OBLIGATIONS OF PROVIDERS AND DEPLOYERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES (CHAPTER III, SECTION 3) *

Javier García Luengo
Full Professor of Administrative Law
University of Oviedo

* This paper has been written within the framework of the Research Project 'Algorithmic tools for citizens and public administrations', funded by the Spanish Ministry of Science and Innovation (PID2021-126881OB-I00).

1. *Introduction*

The Regulation of the European Parliament and of the Council, laying down harmonised rules on artificial intelligence (Artificial Intelligence Regulation), determines the subjective scope of application of its requirements for high-risk AI systems in a set of articles found in Chapter III ('Obligations of providers and deployers of high-risk AI systems and other parties') of its Title III ('High-risk AI systems').

The first point to note is that, as highlighted by the Council of the Union in its General Approach of 6 December 2022, when introducing paragraph 52a (now recital 83) in the recitals of the Regulation, operators within the AI value chain 'could act in more than one role at the same time and should therefore fulfil cumulatively all relevant obligations associated with those roles. For example, an operator could act as a distributor and an importer at the same time'.

Having made this consideration, to which we will return at the end of our exposition, the operators identified and regulated by the Regulation are the following (Article 2.1):

- Providers placing AI systems on the market 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.
- Deployers of AI systems that have their place of establishment or are located in the Union.
- Providers and deployers of AI systems that have their place of establishment or are located in a third country whenever the output produced by the AI system is used in the Union.
- Importers and distributors of AI systems.
- Product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark.
- Authorised representatives of providers, which are not established in the Union.
- Affected persons that are located in the Union.

The scope of the Regulation, however, does not include end-users when used in a personal, non-professional activity, research or development activities in the field of AI,[1] or systems that are placed on the market and

[1] In this sense, p. e., H. Ruschemeier, *AI as a challenge for legal regulation – the scope*

put into service or used, with or without modifications, exclusively for military, defence or national security purposes in the field of defence. [2]

It is very significant that the regulation, as was already the case with Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of individuals with regard to the processing of personal data, has significant extraterritorial effects [3] as it affects operators established in third countries in the sense that we will observe when analysing each figure.

While an overview of the scope of application of the Regulation has already been given when commenting on its general provisions, we must now specify for each of these figures the obligations which, according to the Regulation, are incumbent on them when they operate high-risk AI systems.

2. *Providers of high-risk AI systems*

2.1. *Scope of the concept of provider*

According to the legal definition in Article 3(2) of the Regulation, an AI system provider is any natural or legal person, public authority, agency, or other body that develops a high-risk AI system or for which such an AI system is 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, regardless of whether such providers are physically present or established in the Union or a third country. Providers of high-risk AI systems are subject to a set of obligations specified in Articles 16 ff. of the Regulation.

The Regulation also takes into account the fact that, throughout the chain of marketing and implementation of high-risk AI systems, there may

---

of application of the artificial intelligence act proposal, in *ERA Forum*, 2023, 23, pp. 361 ff., p. 370.

[2] The Regulation also does not apply to AI systems that are not placed on the market or put into service in the Union in cases in which their output results are used in the Union exclusively for military, defence, or national security purposes, regardless of the type of entity carrying out these activities.

[3] These effects have already been highlighted by B. Townsend, *Decoding the Proposed European Union Artificial Intelligence Act*, in *Insights*, Volume: 25 Issue: 20, 2021, pp. 1 ff., p. 5.

be changes in the position of operators, which may lead to a reorganization of their obligations and, in particular, other operators may become providers and may have to assume the obligations of this type of operator.

The assumption of obligations that concern us here are as follows:

- *Transformation of other operators into providers*

Firstly, any distributor, importer, deployer, or other third party should be considered a provider of a high-risk AI system for the purposes of the AIA and shall be subject to the obligations of the provider in any of the following circumstances:

i. When they put their name or trademark on a high-risk AI system previously placed on the market or already put into service, which we understand to be applicable only if they do so in a way that implies vis-à-vis third parties the assumption of the provider's position (and clearly not the in case in which the importer is identified alongside the provider). This is without prejudice to contractual agreements stipulating that obligations are otherwise allocated.
ii. When they make a substantial modification on a high-risk AI system that has already been placed on the market or has already been put into service with the result that it remains a high-risk AI system.
iii. When they modify the intended purpose of an AI system, including a general-purpose AI system which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system.

