apdcat
Autoritat Catalana de
Protecció de Dades

RGPD vs AIR
Analysis of a partial overlap

Authors: Pablo Gavara Feijóo and María Piedrafita Abión, student interns at the Catalan Data Protection Authority (APDCAT), July 2024.

APDCAT supervisors: Joana Marí Cardona, Data Protection Officer and Head of Strategic Projects, and Guillem López Sanz, Head of Institutional Relations and Organisation.

The views expressed in this document are the responsibility of their authors and do not necessarily reflect the official position of APDCAT.

Generalitat
de Catalunya

© Barcelona, 2024

The content of this report is the property of the Catalan Data Protection Authority and is subject to a Creative Commons BY-NC-ND licence.

Attribution for the authors of the work must be made by including the following mention:

Work belonging to the Catalan Data Protection Authority.

Licensed under the CC BY-NC-ND licence.

The licence has the following characteristics:

You are free to:

Copy, distribute and publicly communicate the work, under the following terms:

- Attribution: Appropriate credit for must be made as indicated by the author or licensor (in any case, not in a way that suggests that they endorse you or your use of their work).
- Non-commercial: This work may not be used for commercial or promotional purposes.
- No derivatives: You may not alter or transform this work or generate a derivative work from it.

Notice: When reusing or distributing the work, the terms of the licence for this work must be clearly mentioned.

You can consult the full text of the licence.

Index

1. Introduction

This work was done by two student interns from the law degree programme at Pompeu Fabra University during their placement with the Catalan Data Protection Authority in July 2024: Pablo Gavara Feijóo and María Piedrafita Abión.

On behalf of the APDCAT team, Joana Marí Cardona, Data Protection Officer and Head of Strategic Projects, and Guillem López Sanz, Head of Institutional Relations and Organisation, supervised this work.

The APDCAT believes that publishing this report is of interest to publicise this first consideration of the new Artificial Intelligence Regulation and its overlap on some points with the General Data Protection Regulation.

2. The Artificial Intelligence Regulation

Regulation 2024/1689, on Artificial Intelligence (AIR) was published on 12 July 2024. This regulation is intended to create a legislative framework to preserve the essential values of the European Union (EU) without restricting European competitiveness. It is the result of a long legislative process of consensus that seeks to reconcile entrepreneurial freedom and technological progress with respect for fundamental rights and the security of AI systems.

The Regulation is a set of rules that, unlike Regulation 2016/679 (General Data Protection Regulation; RGPD), does not set out to establish rights for citizens and is not aimed at the end users of AI systems[1]. The AIR regulates the conditions for the entry of AI systems into the EU's economic market. Therefore, providers, distributors and deployers from third countries will have to comply with certain obligations to be able to enter the EU. This integral and preventative focus of the AIR aspires to produce its content as a "Brussels effect" that has already been achieved in data protection, while establishing global standards. Consequently, although the regulation has EU scope, it inevitably has effects outside this region. Until now, most countries outside the EU have either chosen to follow the model of sectoral regulations or self-regulation from the private sector or have adopted a position we could describe as *laissez-faire*.

The AIR, according to its article 1.1, has the following purpose:

> "to improve the functioning of the internal market […], to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter […], including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation".

Intent to produce a new Brussels effect. Example.

[1] See Annex "Points of connection between the GDPR and the AIR".

Recital 21 AIR says: “In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, **irrespective of whether they are established within the Union or in a third country**, and to deployers of AI systems established within the Union.”

In line with these recitals and the other articles, we believe that providers must not only comply with the AIR but will also consequently be affected by other European regulations with which they will have to comply according to the AIR. The data protection regulation, the GDPR, must be mentioned among these. Article 3 of it establishes that it applied to processing of personal data by controllers or processors regardless of whether they are established in the EU, on condition that the processing activities relate to:

- The offer or goods and services to data subjects who reside in the EU, regardless of whether these require payment;
- monitoring of their behaviour, insofar as it takes place within the EU.

3. Principal definitions[2]

- **AI literacy (article 3(56) AIR)**: skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause.
- **Fundamental rights impact assessment (Recital 96 AIR)**: the aim of this is that the deployer identifies the specific risks to the rights of individuals or groups of individuals who are likely to be affected and to identify measures to be taken in the case of a materialisation of those risks.
- **Biometric data (article 3(34) AIR)**: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data.
- **Biometric identification (article 3(35) AIR)**: the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database.
- **General-purpose AI model (article 3(63) AIR)**: means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications,

[2] See “Glossary of definitions”.

except AI models that are used for research, development or prototyping activities before they are placed on the market.

- **Provider (article 3(3) AIR)**: a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

- **Deployer (article 3(4) AIR)**: a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

- **Risk (article 3(2) AIR)**: the combination of the probability of a occurrence of harm and the severity of that harm.

- **AI system (article 3(1) AIR)**: a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

- **High-risk AI system (article 6(1) AIR)**: an AI system is considered to be high risk when that system is intended to be used as a safety component of a product covered by the Union harmonisation legislation or that the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment for its placing on the market or putting into service in pursuant to the Union harmonisation legislation.

- **Remote biometric identification system (article 3(41) AIR)**: an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database.

- **Real-time remote biometric identification system (article 3(42) AIR)**: a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention.

- **High-risk post-remote biometric identification system (article 3(43) AIR)**: any remote biometric identification system other than a real-time remote biometric identification system.

- **Human oversight (article 14(1) AIR)**: High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.

