the system would focus solely on the luggage images. Similarly, the x-ray images focused only on objects, minimising the inclusion of objects irrelevant to the project. Finally, the data that could be used by law enforcement agencies were generated synthetically to avoid using real data, according to their feedback and requirements.

*Figure 10: Passenger face blurring***Bag ID:** b5390d4c-987d-4183-a5e1-e185681728b0**Flight ID:** 2025-03-11-2203-FE8075**Alerted:** 3/11/2025, 2:34:11 PM

Finally, this deliverable was produced, in which a questionnaire was distributed to the involved partners to analyse how the issues were resolved. This allowed us to gather the necessary information and address the engineers' questions.

The system has been audited internally with deliverables 1.4, 2.1, and 2.2.

Minimisation and reporting of negative impacts

No serious issues arose during the development and implementation of artificial intelligence systems across their use cases. A risk management system was established from the outset of the project through the first deliverable, constant communication among partners, open channels of communication with the ethics and legal teams, and the final deliverable.

The collaboration between engineers, end users, and the legal and ethics team has created a model that minimises the implementation of potential issues in the scanner.

The final step to be implemented is the impact assessment for this deliverable, which can be considered a success.

Trade-offs

In the practical implementation of AI—in our case, for border security purposes—the principle of personal data privacy will therefore be balanced against security requirements.

As this is being used in a highly controlled security context, the necessary measures have been taken to ensure that the impact on the privacy of individuals is minimal. It focuses solely on luggage, obscures passengers' faces, and uses synthetic data for PNR information.

Even so, in a real-world implementation of its use, the privacy principles governing its use by law enforcement agencies, as set out in Directive 2016/680, must be balanced against the principle of security, ensuring an ethical use of data in line with the security objectives set out at the borders.

Redress

To ensure that there are no issues with the system's use, a communication channel has been established with the project's principal investigator so that explanations can be sought regarding the project. Furthermore, all those who have participated in the use cases have been provided with details of the open communication channels in case they need to seek clarification on how to use the system. They were also informed of the project's objectives, purpose, rights as participants, and contact person.

Legal and ethical assessments were also conducted during the project to analyse the impact of its use and the proper handling of data within the project.

Although there is a certain degree of international consensus on the basic principles that should underpin the design of intelligent systems, it must not be forgotten that this is being applied within a European framework and cultural perceptions play an important role [21] when it comes to upholding fundamental rights, the rule of law, and democracy [12]. Consequently, the analysis may not necessarily be valid in other countries.

4 CONCLUSIONS

This document aims to prevent risky situations arising from the implementation of artificial intelligence systems in customs control.

The first point to note is that there are no specific guidelines for the use of artificial intelligence in security and crime-fighting matters, as there are for the processing of personal data. The ethical guidelines for achieving reliable artificial intelligence are so flexible that they allow the key points to be adapted to the specific context and use in question.

This has enabled us to analyse the seven points from a novel perspective given the subject matter. It should be noted that the analysis of the seven principles has been very fruitful, given the project's challenges, the use of various artificial intelligence systems, the protection of passengers' privacy, the need to achieve a high accuracy rate, human oversight, and the different ways in which the data can be used, depending on whether it is law enforcement agencies or members of the public.

From the outset, an 'ethics and law by design' approach has been adopted. This involved considering ethical and legal requirements in the design of the scanner and artificial intelligence systems.

This is an advantage because it means that engineers must address the problems that may arise from the implementation of these systems. Likewise, end users have become aware of the impact of using a system such as the one proposed on passengers' rights.

The overall assessment is positive. The negative impact on citizens' fundamental rights can be considered minimal, while the positive impact on security is greater, as it enables the use of systems that streamline and improve baggage screening, particularly in relation to the smuggling of drugs and cigarettes, or the illegal movement of money in or out of the country. This tool facilitates the work of state law enforcement agencies.

One of the biggest challenges in this type of project is the use of law enforcement agencies' real-world data. Developers cannot use this police investigation data unless they have special authorisation from their governments, and this is not always easy to obtain. This is why there are two possible solutions. The first involves creating synthetic data that considers the categories of data used, as has been done with passenger name record data. The main problem is the difficulty of creating it in such a way that the algorithm can use it to generate examples similar to real-world scenarios. The other option is to create sandboxes in which the machine is made available to law enforcement agencies so that they can test and train the algorithms implemented in the scanner using real data.

Another key aspect of the correct use of this type of device is training the end users. This training, carried out in real-world scenarios, is essential for the proper use of the machine. However, raising awareness of the risks and issues that the use of AI poses to passengers' fundamental rights is also important. The impact can be positive, neutral, or negative. End users must be aware that the system must be controlled by humans and that final decisions are backed by humans, who are ultimately responsible for its use and application. More specific training on ethical and legal issues would be necessary for professional users of this type of intelligent system.