In such cases, the provider who initially placed the AI system on the market or put it into service shall cease to be considered as the provider of that AI system but shall cooperate closely with new providers [4] and furnish the necessary information, technical access or other assistance reasonably foreseeable to fulfil the obligations set out in the Regulation, in particular as regards compliance with the conformity assessment of high-risk AI systems.

Nevertheless, any initial provider that has clearly indicated that its AI system should not be transformed into a high-risk AI system is not subject to the obligation to hand over the documentation.

Consideration should also be given to the fact that, even if the provider

[4] Without prejudice to the need to observe and protect intellectual and industrial property rights, confidential business information, and trade secrets, in accordance with Union and national law.

is located in a third country, the Regulation is declared applicable when 'the output produced by the AI system is used in the Union'.

This regulation is always reasonable for the deployer insofar as it controls where its services are provided. The provider, however, may legitimately be unaware that the results of systems are being used in the European Union. In such a scenario, requiring the provider to comply with the obligations of the Regulation for providers seems disproportionate. This, however, must not prevent measures against users of the service or measures blocking the use of the system in the EU. [5]

- In particular, the case of high-risk AI systems that are safety components of other products

In the case of high-risk AI systems, which are safety components of products covered by the Union harmonization legislation listed in Section A of Annex I, [6] the product manufacturer shall be considered as the provider of the high-risk AI system and shall be subject to the obligations foreseen for those operators if (i) it places the system on the market together with the product under its name or trademark, or where (ii) the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

A long list of obligations applies to all these parties, considered providers, which we will now analyse.

2.2. *Obligations of providers of high-risk AI systems*

The main and first obligation in the list in Article 16 is that **providers must ensure that their high-risk AI systems comply with the**

---

[5] In this sense, P. A. De Miguel Asensio, *Propuesta de Reglamento sobre Inteligencia Artificial*, in *La Ley Unión Europea*, n° 92, 2021, pp..1 - 8, Section IV, www.laleydigital.com.

[6] This includes products such as machinery (within the meaning of Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery), toys, recreational craft and personal watercraft, lifts and safety components for lifts, equipment, and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, cableway installations, personal protective equipment, equipment burning gaseous fuels, medical devices and in vitro diagnostic medical devices.

requirements imposed by the Regulation. This basic obligation, the substantial content of which has been analysed in the previous chapter of this work, is essentially fulfilled through the prior conformity assessment and the obligations of surveillance, adoption of corrective measures, and cooperation with the authorities that we will analyse in this section. It is, therefore, the objective to which all the other obligations laid down in the Regulation are more or less directly subordinate.

The following obligation, which is of an instrumental but basic nature, and which curiously has only been included in the Regulation since the General Approach of the Council of the European Union, is the obligation to **identify** the provider himself by mentioning his name, his registered trade name or trademark and his contact address.

This identification should be made on the high-risk AI system itself, if possible, and otherwise on the packaging or documentation accompanying the product.

Thirdly, the provider **must have a quality management system in place** which complies with Article 17 of the Regulation.

This implies that the provider must have documentation that systematically and in an orderly manner sets out the policies, procedures and instructions applicable to the high-risk AI system, including at least the following aspects:

i. The strategy for regulatory compliance (including compliance with conformity assessment procedures and procedures for managing modifications to high-risk AI systems).
ii. The techniques, procedures, and systematic actions to be used in the design and design control and design verification of the high-risk AI system.
iii. The techniques, procedures, and systematic actions to be used in the development of the high-risk AI system and in the control and quality assurance of the high-risk AI system.
iv. The examination, test, and validation procedures to be carried out before, during, and after the development of the high-risk AI system and the frequency with which they will be carried out.
v. The technical specifications, including standards, to be applied and, where the relevant harmonised standards do not apply in full or do not cover all the requirements for high-risk AI systems, the means to be used to ensure that the high-risk AI system meets those requirements.
vi. The systems and procedures for data management, including data

acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention, and any other data-related operations carried out prior to and for the purpose of placing on the market or the putting into service of high-risk AI systems.

vii. The risk management system (referred to in Article 9 of the Regulation).

viii. The setting-up, implementation, and maintenance of a post-market monitoring system, in accordance with Article 72 of the Regulation.

ix. The procedures related to the reporting of a serious incident in accordance with Article 73 of the Regulation.

x. The handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers, or other interested parties.

xi. The systems and procedures for record-keeping of all relevant documentation and information.

xii. The resource management, including security-of-supply related measures.

xiii. The accountability framework setting out the responsibilities of the management and other staff with regard to all these aspects.