4. Obligations of the deployer

The obligations of deployers of high-risk AI systems are set out in article 26 AIR. In relation to the area of data protection, the following should be noted:

- They must ensure that the input data are relevant and sufficiently representative in view of the intended purpose. (pt 4)

- They will preserve the logs that the systems generate automatically for a minimum period of six months, unless other regulations (especially regarding data protection) state otherwise. (pt 6)

- They must use the information supplied by the provider in accordance with article 13 AIR to prepare the DPIA (Data Protection Impact Assessment) in compliance the obligation to compete an data protection impact assessment (pt 9)

  Article 13 establishes the obligations of “Transparency and provision of information to deployers”, which must not be confused with those from article 50 “Transparency obligations for providers and deployers of certain AI systems”. The former are for providers towards deployers; in contrast, the latter are for providers and deployers towards natural persons who are users who are exposed to or interact with an AI system.

- AI in the workplace: the legal representatives of workers and the affected workers must be informed of their exposure to the use of the high-risk AI system. In this sense, the express regulation of this aspect by the regulation that must implement the AIR in internal law, in a similar way to articles 87–90 of Spain’s Organic Data Protection Act. (pt 7)

- In the political and criminal sphere: in the case of denial of authorisation to use a high-risk AI system for post remote biometric identification, use of it should cease with immediate effect and the associated personal data should be deleted. (pt 10.II)

- Without prejudice to the transparency obligations from article 50, in the cases of systems from Annex III that make decisions or help make decisions relating to natural persons, any natural persons who are exposed to the use of the system will be informed. (pt 11)

  This last point should be linked to different provisions of the GDPR. Firstly, the obligations of transparency under article 50, which are, in essence, the ones that the provider or deployer must satisfy with regards to natural persons (users) of AI systems with which they interact or to which they are exposed. These could be satisfied in the same moment in which transparency must be given to the information specified in articles 13 and 14 GDPR, in accordance with the general principle of transparency from article 12 GDPR (Transparent information, communication and modalities for the exercise of the rights of the data subject). See the “Transparency and disclosure of information” section below.

  Similarly, the fact that we are discussing systems that take decisions or help take decisions relating to natural persons means it is necessary to connect it to article 22 GDPR, relating to automated individual decision making, including profiling. Section 1 of this article states that any data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Therefore, a high-risk AI system from Annex III would not be able to take decisions that produce legal effects concerning natural persons, if this is not done in accordance with any of the causes or cases set out in articles 2, 3 and 4 of this article. Section 2 sets out three grounds for non-application of the previous section: a) it is necessary for the conclusion or performance of a contract between the data subject and the controller; b) it is authorised by Union or Member State law and appropriate steps are taken to protect the rights, freedoms and legitimate interests of the data subjects; or, c) with the explicit consent of the data subject.

This last point should also be made in relation to article 86 AIR (right to explanation of individual decision making). This article establishes that any person who is affected by a decision that the deployer has made based on a high-risk AI system and that produces legal effects of significantly affects him or her in the areas of health, safety and fundamental rights, can demand "clear and meaningful" explanations of the role of AI in the decision. This is one of the few rights that we could consider that the AIR establishes for users or persons affected by the use of an AI system. The term person should be understood in the sense of natural person, or at least this can be inferred from the reference to safety, health and fundamental rights.

It should be underlined that the deployer is also responsible for carrying out the fundamental rights impact assessment (FRIA) in accordance with article 27 AIR.

Section C of Annex VIII AIR lists the information that deployers must submit to register high-risk systems. The need to include a summary of the conclusions of the FRIA from article 27 AIR and a summary of the DPIA when appropriate should be noted.

Digression: the new obligation to provide a summary of the DPIA in the field of high-risk AI systems

If we restrict ourselves to the scope of the GDPR, it is not obligatory to publish the data protection impact assessment from article 35 GDPR. It should however be noted that while this is not a legal requirement of the GDPR, according to the Directives of the article 29 Working Group (now the European Data Protection Board) on the data protection impact assessment[3], publication of the DPIA could help foster confidence in the processing of the data and demonstrate proactive responsibility and transparency. In this sense, it was noted that it is not necessary to publish the whole assessment, but that it would be good to publish some parts or a summary of it.

Article 49 AIR establishes the obligation of providers and deployers (depending on the type of system and risk) to register AI systems in the EU database from article 71 AIR. Article 71(4) AIR (EU database for high-risk AI systems listed in Annex III) states that with the exception of what is stated in article 49(4)[4], information submitted to the

[3] Directives on the data protection impact assessment (DPIA) and to determine whether processing "results in a high risk" for the purposes of Regulation (EU) 2016/679, WP 248 rev.1.

[4] This refers to the high-risk AI systems from points 1, 6 and 7 of Annex III, in the areas of law enforcement, migration, asylum and border control management.

database must be accessible and will be available to the public in a user-friendly way. The content that must be submitted for registration is set out in Annex VIII cited above. And with regards to what interests us here, it is worth noting the obligation to provide a summary of the data protection impact assessment, which until now was not in any case a legal obligation as such but rather a soft law recommendation.

In relation to deployers, a question that now concerns us, we must consider article 49(3) and (4). Section 3 states that before putting into service or using a high-risk AI system from the list in Annex III, with the exception of those from Section 2 (critical infrastructure), deployers of high-risk AI systems that are public authorities, institutions, offices or agencies of the Union, or persons acting on their behalf, must register themselves, select the system and register its use in the database from article 71. Section 4 which, as is noted above, refers to points 1, 6 and 7 of Annex III, excludes, in the case of Section C of Annex VIII, the obligation to present points 4 and 5. Therefore, in these cases, neither the FRIA nor the DPIA need to be provided for registration.