The information provided to those involved in the use of these artificial intelligence systems (in our case, passengers) must be clear and accurate so that they are aware of the use of these artificial intelligence systems and of their rights. Not only for this project but also when faced with

approximately automated decisions that affect their fundamental rights. This provides a democratic mandate for its use in security matters.

It is advisable to include a clause along the lines of '*in dubio pro reo*' in our particular case, any errors have a minimal impact on passengers' rights given that final decisions rest with the authorities and that the AI analysis focuses solely on objects rather than people.

REFERENCES

- [1] DE ALMEIDA, P. G. R., DOS SANTOS, C. D. and FARIAS, J. S. (2021). Artificial Intelligence Regulation: a framework for governance. *Ethics Inf Technol* **23** 505–25.
- [2] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE. (2019). *Ethics guidelines for trustworthy AI*. European Commission, Brussels.
- [3] VALLS PRIETO, J. (2021). *Inteligencia artificial, Derechos humanos y bienes jurídicos*. Thomson Reuters, Pamplona.
- [4] MANGAS MARTÍN, A. (2008). *Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo*. Fundación BBVA, Bilbao.
- [5] ANON. (1950). *European Convention on Human Rights*.
- [6] COUNCIL OF EUROPE. (2025). Guide on Article 5 of the Convention – Right to liberty and security.
- [7] MARTÍN Y PÉREZ DE NANCLARES, J. (2008). Título II Libertades. In *Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo* (A. Mangas Martín, ed). Fundación BBVA, Bilbao.
- [8] ANON. (2000). *European Charter of Human Rights*.
- [9] VOGIATZOGLOU, P. and VALCKE, P. (2022). Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law. In *Research Handbook on EU Data Protection Law* (E. Kosta, R. Leenes and I. Kamara, ed). Edward Elgar Publishing.
- [10] OJANEN, T. (2016). Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter: ECJ 6 October 2015, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*. *European Constitutional Law Review* **12** 318–29.
- [11] BRKAN, M. (2019). The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal* **20** 864–83.
- [12] COUNCIL OF EUROPE. *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*.
- [13] BREY, P. A. E. (2012). Anticipatory Ethics for Emerging Technologies. *Nanoethics* **6** 1–13.
- [14] MORLEY, J., ELHALAL, A., GARCIA, F., KINSEY, L., MÖKANDER, J. and FLORIDI, L. (2021). Ethics as a Service: A Pragmatic Operationalisation of AI Ethics. *Minds & Machines* **31** 239–56.
- [15] VALLS-PRIETO, J. (2025). Governance of AI in the Judicial System. In *Digitalization and Artificial Intelligence in Courts: Opportunities and Challenges* (F. Esteban de la Rosa, P. Cortés and N. Marchal Escalona, ed) p 0. Oxford University Press.
- [16] WUERMEILING, U. (2012). Modernization of European data protection law at a turning point. *Computer Law & Security Review* **28** 587–8.
- [17] MCDERMOTT, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society* **4** 2053951716686994.
- [18] FELZMANN, H., VILLARONGA, E. F., LUTZ, C. and TAMÒ-LARRIEUX, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society* **6** 2053951719860542.
- [19] FLETCHER, R. R., NAKESHIMANA, A. and OLUBEKO, O. (2021). Addressing Fairness, Bias, and Appropriate Use of Artificial Intelligence and Machine Learning in Global Health. *Front. Artif. Intell.* **3** 561802.
- [20] RYAN, M. and STAHL, B. C. (2021). Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. *JICES* **19** 61–86.
- [21] ROBINSON, S. C. (2020). Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society* **63** 101421.

APPENDIX A

Ethics of AI (Trustworthy AI)

This is the questionnaire of task 2.2. Only for those partners who are implementing artificial intelligence systems in the project.

Just in case you are development/using Artificial intelligence. There are seven ethical principles. Not all of them should apply to the project, but if it is the case, how do you integrate them to your tasks in the project?

BAG-INTEL TECHNOLOGY:

[Name]

[Executive summary of the technology description]

1. Human agency and oversight

Human agency:

Did you consider the task allocation between the AI system and humans for meaningful interactions and appropriate human oversight and control?

Did you take safeguards to prevent overconfidence in or overreliance on the AI system for work processes?

Human oversight:

Did you consider the appropriate level of human control for AI system? Which mechanisms and measures are implemented to ensure human control?

Is there is a self-learning or autonomous AI system? If so, did you put in place more specific mechanisms of control and oversight?

Which detection and response mechanisms did you establish to assess whether something could go wrong?

2. Technical robustness and safety

Resilience to attack and security:

Did you assess potential forms of attacks to which the AI system could be vulnerable?

Did you estimate the likely impact of a failure of your AI system when it provides wrong results, becomes unavailable, or provides societally unacceptable results (for example discrimination)?