This is, therefore, an extensive obligation to record all the efforts necessary to comply with the Regulation, from the design of the system to any incident that may occur during its implementation, which is absolutely essential insofar as the control exercised by the authorities, according to the model chosen by the Regulation, is not based on a prior authorization, which would allow the Administration to open and create a specific file with the elements that accredit compliance with the law.

The next obligation is closely related to the same idea, as the provider must also **keep the following documentation**:

1. The technical documentation referred to in Article 11 of the Regulation, i.e., documentation demonstrating that the high-risk AI system complies with the requirements set out in Section Two of the Regulation and clearly and comprehensively provides the national competent authorities and notified bodies with all the information they need to assess whether the AI system in question complies with those requirements. Such documentation should include at least the items required in Annex IV of the Regulation (which means keeping at least a detailed description of the elements of the AI system and its

development process and modifications) or, in the case of SMEs, including start-ups, they may provide such information in a simplified form and to facilitate this, the Commission will establish a simplified form of technical documentation targeted at the needs of small and micro-enterprises. Where SMEs and emerging companies choose to submit information in a simplified form, they will use this form and Notified Bodies are obliged to accept this form for the purposes of conformity assessment.

2. The documentation concerning the quality management system referred to in Article 17 of the Regulation means that the documentation reflecting in a systematic and orderly manner the written policies, procedures and instructions that make up the quality management system must be kept.
3. The documentation relating to changes approved by the notified bodies, where applicable.
4. The decisions and other documents issued by the notified bodies, where applicable.
5. The EU declaration of conformity is referred to in Article 47 of the Regulation.

The aim of this obligation is to facilitate the monitoring of the AI system by the competent authorities and the examination of the adequacy between what was communicated to the authorities at the time when the AI system was introduced in the market and the actual functioning of the system.

This documentation must be kept for a period of ten years after the AI system has been placed on the market or put into service and must be kept at the disposal of the competent national authorities.

This provision may be problematic if the system undergoes a substantial modification during this period that makes it, in fact, an essentially different instrument. In such a case, in order to avoid circumvention of the law, it should be understood that the duty to retain documentation (which serves as a basis for proper control of compliance with the obligations arising from the Regulation) extends for ten years from the time at which the modification was introduced or put into service.

On the other hand, the envisaged limitation of the obligation to a period of ten years is at odds with the essentially dynamic nature of some of the documents to be kept, such as those describing the quality management system or those relating to changes in the AI system itself. Strictly speaking, it does not seem to us to be a good idea to limit the obligation to keep the basic documentation of the system over time by means of a fixed period that

is the same for all systems.[7] Since the maintenance of this obligation over time is not particularly burdensome, it should be extended to the time during which the AI system remains in operation or, if a technically flawless regulation is desired, to the time during which the obligations derived from compliance with the Regulation can still be demanded of the providers.

The issue is of particular importance, and the following statement in recital 18 of the Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (COM/2022/496 final) is particularly worrying:

> '*The limitation of disclosure of evidence as regards high-risk AI systems is consistent with [the AI Act], which provides certain specific documentation, record keeping and information obligations for operators involved in the design, development and deployment of high-risk AI systems. Such consistency also ensures the necessary proportionality by avoiding that operators of AI systems posing lower or no risk would be expected to document information to a level similar to that required for high-risk AI systems under [the AI Act]*'.

If the two systems are to be coordinated, which is obviously desirable, it makes no sense to limit the obligation to retain documentation to a fixed period of ten years without considering that damage resulting from a high-risk AI system can manifest itself long after it has been put into service.

It does not make sense that the provider can refuse to provide the information requested by a liability claimant because the ten years for keeping it have passed, but neither is it reasonable to presume that a duty of care has been breached by failing to produce such documentation when the request for production is made beyond the aforementioned legally fixed period. For this reason, it is essential that the duty of preservation is accompanied by the time in which the system is in operation and can, therefore, cause injury to third parties and even that this duty extends

[7] The passage of a period of 10 years can be counter-argued, it is sufficient for the high-risk AI system to have been sufficiently analysed and studied and it would not make sense to keep information that might already be obsolete. However, we see no reason to make such general assertions and, above all, contrary to the dynamic nature of several of the documents on which the provider's obligation of custody falls.

beyond that time for a period equivalent to the limitation period of the liability action. [8]

Moreover, the limitation of the retention period for technical documentation is not compatible with recital 71 of the Regulation itself, which justifies, on reasonable grounds, the need to retain technical information throughout the life of the AI system. [9]

This obligation should be understood to be fulfilled to the extent that Article 72 effectively requires the maintenance of a post-market monitoring system for AI systems that will actively and systematically collect, document, and analyse relevant data that may be provided by the deployers or collected from other sources on the performance of high-risk AI systems throughout their lifetime, and that allows the provider to assess ongoing compliance with the requirements set out in Chapter III, Section 2 of the Regulation.