Therefore, to summarise and clarify the scope of this new data protection obligation: deployers who are public authorities, institutions, offices or agencies of the Union must submit for registration a summary of the DPIA, which will be made public and accessible to everyone, before using a high-risk AI system from Annex III (excluding the systems from points 1, 2, 6 and 7).

It is worth noting that after analysing all of the cases of high-risk AI systems in Annex III we can conclude that all of them, directly or potentially, to a greater or lesser extent, can process personal data. Annex III is divided into 8 areas which in turn are divided into 25 different types of AI systems. The 8 areas are as follows:

(1) biometrics;

(2) critical infrastructure;

(3) education and vocational training;

(4) employment, workers' management and access to self-employment;

(5) access to and enjoyment of essential private services and essential public services and benefits;

(6) law enforcement

(7) migration, asylum and border control management;

(8) administration of justice and democratic processes.

On the same line, the European Data Protection Committee has issued a declaration recommending that Member States attribute to Data Protection Supervisory Authorities the competences relating to the supervision of high-risk AI systems listed in Annex III mentioned above, especially when these high-risk AI systems pertain to sectors where people's rights and freedoms could be affected in the area of the processing of their personal data. This is clearly apart from cases in which the AIR attributes the competence to another authority in relation to another specific sector.

This contrasts with article 74(8) AIR, which establishes the obligation of Member States to designate as market surveillance authorities the supervisory authorities entrusted with data protection or any other designated authority, in the case of high-risk AI systems included in points 1, 6, 7 or 8 of Annex III.

5. Transparency and provision of information

Recital 58 of the RGPD sets out the foundations of the principle of transparency. This requires that any information that is directed at the data subject or at the general public must be precise, concise, easily accessible and comprehensible; and must use clear and plain language and, where appropriate, visualisation.

Therefore, as stated in article 12 GDPR, the controller has the obligation to take the appropriate action to provide the data subject with the information described in articles 13 and 14 GDPR.

Information must be provided in writing or by other means. If it is provided to the public on a website, it can be provided electronically.

In this sense, article 13 establishes that data controller must provide the following information to the data subject:

- the identity and contact details of the controller and, if applicable, its representative;
- the contact details of the data protection officer, if applicable;
- the purpose of the processing to which the personal data will be subjected and the legal basis of the processing;
- The legitimate interests pursued by the controller or by a third party, in the case of point (f) of Article 6(1);
- the recipients or categories of recipients of the personal data, if applicable.
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission;
- the period for which the personal data will be stored;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where it is a case of point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time

- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data;
- the existence of automated decisions as mentioned in article 22 GDPR;

In the event that the controller uses the personal data for a different purpose to the one for which they were collected, it will first inform the data subject of this new purpose.

In addition, article 14 GDPR sets out the information to be provided by the data controller when the personal data are not obtained directly from the data subject. In this case, the following must be added to the information that appears in article 1:

- the categories of personal data that are processed.
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

Similarly, article 14(4) states that in the event that the controller uses the personal data for a different purpose to the one for which they were collected, it will first inform the data subject of this new purpose.

If we turn to the AIR, we find that its article 13 states that high-risk systems must be designed and developed in a way that ensures a sufficient level of transparency for deployers to interpret and use correctly their output results, and also to be able to fulfil the obligations set out in Section 3 (articles 16 to 27). It also establishes that high-risk AI systems must be accompanied by instructions for use, which must include concise, comprehensive, correct and clear information that is pertinent, accessible and understandable for deployers (pt 2).

Section 3 establishes the minimum content for the instructions for use From this content, the following should be noted: the level of accuracy, robustness and cybersecurity; potential risks that might appear and affect health and security or fundamental rights (in connection with the FRIA from article 27); specifications relating to input data or any relevant information about the training data set, validation and testing employed, taking into account the purpose of the system; any information that enables deployers to interpret the outputs as well as using it correctly; and, a description of the mechanisms included in the system that permits deployers to obtain, store and correctly interpret the logs (article 12 AIR). All of this information will also be used for the purposes of complying with the GDPR's transparency and information obligations when AI systems process personal data.

This, however, should not be confused with what is set out in article 50 AIR on the transparency obligations to natural persons of providers and deployers.

Specifically, this article states that providers must ensure that AI systems that are intended to interact with natural persons must be designed and developed in such a way that natural persons concerned are informed that they are interacting with an artificial intelligence system. This will not apply when it is obvious from the point of view of a reasonable informed, observant and circumspect natural person, nor when the AI systems are intended to detect, prevent, investigate or prosecute offences (pt 1). Natural persons must be informed in a clear and distinguishable manner, and no later than the first interaction with or exposure to the AI system (pt 5).

Article 11 AIR regulates the technical documentation of a high-risk system and its minimum content is specified in Annex IV. With regards to what interests us here, it is worth noting point 1 (g) and (h) of the Annex in question, which state that it must include a basic description of the user interface provided to the deployer and the instructions for use.