Accuracy

Did you assess what level and definition of accuracy would be required in the context of the AI system and use case?

Did you put in place measures to ensure that the data used is comprehensive and up to date?

Reliability and reproducibility:

Did you put in place a strategy to monitor and test if the AI system is meeting the goals, purposes and intended applications?

3. Transparency**Traceability:**

Did you establish measures that can ensure traceability?

Explainability:

Did you assess to what extent the decisions and hence the outcome made by the AI system can be understood?

Did you ensure an explanation as to why the system took a certain choice resulting in a certain outcome that all users can understand?

Did you design the AI system with interpretability in mind from the start?

Communication:

Did you establish mechanisms to inform (end-)users on the reasons and criteria behind the AI system's outcomes?

Will you clearly communicate characteristics, limitations and potential shortcomings of the AI system to the end user?

4. Diversity, non-discrimination and fairness**Unfair bias avoidance:**

Did you assess and acknowledge the possible limitations stemming from the composition of the used data sets?

Depending on the use case, did you ensure a mechanism that allows others to flag issues related to bias, discrimination or poor performance of the AI system?

Did you establish clear steps and ways of communicating to end users on how such issues can be raised?

Accessibility and universal design:

Did you take the impact of your AI system on the potential user audience into account?

Did you assess whether there could be persons or groups who might be disproportionately affected by negative implications?

Stakeholder participation:

Did you consider a mechanism to include the participation of different stakeholders in the AI system's development and use?

5. Societal and environmental well-being

Sustainable and environmentally friendly AI:

Did you establish mechanisms to measure the environmental impact of the AI system's development, deployment and use (for example the type of energy used by the data centres)?

Did you ensure measures to reduce the environmental impact of your AI system's life cycle?

6. Accountability

Auditability:

Did you establish mechanisms that facilitate the system's auditability, such as ensuring traceability and logging of the AI system's processes and outcomes?

Did you ensure, in applications affecting fundamental rights (including safety-critical applications) that the AI system can be audited independently?

Minimising and reporting negative Impact:

Did you carry out a risk or impact assessment of the AI system, which takes into account different stakeholders that are (in)directly affected?

Did you provide training and education to help developing accountability practices?

- Which workers or branches of the team are involved? Does it go beyond the development phase?
- Do these trainings also teach the potential legal framework applicable to the AI system?

Documenting trade-offs:

Did you establish a mechanism to identify relevant interests and values implicated by the AI system and potential trade-offs between them?

How do you decide on such trade-offs? Did you ensure that the trade-off decision was documented?



REVISION SUMMARY

File name: BAG-INTEL-Deliverable 2.2-v1.0.docx

(Run on 27 May 2026, 07:53:00 AM GMT)

Trinka scanned and edited your text using 'Power Mode' for 'Academic' writing, identifying language errors and the areas of improvement. Here are the details.

This file had 15136 words and 1005 revisions. Our initial assessment showed 54% as the language score for your uploaded file. The distribution of errors and improvements is shown below. A total of 2 suggestions have been added as comments in the document.

Category	Subcategory	Language Category	Revisions
Correctness	Syntax & Vocabulary	Syntax	152
	Syntax & Vocabulary	Other Errors	131
	Punctuation	Punctuation	109
	Grammar	Verbs	74
	Grammar	Articles	41
	Grammar	Prepositions	33
	Syntax & Vocabulary	Accurate Phrasing	19
	Grammar	Adjectives/Adverbs	13
	Grammar	Pronouns & Determiners	13
	Grammar	Singular-Plural Nouns	11
	Grammar	Tense	10
	Grammar	Conjunctions	8
	Grammar	Subject-Verb Agreement	6
	Grammar	Word Form	4
	Spelling	Spellings & Typos	3
	Spelling	Regional Spellings	0
	Syntax & Vocabulary	Run-on Sentence	0
	Syntax & Vocabulary	Fragment	0
Clarity		Brevity	17
		Word Choice	14
		Word Order	3
		Vague Words/Phrases	0
		Idioms/Cliches	0

		Long Sentences	0
		Complex Words	0
		Hedge Words	0
		Long Paragraphs	0
Fluency		Active/Passive Voice	2
		Plain Language	1
		Redundancy	0
		Noun Stacks	0
		Enhancement	0
Style		Capitalization & Spacing	62
		Regional Style	30
		Formal Word/Phrase Choice	2
		Contractions	2
		Consistency	0
		Symbols/Notations	0
		Number Style	0
Style Guide Compliance		Style guide-NONE	245

Settings Applied:**Document type:** Academic**Language preference:** UK English**Editing mode:** Power Mode**Proofread preference:** Correctness, Clarity, Fluency, Style, Spelling**Style guide:** None**Add a supplementary page with the revision summary:** Yes**Show non-actionable suggestions as comments:** Yes