It is paradoxical, however, that the post-market monitoring system itself will be based on a post-market monitoring plan, which will be part of the technical documentation referred to in Annex IV and which, therefore, according to Article 18, only has to be kept for 10 years.

On the other hand, appropriate measures must be put in place for the retention of documentation when the provider ceases his activity during the period for which his obligations are in force. In the latter respect, according to the Regulation, each Member State shall determine conditions under

---

[8] Although the non-harmonization of the limitation period for liability actions may make this issue problematic, a reasonable time limit could be set to ensure both the legal certainty of the provider and the effectiveness of possible actions taken by those affected.

[9] Recital 71 of the Regulation states: '*Having comprehensible information on how high-risk AI systems have been developed and how they perform throughout their lifetime is essential to enable traceability of those systems, verify compliance with the requirements under this Regulation, as well as monitoring of their operations and post market monitoring. This requires keeping records and the availability of technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements and facilitate post market monitoring. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk-management system and drawn in a clear and comprehensive form. The technical documentation should be kept up to date, appropriately throughout the lifetime of the AI system. Furthermore, high-risk AI systems should technically allow for the automatic recording of events, by means of logs, over the duration of the lifetime of the system*'.

which the documentation remains at the disposal of the national competent authorities for the ten-year period for the cases when a provider or its authorised representative established on its territory goes bankrupt or ceases its activity prior to the end of that period.

Finally, providers that are financial institutions subject to requirements regarding their internal governance, arrangements, or processes under Union financial services law shall maintain the technical documentation as part of the documentation kept under the relevant Union financial services law. This special provision may be problematic because retention periods may differ, and there is no justification for applying a more lenient regime here, where appropriate, precisely in an area where the risks of misuse of an AI system are obvious.

The next obligation for providers of high-risk AI systems is to **retain the log files automatically generated by their high-risk AI systems**.

Such log files should have minimum enrolment capacities as determined in Article 12, to the commentary of which we refer [capacities to be higher for high-risk AI systems referred to in Annex III 1), a) of the Regulation, i.e., for remote biometric identification systems].

This is an obligation elaborated in Article 19 of the Regulation, which requires these files to be kept for a period of time adequate for the intended purpose of the high-risk AI system.

Some aspects of this regulation need to be clarified:

First, the obligation to generate log files extends throughout the life cycle of the system to the extent that such files are under the control of the provider of the high-risk AI system.

Secondly, the obligation to keep such log files does not seem to extend for the entire lifetime of the system but for the time determined by EU law, especially data protection law, or by the Member State concerned - the regulation only provides for a minimum of six months. Therefore, special rules, including those issued by Member State authorities, may determine a longer duration of this obligation to retain log files, an obligation that could be extended if the size of the data collected is not excessive to the entire life of the AI system. The Regulation thus combines the requirements of the principle of proportionality with the need to ensure post-marketing follow-up, leaving the decision on the length of retention to the sectoral legislator.

The next obligation of providers of high-risk AI systems is to **ensure that such systems are subject to the relevant conformity assessment procedure** before being placed on the market or put into service.

This conformity assessment[10] can be followed by two procedures. Firstly, the conformity assessment procedure based on internal control (Annex VI of the Regulation), and secondly, for those AI systems where this route is chosen or where no harmonized standards or common specifications exist (or have not been implemented or cannot be implemented in the system), the conformity assessment procedure based on the assessment of the quality management system and the assessment of the technical documentation carried out by a notified body (Annex VII of the Regulation).

The provider of a high-risk AI system is also obliged to draw up an **EU declaration of conformity** in accordance with Article 47 of the Regulation, whereby it assumes responsibility for compliance with the requirements set out in Section 2 of the Regulation.

The declaration shall be written in a machine-readable form, signed electronically or in manuscript, shall have the content set out in Annex V of the Regulation, and shall be kept up to date, as appropriate, and at the disposal of the national competent authorities for a period of 10 years after the high-risk AI system has been placed on the market or put into service.