6. Data protection by design and by default. Responsibilities.

Data protection by design and by default within the field of the AIR must apply to the providers of AI systems, as deployers will in many situations not have the capacity to affect how data are processed by the system. This can be seen in different recitals of the AIR, among which 69 and the start of 93 are especially noteworthy. Recital 69 states that the right to privacy and the protection of personal data must be guaranteed through the whole of the lifecycle of the system and it specifically refers to the principles of minimisation and data protection by design and by default. It also cites anonymisation, encryption and the use of technologies that prevent the transmission of data between the parties as examples of measures to be taken by providers to comply with these principles.

Moreover, Recital 93 states that the risks relating to AI systems could derive from both their design and their use. In any case, both when determining the personal data processing means and at the moment of the processing itself, suitable technical and organisational measures must be taken, such as pseudonymisation. Equally, it should be guaranteed that by default, only the personal data that are necessary for each of the specific purposes of processing are processed and that they will not be accessible, without intervention of the controller, to an indefinite number of persons.[5] It would be of interest if AI systems did not store this information that is not of interest for the intended purpose. Therefore, the AI system should not be able to identify it as it erases it immediately in accordance with the principle of purpose limitation and data minimisation.

In this sense, it is relevant to mention Recital 78 GDPR, which expresses the marked protective and preventive character of the data protection regulation, which states:

> "The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. **When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process**

[5] The impact of this last point in the field of generative artificial intelligence should be seen

> **personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications** and, with due regard to the state of the art, to make sure that **controllers and processors are able to fulfil their data protection obligations.** The principles of data protection by design and by default should also be taken into consideration in the context of public tenders."

The intervention of the provider must enable the other agents to comply with the principles of article 25 GDPR. Afterwards, therefore, products, services and applications (in this case, an AI system) that, in accordance with the state of the art, proactively complies with the data protection regulations should be selected with care (by the deployers). Ultimately, privacy friendly AI systems must be chosen.

Consequently, applying this observation in the field of artificial intelligence, we can conclude that, providers do also have to take into account the right to data protection when designing and programming AI systems ("…producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products…"). So, providers must design AI systems that are suitable for deployers to use them without infringing the data protection regulations for reasons that are cannot be attributed to them.

Although article 16 ("Obligations of providers of high-risk AI systems") does not establish any direct data protection obligation, we can attributed them by virtue of:

- (1) the reference in the article to **Section 2** of the same chapter, compliance with which must be monitored; it includes, among others, article 10 "Data and data governance";

- (2) **Recital 10** AIR when it says that "This Regulation does not seek to affect the application of existing Union law governing the processing of personal data…" and **article 2.7** AIR ("…This Regulation shall not affect Regulation (EU) 2016/679 or (EU) 2018/1725, or Directive 2002/58/EC or (EU) 2016/680, without prejudice to Article 10(5) and Article 59 of this Regulation.") in relation to the aforementioned **Recital 78** GDPR.

We can conclude that, while data processing deriving from the use of AI systems is the responsibility of the deployer, with regards to the principle of data protection by design and by default, this would also fall on the provider to a significant extent. Furthermore, the principle of accountability should be taken into account with regard to assessing whether data protection is an aspect that was taken into account when choosing the AI system.

7. Human supervision and literacy

The AIR does not create or envisage any specific figure to perform the tasks of supervision or vigilance of AI systems. Despite this, Recital 73 and article 26(2) (Obligations of the deployers of high-risk AI systems) establish that deployers must assign human oversight of the systems to natural persons who have the necessary competence, training and authority.

Therefore, the organisation's workers must be trained. Recitals 20 and 91 and article 4 AIR on literacy are important on this point.

Recital 20 indicates that AI literacy must provide all of the agents in the AI value chain with the necessary knowledge to ensure appropriate compliance with and correct implementation of the AIR. For its part, Recital 91 states that deployers must ensure that the people entrusted with putting into practice the instructions for use and human supervision established in the AIR have the necessary competences, in particular an appropriate level of literacy, training and authority regarding AI to exercise these tasks adequately.

The principal article in the text of the AIR with regards to literacy is number 4, "AI literacy". This states:

> "Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used."

Equally, Recital 83 notes that to guarantee legal certainty and facilitate compliance with the Regulation, it is necessary to clarify the function and the specific obligations of the operators of all of the value chain.

It would also be of interest to analyse what role the data protection officer must take in relation to the artificial intelligence regulations. In any case, regarding AI systems that process personal data, data protection officers would maintain all of their functions.

8. AI value chain and continuous improvement process

The terms of article 25 AIR (see also Recital 84) are relevant, which mean that in certain situations, other figures such as the deployer, undertake obligations of the provider in high-risk systems. This case occurs when, for example, a deployer gives his or her name to a high-risk system, substantially modifies this system or modifies the intended purpose of an AI system (including those of general use), in such a way that it becomes a high-risk AI system.

Article 26(5) AIR states that deployers have the duty to monitor the correct operation of systems on the basis of the instructions for use and, when applicable, to inform the provider or distributor and the national competent authority (post-marketing monitoring). The duty to inform "without undue delay" applies if it can be seen that the use of the system could generate a risk in the sense of article 79(1), when a serious incident is detected. Risks that could generate a serious incident are those that affect health, safety and fundamental rights. Therefore, data protection, as a fundamental right, would be included in the deployer's area of vigilance that could give rise to risks that activate the procedure from article 79 that might lead to use of the system in question being suspended.

These procedures will mean that the relationship between the provider and the deployer is close, and so when an error is found, it is raised as quickly as possible by the corresponding person in the value chain.

9. Measures to be promoted by deployers

Article 62 sets out a series of measures to be taken by member states (in particular SMEs and start-ups, and in some cases the local public authorities). Specifically, it establishes the following:

- Priority access to AI regulatory sandboxes.
- Specific awareness raising and training activities on the AIR.
- Communication channels, with the aim of providing advice and responding to doubts raised in relation to the AIR.
- Facilitating participation in the standardisation development process.

Obligations for the AI Office (European Commission) are also established, such as:

- Providing standardised templates.
- Developing a single information platform.
- Organising communication campaigns to raise awareness about the obligations arising from the AIR.
- Evaluating and promoting the convergence of best practices in public procurement procedures in relation to AI systems

10. References

Barrio Andrés, M. (ed.) (2024). *El Reglamento Europeo de Inteligencia Artificial*. Tirant lo Blanch.

Terrón Santos, D. & Domínguez Álvarez, J. L. (2019). *Nueva regulación de la protección de datos: y su perspectiva digital* (Third edition). Editorial Comares.

Glossary of definitions

AI literacy (article 3(56) AIR): skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause.

Logs (article 12(1) AIR): automatic recording of events over the lifetime of the system.

Supervisory authority (article 4(21) GDPR): an independent public authority which is established by a Member State pursuant to Article 51.

Market surveillance authority (article 3(26) AIR): the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020.

National competent authority (article 3(48) AIR): a notifying authority or a market surveillance authority; as regards AI systems put into service or used by Union institutions, agencies, offices and bodies, references to national competent authorities or market surveillance authorities in this Regulation shall be construed as references to the European Data Protection Supervisor.

Notifying authority (article 3(19) AIR): the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

Conformity assessment (article 3(20) AIR): the process of demonstrating whether the requirements set out in Chapter III, Section 2 relating to a high-risk AI system have been fulfilled.

Fundamental rights impact assessment (Recital 96 AIR): the aim of this is to identify the specific risks to the rights of individuals or groups of individuals likely to be affected and identify measures to be taken in the case of a materialisation of those risks.

Data protection impact assessment (Recital 90 GDPR): this should be carried out by the controller prior to the processing in order to assess the likelihood and severity of the high risk, taking into account the nature, scope, context, purposes of the processing and the sources of the risk.

Making available on the market (article 3(10) AIR): the supply of an AI system or a general-purpose AI model for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.

Safety component (article 3(14) AIR): a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property.

Consent of the data subject (article 4(11) GDPR): any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Biometric data (article 3(34) AIR): personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data.

Input data (article 3(33) AIR): data provided to or directly acquired by an AI system on the basis of which the system produces an output.

Training data (article 3(29) AIR): data used for training an AI system through fitting its learnable parameters.

Personal data (article 4(1) GDPR): any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Recipient (article 4(9) GDPR): a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Distributor (article 3(7) AIR): a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

Profiling (article 4(4) GDPR): any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Enterprise (article 4(18) GDPR): a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

AI regulatory sandbox (article 3(55) AIR): a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision.

Intended purpose (article 3(12) AIR): the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.

Law enforcement (article 3(46) AIR): activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.

Biometric identification (article 3(35) AIR): the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database.

Serious incident (article 3(49) AIR): an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

a) the death of a person, or serious harm to a person's health;

b) a serious and irreversible disruption of the management or operation of critical infrastructure;

c) the infringement of obligations under Union law intended to protect fundamental rights;

d) serious harm to property or the environment.

Critical infrastructure (article 3(62) AIR): critical infrastructure as defined in Article 2, point (4), of Directive (EU) 2022/2557.

Instructions for use (article 3(15) AIR): the information provided by the provider to inform the deployer of, in particular, an AI system's intended purpose and proper use.

Placing on the market (article 3(9) AIR): the first making available of an AI system or a general-purpose AI model on the Union market.

Restriction of processing (article 4(3) GDPR): the marking of stored personal data with the aim of limiting their processing in the future.

General-purpose AI model (article 3(63) AIR): means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.

AI Office (article 3(47) AIR): the Commission's function of contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance, provided for in Commission Decision of 24 January 2024; references in this Regulation to the AI Office shall be construed as references to the Commission.

Operator (article 3(8) AIR): a provider, product manufacturer, deployer, authorised representative, importer or distributor.

International organisation (article 4(26) GDPR): an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Putting into service (article 3(11) AIR): the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose.

Provider (article 3(3) AIR): a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

Pseudonymisation (article 4(5) GDPR): the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Representative (article 4(17) GDPR): a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Deployer (article 3(4) AIR): a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Controller (article 4(7) GDPR): the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Risk (article 3(2) AIR): the combination of the probability of a occurrence of harm and the severity of that harm.

AI system (article 3(1) AIR): a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

High-risk AI system (article 6(1) AIR): an AI system is considered to be high risk when that system is intended to be used as a safety component of a product covered by the Union harmonisation legislation or that the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment for its placing on the market or putting into service in pursuant to the Union harmonisation legislation.

Remote biometric identification system (article 3(41) AIR): an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database.

Real-time remote biometric identification system (article 3(42) AIR): a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention.

High-risk post-remote biometric identification system (article 3(43) AIR): any remote biometric identification system other than a real-time remote biometric identification system.

Post-marking monitoring system (article 3(25) AIR): all activities carried out by providers of AI systems to collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions.

Human oversight (article 14(1) AIR): High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.