A copy of the EU declaration of conformity in a language that can be easily understood by the competent national authorities of the Member State(s) in which the high-risk AI system is placed on the market or made available on the market shall be supplied to them on request.

Where high-risk AI systems are subject to other Union harmonization legislation that also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union law applicable to the high-risk AI system, identifying the Union harmonization legislation to which the declaration relates.

Obviously, the EU declaration of conformity is a type of responsible declaration that binds the provider as it declares that it complies with the requirements that the Regulation and other EU legislation impose on its high-risk AI system, leaving the provider responsible for any non-compliance.

Closely related to this last obligation is the obligation to **affix the CE marking to the high-risk AI system**, as this marking is the symbol that proves to third parties that the system complies with European regulations.

---

[10] The detailed analysis of which corresponds to Chapter VII of this work, to which we return in substance.

This obligation shall be fulfilled by affixing the CE marking visibly, legibly, and indelibly on the high-risk AI system itself or, where that is not possible, on its packaging or accompanying documentation to indicate the conformity of the system with the Regulation.

The **registration obligations** that the provider of the high-risk AI system must also fulfil are that both the provider and the high-risk AI system must be registered in the EU database for high-risk AI systems maintained by the European Commission.

Such registration must take place before a high-risk AI system listed in Annex III is placed on the market or put into service, except for AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic or the supply of water, gas, heat or electricity (systems referred to in Annex III(2) of the Regulation).

The next obligation of providers of high-risk AI systems is to take the necessary corrective measures and to provide market surveillance authorities with information on risks identified in their system that affect the health, safety, or fundamental rights of individuals. [11]

The essential obligation is that all providers of high-risk AI systems who consider or have reason to consider that a high-risk AI system that they have placed on the market or put into service is not in conformity with the Regulation shall immediately take the corrective measures necessary to bring it into conformity, to withdraw it from the market, to disable it, or to recall it, as appropriate. Furthermore, they shall inform the distributors of the high-risk AI system concerned and, where applicable, the deployers, the authorized representative, and the importers accordingly.

In addition, where a high-risk AI system presents a risk affecting the health, safety, or fundamental rights of persons, and the provider becomes aware of such a risk, the provider shall immediately investigate the causes in collaboration with the reporting deployer, where applicable, and inform the market surveillance authorities competent for the high-risk AI system

[11] As any system may involve a greater or lesser degree of risk, the rule clarifies, with reference to Article 3(19) of Regulation (EU) 2019/1020 , that risk shall be considered to be present to a degree beyond what is considered reasonable and acceptable in relation to its intended purpose or under normal or reasonably foreseeable conditions of use of the system in question, including the duration of its use and, where appropriate, its commissioning, installation and maintenance requirements.

concerned and, where applicable, to the notified body that issued a certificate for that system, of the nature of the non-compliance and any corrective action taken.

The wording of this obligation in Article 20 of the Regulation raises some doubts:

While the Regulation identifies, at least clearly, all subjects to whom the provider of the high-risk AI system must inform about the risks and the corrective measures taken, it does not set specific reaction times since, although the investigation of the causes of the non-compliance causing the risk and the adoption of the corrective measures must be 'immediate', no specific maximum time is set for their adoption or for complying with the (limited) information measures. This contrasts with the provisions of Article 74 of the Regulation, which provides that where the market surveillance authority (with or without cooperation with national authorities) detects non-compliance, it may impose on the provider corrective measures to be taken within a time limit which the market surveillance authority may prescribe, but in any event within the shorter of 15 working days, or as provided for in the relevant Union harmonization legislation. It may also make more stringent determinations, such as withdrawing or recalling the high-risk AI system concerned from the market.

It is significant in this context that there is no obligation to notify the competent authorities of corrective actions, which are notified to the distributors of the high-risk AI system, the deployers, the authorised representative, and the importers.

Authorities are informed of 'alerts', so to speak, when the identified risk affects the health, safety, or fundamental rights of individuals.

This regulation does not make sense because the adoption of a corrective measure is a serious event that should not only lead to communication with the competent authority but also to an assessment of the possible damage caused.

This regulation also contrasts poorly with other more developed regulations in other areas of administrative intervention, such as food safety,[12] in which the systems of alerts and cooperation between the

[12] Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority, and laying down procedures in matters of food safety defines a clear duty to inform the competent

provider who detects non-compliance and the authorities are much more developed, and the duties of information and the adoption of preventive measures are better defined. It is hard to understand why risk prevention should be approached without building on sectoral approaches, disregarding the great experience that the European Union has in other equivalent areas of regulation.

The next obligation to be considered is **to demonstrate, upon a reasoned request by the competent national authority, the compliance of the high-risk AI system with the requirements set out in the Regulation itself** (in particular Section 2).

This obligation to cooperate with the competent authorities is further developed in Article 21 of the Regulation, which imposes two complementary mandates in this respect:

Firstly, providers of high-risk AI systems shall, upon a reasoned request from a competent authority, provide that authority with all the information and documentation necessary to demonstrate the compliance of the high-risk AI system with the requirements set up in Section 2 of the Regulation and shall do so in a language which can be easily understood by the authority in one of the official languages of the institutions of the Union as indicated by the Member State concerned.

Secondly, such providers shall, upon a reasoned request by a competent authority, give access to the automatically generated log files of the high-risk AI system to the extent that these files are under their control.

Information obtained in the performance of these cooperation obligations shall, however, be treated in accordance with the confidentiality obligations set out in Article 78 of the Regulation.

The final obligation under Article 16 of the Regulation is to ensure that high-risk AI systems comply with the accessibility requirements for persons with disabilities set out in Directives (EU) 2016/2102 and (EU) 2019/882.

Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies imposes in Article 4 a general obligation

---

authorities of the risks and measures taken (Article 19), to the consuming public itself (Article 10) and also establishes a rapid alert network that coordinates the European Commission with the national authorities (Article 50), in a tried and tested system that could have been replicated in the case of the risks generated by high-risk AI systems, which can also threaten the same protected legal assets covered by Regulation 178/2002.

on Member States to ensure that public sector bodies take the necessary measures to increase the accessibility of their websites and mobile applications by making them perceivable, operable, understandable and robust.

The aim of the Directive is to make these public instruments more accessible to users, in particular to people with disabilities.

There is, however, a general exception to the general obligation, as defined in Article 5 of the Directive, which states that accessibility need not be increased where this would impose a disproportionate burden on public sector bodies.

Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services has a more general scope and imposes, in Article 4, an obligation on all economic operators to place on the market only products and provide only services that comply with the accessibility requirements set out in Annex I of the Directive. Annex I imposes a long list of specific accessibility obligations, in particular concerning information technology systems and services, such as ensuring that the product, including its user interface, contains features, elements and functions that enable persons with disabilities to access, perceive, operate, understand and control the product, including ensuring that when the product provides the functions of communication, operation, information, control and guidance, it must do so through more than one sensory channel (including providing alternatives to visual, auditory, spoken and tactile communication).

As we saw for the general obligation imposed in Directive 2016/2102, also these general obligations of Directive 2019/882 are qualified by Article 14, as the accessibility requirements of Annex I shall only apply to the extent that compliance with them (i) does not require a significant change in a product or service that results in the fundamental alteration of its basic nature, and (ii) does not result in the imposition of a disproportionate burden on the economic operators concerned.

These accessibility obligations, which were introduced in the final text of the Regulation following the consensus reached between the European Parliament and the Council, are entirely plausible and require a delicate balance between the rights of persons with disabilities and the very economic and functional viability of the AI system in question. A balance that, in our opinion, both directives and, especially Directive 2019/882, strike on this issue.

In addition to the obligations imposed in Article 16, Article 73[13] of the Regulation requires providers of high-risk AI systems to **report any serious incident to the market surveillance authorities of the Member States** where the incident occurred.

In this case, the Regulation does determine with precision the timing of the notification, the general rule being that the notification shall be made immediately after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link and, in any case, no later than 15 days after the provider or the person responsible for the deployment becomes aware of the serious incident. The timeframe for notification should also take into account the magnitude of the serious incident, meaning that the more serious the incident, the more diligence the provider will have to take to establish the causal link between the system and the incident and to notify the competent authority.

In addition, there are two more specific rules on the notification period:

- In the event of a widespread breach or serious incident involving serious and irreversible disruption to the management or operation of critical infrastructure (Article 3(49)(b) of the Regulation), the report shall be provided immediately and no later than two days after the provider or deployer becomes aware of the incident.
- In the event of the death of a person, the report shall be made immediately after the provider or the person responsible for deployment has established, or as soon as it suspects, a causal link between the high-risk AI system and the serious incident within a period not exceeding 10 days from the date on which the provider or, where applicable, the person responsible for deployment becomes aware of the serious incident.

This regulation is justified insofar as a systemic failure affecting critical infrastructures can have a catastrophic effect, and obviously, the death of a person is an incident of the utmost seriousness. However, it does not make sense to require an immediate report and then set a time limit of ten days for the act of reporting.