Third party (article 4(10) GDPR): a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Processing (article 4(2) GDPR): any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Annex: Points of connection between the GDPR and the AIR[6]

- Article 1. Subject matter

- Article 2. Material scope vs Article 2 Scope.

- The AIR, unlike the GDPR, does not establish the principles of the regulation that it develops. Likewise, it does not establish rights nor is it directed at end users; instead it basically focusses on establishing obligations for providers, deployers of systems, etc.

- Definitions: art. 4 vs art. 3. The number of definitions differs greatly with 26 in the GDPR while the AIR has 68, more than double. This is essentially because the AIR is a much more technical regulation that the GDPR.

[6] Throughout the English version of this Annex we have used the official versions of the regulations in English.

GDPR	AIR
Article 1. Subject matter and objectives. 1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.	**Article 1. Subject matter.** 1. The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation. 2. This Regulation lays down: (a) harmonised rules for the placing on the market, the putting into service, and the use of AI systems in the Union; (b) prohibitions of certain AI practices; (c) specific requirements for high-risk AI systems and obligations for operators of such systems; (d) harmonised transparency rules for certain AI systems; (e) harmonised rules for the placing on the market of general-purpose AI models; (f) rules on market monitoring, market surveillance, governance and enforcement; (g) measures to support innovation, with a particular focus on SMEs, including start-ups.
Article 2. Material scope 1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	**Article 2. Scope** 1. This Regulation applies to: (a) providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country; (b) deployers of AI systems that have their place of establishment or are located within the Union; (c) providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union; (d) importers and distributors of AI systems; (e) product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark; (f) authorised representatives of providers, which are not established in the Union; (g) affected persons that are located in the Union.

GDPR	AIR
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.	2. For AI systems classified as high-risk AI systems in accordance with Article 6(1) related to products covered by the Union harmonisation legislation listed in Section B of Annex I, only Article 6(1), Articles 102 to 109 and Article 112 apply. Article 57 applies only in so far as the requirements for high-risk AI systems under this Regulation have been integrated in that Union harmonisation legislation.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	3. This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences. This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities. This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.
	4. This Regulation applies neither to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States, provided that such a third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals.
	5. This Regulation shall not affect the application of the provisions on the liability of providers of intermediary services as set out in Chapter II of Regulation (EU) 2022/2065.
	6. This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

GDPR	AIR
	7. Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulation (EU) 2016/679 or (EU) 2018/1725, or Directive 2002/58/EC or (EU) 2016/680, without prejudice to Article 10(5) and Article 59 of this Regulation. 8. This Regulation does not apply to any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Such activities shall be conducted in accordance with applicable Union law. Testing in real world conditions shall not be covered by that exclusion. 9. This Regulation is without prejudice to the rules laid down by other Union legal acts related to consumer protection and product safety. 10. This Regulation does not apply to obligations of deployers who are natural persons using AI systems in the course of a purely personal non-professional activity. 11. This Regulation does not preclude the Union or Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or from encouraging or allowing the application of collective agreements which are more favourable to workers. 12. This Regulation does not apply to AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 or 50.

Definitions from article 4 GDPR[7]	Definitions from article 3 AIR
1. Personal data	1. AI system
2. Processing	2. Risk
3. Restriction of processing	3. Provider
4. Profiling	4. Deployer
5. Pseudonymisation	5. Authorised representative
6. Filing system	6. Importer
7. Controller	7. Distributor
8. Processor	8. Operator
9. Recipient	9. Placing on the market
10. Third party	10. Making available on the market
11. Consent of the data subject	11. Putting into service
12. Personal data breach	12. Intended purpose
13. Genetic data	13. Reasonably foreseeable misuse
14. Biometric data	14. Safety component
15. Data concerning health	15. Instructions for use
16. Main establishment	16. Recall of an AI system
17. Representative	17. Withdrawal of an AI system
18. Enterprise	18. Performance of an AI system
19. Group of undertakings	19. Notifying authority
20. Binding corporate rules	20. Conformity assessment
21. Supervisory authority	21. Conformity assessment body
22. Supervisory authority concerned	22. Notified body
23. Cross-border processing	23. Substantial modification
24. Relevant and reasoned objection	24. CE marking
25. Information society service	25. Post-marking monitoring system
26. International organisation	26. Market surveillance authority
	27. Harmonised standard
	28. Common specification
	29. Training data
	30. Validation data
	31. Validation data set
	32. Testing data
	33. Input data
	34. Biometric data
	35. Biometric identification
	36. Biometric verification
	37. Special categories of personal data
	38. Sensitive operational data
	39. Emotion recognition data
	40. Biometric categorisation system
	41. Remote biometric identification system
	42. Real-time remote biometric identification system
	43. Post-remote biometric identification system
	44. Publicly accessible space
	45. Law enforcement authority
	46. Law enforcement
	47. AI Office

[7] Colour coding: reference by the AIR to the GDPR (green); parallels (orange); and differences (red).

Definitions from article 4 GDPR[7]	Definitions from article 3 AIR
	48. National competent authority
	49. Serious incident
	50. Personal data
	51. Non-personal data
	52. Profiling
	53. Real-world testing plan
	54. Sandbox plan
	55. AI regulatory sandbox
	56. AI literacy
	57. Testing in real-world conditions
	58. Subject
	59. Informed consent
	60. Deep fake
	61. Widespread infringement
	62. Critical infrastructure
	63. General-purpose AI model
	64. High-impact capabilities
	65. Systemic risk
	66. General-purpose AI system
	67. Floating-point operation
	68. Downstream provider

- Definition 37 (Special categories of personal data) in the AIR refers to article 9(1), GDPR (Processing of special categories of personal data).