On the other hand, the Regulation also allows, in order to ensure a speedy report, the provider or, where appropriate, the deployer to initially submit an incomplete notification, followed by a complete notification.

A separate but related obligation is contained in Article 73(6) of the

[13] See the contribution by Fernández Fernández in this volume.

Regulation, which obliges the provider to carry out without delay, upon notification of a serious incident, the necessary investigations in relation to the incident and the AI system concerned.

In this investigation, which shall include a risk assessment of the incident and corrective actions, the provider shall cooperate with the competent authorities and, where appropriate, the notified body concerned, and, in particular, shall not perform any investigation that involves altering the AI system concerned in a way which may affect any subsequent evaluation of the causes of the incident, prior to informing the competent authorities of such action.

2.3. *Sanctioning instruments to ensure compliance with the obligations of providers of high-risk AI systems* [14]

Compliance with the obligations described in the previous section is ensured by the Regulation itself with important coercive mechanisms, as non-compliance with these obligations is sanctioned as an administrative offence with significant penalties.

In particular, according to Article 99(4) of the Regulation, any breach of the obligations of providers of high-risk AI systems, as provided for in Article 16, shall be subject to administrative fines of up to EUR 15,000,000 or, if the offender is an undertaking, up to 3 % of its total worldwide turnover for the preceding financial year, whichever is the higher.

The use of the total worldwide turnover is not an appropriate magnitude to set the sanction proportionally, even though it is a parameter widely used by EU regulations (for example, to set sanctions in competition matters), because the turnover does not reflect the actual net worth of the company, so that a company with a high turnover but low net worth can be sanctioned for excess, while a minor sanction is imposed on companies with a moderate turnover but high net worth. Nor does it seem justified to lower the proportional penalty for SMEs on the basis of their turnover rather than on the basis of their net worth.

In addition, the supply of incorrect, incomplete, or misleading information to notified bodies or national competent authorities in reply

[14] For further information, see, in this book, D. Rodríguez Cembellín, 'Penalties'.

to a request shall be subject to administrative fines of up to EUR 7,500,000 or, if the offender is an undertaking, up to 1% of the total worldwide turnover for the preceding financial year, whichever is higher.

3. *Authorised representatives of the providers of high-risk AI systems*

3.1. *Obligations of authorised representatives*

The following operator referred to in the Regulation is the authorised representative for providers located in third countries.

Thus, Article 22 of the Regulation requires that, before placing their high-risk AI systems on the Union market, providers established in third countries must designate, by means of a written mandate, an authorised representative established in the Union.

The tasks for the execution of which the representative must be authorised by the mandate are as follows:

- Verify that the provider:
  - Has drawn up the EU declaration of conformity.
  - Has the technical documentation required by the Regulation.
  - Has carried out an appropriate conformity assessment procedure.
- Keep at the disposal of the competent authorities and national authorities or bodies for a period of 10 years after the high-risk AI system has been placed on the market or put into service:
  - The contact details of the provider who appointed the authorised representative.
  - A copy of the EU declaration of conformity.
  - The technical documentation
  - If appropriate, the certificate issued by the notified body.
- Provide a competent authority, upon a reasoned request, with all information and documentation (including that referred to in the previous point) necessary to demonstrate the compliance of a high-risk AI system with the requirements of the Regulation, and in particular, access to the log files automatically generated by that system, to the extend such files are under the control of the provider.
- Cooperate with the competent authorities, upon reasoned request, in any actions taken in relation to the high-risk AI system, in particular, to reduce and mitigate the risks involved in the high-risk AI system.
- Where applicable, comply with the registration obligations, or if the

registration is carried out by the provider itself, ensure that information on the name, address, and contact details of the authorised representative itself is correct.

The mandate shall also entitle the authorised representative to be contacted by the competent authorities, in addition to or instead of the provider, with reference to all issues related to ensuring compliance with the Regulation.

The authorised representative must also provide the market surveillance authorities, upon request, with a copy of the mandate in one of the official languages of the Union institutions, as indicated by the competent authority.

Finally, the authorised representative shall terminate the mandate if he considers or has reason to believe that the provider is in breach of his obligations under the Regulation. In such a case, it shall also immediately inform the relevant market surveillance authority and, where applicable, the relevant notified body of the termination of the mandate and of the reasons for this measure.