- Definitions 50 and 51 (Personal data and Non-personal data) from the AIR refer to definition 1 (Personal data) from the GDPR.

- Definition 52 (Profiling) from the AIR refers to definition 4 (Profiling) in the GDPR.

- Definition 34 (Biometric data) from the AIR might refer to definition 14 (Biometric data) from the GDPR:

Definition 14 from the GDPR	Definition 34 from the AIR
‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.	‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data.

- We can establish a parallel between the following definitions:

GDPR	AIR
Definition 7: “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Definition 4: “deployer” means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.
Definition 11: “consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.	Definition 59: “‘informed consent” means a subject’s freely given, specific, unambiguous and voluntary expression of his or her willingness to participate in a particular testing in real-world conditions, after having been informed of all aspects of the testing that are relevant to the subject’s decision to participate.
Definition 12: “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.	Definition 49: “serious incident” means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following: (a) the death of a person, or serious harm to a person’s health; (b) a serious and irreversible disruption of the management or operation of critical infrastructure; (c) the infringement of obligations under Union law intended to protect fundamental rights; (d) serious harm to property or the environment
Definition 17: “representative” means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.	Definition 5: “authorised representative” means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.
Definition 21: “supervisory authority” means an independent public authority which is established by a Member State pursuant to Article 51.	Definition 26: “market surveillance authority” means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020.
	Definition 48: “national competent authority” means a notifying authority or a market surveillance authority; as regards AI systems put into service or used by Union institutions, agencies, offices and bodies, references to national competent authorities or market surveillance authorities in this Regulation shall be construed as references to the European Data Protection Supervisor.

- A certain similarity between what Section 1 of Chapter IV GDPR seeks to achieve (establishing obligations for the controller and processor, arts. 24 to 31) and certain sections of the AIR, such as Section 3 of Chapter III (Obligations of providers and deployers of high-risk AI systems and other parties, arts. 16 to 27), Chapter IV (Transparency obligations for providers and deployers of certain AI systems, art. 50), Sections 2 and 3 of Chapter V (Obligations for providers of general-purpose AI models, arts. 53 and 54; Obligations of providers of general-purpose AI models with systemic risk, art. 55).

- Chapter VII AIR (Governance, arts. 64 to 70) can be likened to different sections of the GDPR:

  - The equivalent of Section 1 of Chapter VII AIR (Governance at Union level, arts. 64 to 69) would be Section 3 of Chapter VII GDPR (European data protection board, arts. 68 to 76).

  - The equivalent of Section 2 of Chapter VII AIR (National competent authorities, art. 70) would be Chapter VI GDPR (Independent supervisory authorities, arts. 51 to 59). This could also be regarded as equivalent to Section 4 of Chapter III (Notifying authorities and notified bodies, arts. 28 to 39).

- The equivalent of article 35 GDPR (Data protection impact assessment) would be article 27 AIR (Fundamental rights impact assessment for high-risk AI systems).

Article 35 GDPR	**Article 27 AIR**
Article 35. Data protection impact assessment 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. 2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment. 3. A data protection impact assessment	**Article 27. Fundamental rights impact assessment for high-risk AI systems** 1. Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce. For that purpose, deployers shall perform an assessment consisting of: (a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose; (b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used; (c) the categories of natural persons and groups likely to be affected by its use in the specific

Article 35 GDPR	Article 27 AIR
referred to in paragraph 1 shall in particular be required in the case of: a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale. 4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68. 5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board. 6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. 7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in	context; (d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13; (e) a description of the implementation of human oversight measures, according to the instructions for use; (f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms. 2. The obligation laid down in paragraph 1 applies to the first use of the high-risk AI system. The deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by provider. If, during the use of the high-risk AI system, the deployer considers that any of the elements listed in paragraph 1 has changed or is no longer up to date, the deployer shall take the necessary steps to update the information. 3. Once the assessment referred to in paragraph 1 of this Article has been performed, the deployer shall notify the market surveillance authority of its results, submitting the filled-out template referred to in paragraph 5 of this Article as part of the notification. In the case referred to in Article 46(1), deployers may be exempt from that obligation to notify. 4. If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment. 5. The AI Office shall develop a template for a questionnaire, including through an automated tool, to facilitate deployers in complying with their obligations under this Article in a simplified manner.

Article 35 GDPR	Article 27 AIR
paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. 8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. 9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. 10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities. 11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	

- Article 31 GDPR, in the framework of the general obligations imposed on the controller and the processor, requires cooperation with the supervisory authority. Likewise, the AIR does the same in its article 21 (cooperation with competent authorities) in the framework of the obligations of providers and deployers of high-risk AI systems and other parts.

- Section 5 of Chapter IV GDPR governs the code of conduct and certification (arts. 40 to 43) and section 4 of Chapter V AIR governs the codes of practice (art. 56) while Chapter X AIR governs codes of conduct and guidelines (arts. 95 and 96). This could also be linked to section 5 of Chapter III (Standards, conformity assessment, certificates, registration -arts. 40 to 49-).

- We can make a connection between article 59 AIR, which refers to the further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox, and the circumstance covered in article 9(2)g GDPR ("processing is necessary for reasons of substantial public interest"), which is an exception to the prohibition in article 9(1) GDPR, which refers to the processing of special categories of personal data.

- Section 2 of Chapter IV GDPR (Security of personal data -arts. 32 to 34-), which in article 33 regulates notification of a personal data breach to the supervisory authority, is comparable, mutatis mutandis, to Section 2 of Chapter IX AIR (Sharing of information on serious incidents -art. 73-), which in its only article governs the reporting of serious incidents.

- The equivalent of Chapter X GDPR (Delegated acts and implementing acts -arts. 92 and 93-) would be Chapter XI AIR (Delegation of power and committee procedure -arts. 97 and 98-).

- Obviously the last chapter of both regulations (XI of GDPR -arts. 94 to 99- and XIII AIR -arts. 102 to 113-) refers to the final provisions.

In which points does the AIR explicitly cite the GDPR?

It is cited a total of 29 times: 13 in the recitals, 14 in the articles and 2 in the annexes.

Location in the AIR	Reference to the GDPR	Context/content
Recital 10, paragraph 1	Regulation in general.	Regarding the fundamental right to personal data protection.
Recital 14	Article 4(14).	Concept of "biometric data".
Recital 39 (twice)	Article 9(1) (twice).	Processing of biometric data.
Recital 53, paragraph 2	Article 4(4).	If the AI system involves profiling in the sense of the GDPR, and these profiles display a significant risk of prejudicing health, safety or fundamental rights.

Location in the AIR	Reference to the GDPR	Context/content
Recital 54	Article 9(1).	Classification as high-risk systems of those intended to be used for biometric classification in accordance with sensitive attributes or characteristics e.g. 9.1 RGPD.
Recital 67, paragraph 1	Regulation in general.	Data governance and management Transparency about the original purpose of the data collection.
Recital 70 (twice)	Regulation in general. Article 9(2) g.	Processing of special categories of personal data, as a matter of public interest, to ensure the detection and correction of biases associated with high-risk AI systems and avoid potential discrimination.
Recital 95	Regulation in general.	Guaranteeing post-remote biometric identification rights.
Recital 140 (three times)	Article 6(4) and article 9(2) g. Obligations of controllers and rights of data subjects, in general. Article 22(2) b.	Legal basis for providers and potential providers in the AI regulatory sandbox to use personal data collected for other purposes to develop particular AI systems for the public interest in the AI regulatory sandbox. They continue to be applicable. The AIR does not have to provide a legal basis in this regard.
Article 2(7)	Regulation in general.	Scope of the AIR. The AIR will not affect the GDPR.
Article 3(37), (50), (51) and (52) (four times)	Article 9(1). Article 4(1) (twice). Article 4(4).	Definitions of the concepts of "special categories of personal data", "personal data", "non-personal data" and "profiling". These refer to the GDPR.
Article 5(1) h *in fine*,	Article 9.	Prohibited AI practices. The prohibition in paragraph (h) is understood without prejudice to article 9 GDPR regarding processing of biometric data for purposes other than ensuring compliance with the law.
Article 10(5), at the start of paragraph (f) (twice)	Regulation in general (twice).	Data and data governance. Processing of special categories of personal data by providers, to ensure the detection and correction of biases associated with high-risk AI systems.
Article 26(9) and (10) (IV) (twice)	Article 35. Article 9.	Obligations of the deployers of high-risk AI systems. Deployers will use the information provided in accordance with article 13 AIR when they carry out the impact assessment from article 35 GDPR.

Location in the AIR	Reference to the GDPR	Context/content
Article 27(4)	Article 35.	Fundamental rights impact assessment for high-risk AI systems. If any of the obligations set out in article 27 AIR are already fulfilled with the GDPR impact assessment, the fundamental rights impact assessment will complement the data impact assessment from the GDPR.
Article 50(3)	Regulation in general.	Transparency obligations for providers and deployers of certain AI systems. Regarding the data processing regulations for the deployers of a system of recognition of emotions or of a system of biometric categorisation, as well as reporting on the performance of the system to the natural persons exposed to it.
Article 59(1) c	Article 35.	Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox In the AI regulatory sandbox, personal data lawfully collected for other purposes may be processed to develop, train and test certain AI systems when the following conditions, among others, are met: there are effective monitoring mechanisms if any high risks to the rights and freedoms of the data subjects may arise during the sandbox experimentation.
Article 74(8)	The competent data protection supervisory authorities in accordance with the Regulation.	Market surveillance and control of AI systems on the Union market. For high-risk AI systems listed in point 1 of Annex III to this Regulation, in so far as the systems are used for law enforcement purposes, border management and justice and democracy, and for high-risk AI systems listed in points 6, 7 and 8 of Annex III to this Regulation, Member States shall designate as market surveillance authorities for the purposes of this Regulation either the competent data protection supervisory authorities under Regulation (EU) 2016/679 or Directive (EU) 2016/680, or any other authority designated pursuant to the same conditions laid down in Articles 41 to 44 of Directive (EU) 2016/680.

Location in the AIR	Reference to the GDPR	Context/content
Annex V, point 5	Regulation in general.	EU declaration of conformity. This must contain, among other things, a statement that that AI system, when it involves the processing of personal data, complies with the GDPR among other regulations.
Annex VIII, Section C, point 5	Article 35.	Information that must be submitted for registration of high-risk AI systems in accordance with article 49. Information to be submitted by deployers of high-risk AI systems in accordance with Article 49(3). Among other information, it must contain a summary of the data protection impact assessment from article 35 GDPR, when proceeding in accordance with article 26(8) AIR.