3.2. *Sanctioning instruments to ensure compliance with the obligations of authorised representatives*

The Regulation guarantees compliance with the obligations of authorised representatives by subjecting them to the same sanctioning system that is applied to the providers in a regulation, fundamentally contained in paragraphs 4 and 5 of Article 99, which is justified insofar as we are talking about representatives who consciously assume the compliance of essential obligations for guaranteeing the security of high-risk AI systems and who, furthermore, could disassociate themselves, as we have just seen, from their mandate if they appreciate a lack of collaboration on the part of the provider.

4. *Importers*

4.1. *Concept and obligations of importers of high-risk AI systems*

The next type of operator to be analysed is the importer, which is any natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

The importer's obligations are particularly extensive and start from a general one: he must ensure that the high-risk AI system being introduced into the EU must comply with the requirements imposed on them by the Regulation. In concrete terms, this means that he must verify the following points:

- That the provider has carried out the conformity assessment procedure.
- That the provider has drawn up the required technical documentation.
- That the system bears the required CE marking and is accompanied by the EU declaration of conformity and instructions for use.
- That the provider has appointed an authorised representative.

In addition to these formal obligations, the importer must comply with a series of control, documentation, and information obligations regarding the system itself. Specifically, the following:

- If the importer has sufficient reason to believe that a high-risk AI system does not comply with the Regulation, has been falsified or is accompanied by falsified documentation, he shall only place it on the market once it has been brought into conformity with EU legislation.
- If the high-risk AI system presents risks affecting the health, safety, or fundamental rights of persons,[15] it shall inform the system provider, authorised representatives, and market surveillance authorities.
- While the system is under their responsibility, they shall ensure that storage or transport conditions, where applicable, do not jeopardise its compliance with the requirements of the Regulation for the system.
- They shall keep a copy of the certificate issued by the notified body, the instructions for use and the EU declaration of conformity, if applicable, for a period of 10 years after the high-risk AI system has been placed on the market or put into service.
- They shall provide the relevant competent authorities, upon reasoned request, with all the information and documentation necessary to

[15] Recall that, as clarified in footnote 5, such risk shall be considered to occur to a degree beyond what is considered reasonable and acceptable in relation to its intended purpose or under normal or reasonably foreseeable conditions of use of the system in question, including the duration of its use and, where appropriate, its commissioning, installation and maintenance requirements.

demonstrate the conformity of a high-risk AI system with the requirements laid down in the Regulation in a language that can be easily understood by them and shall also ensure that the technical documentation can be made available to those competent authorities.

- They shall cooperate with the relevant competent authorities in any action taken by them in relation to a high-risk AI system placed on the market by importers, in particular to reduce and mitigate the risks posed by that system.

They shall provide the relevant competent authorities, upon reasoned request, with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in the Regulation in a language which can be easily understood by them and shall ensure that the technical documentation can be made available to those competent authorities.

4.2. *Sanctioning instruments to ensure compliance with the obligations of importers*

Again, the Regulation ensures compliance with the obligations of importers by subjecting them to the same system of penalties that applies to providers since, as operators, they consciously assume compliance with obligations essential to ensuring the safety of high-risk AI systems both in that they must ensure that they bring into the EU a system that complies with the requirements of the Regulation, and in that, they assume custody of it while it is within their sphere of responsibility.

5. *Distributors*

5.1. *Concept and obligations of distributors of high-risk AI systems*

These operators are natural or legal persons, other than providers or importers, that are part of the supply and marketing chain of an AI system on the Union market.

Its main obligation is, again, to ensure that the high-risk AI system it distributes complies with the requirements of the Regulation. Although the set of obligations is less than in the case of importers.

In particular, from a formal point of view, they must ensure that:

- The high-risk AI system bears the required CE marking.

- The system is accompanied by a copy of the EU declaration and instructions for use.
- The provider has fulfilled his identification obligations (by including on the high-risk AI system or, where this is not possible, on the packaging of the system or in the accompanying documentation, as appropriate, his name, registered trade name, or registered trademark and contact address) and has an appropriate quality management system in place according to the Regulation.
- The importer has fulfilled his identification obligations (so that he includes on the packaging or accompanying documentation his name, registered trade name or registered trademark and contact address)

From a substantive point of view, and as we saw with importers, the distributors have various control and reporting obligations:

- If the distributor considers or has reason to believe, on the basis of the information in his possession, that a high-risk AI system is not in conformity with the requirements set out in the Regulation, the distributor shall not place it on the market until such conformity has been achieved and if the high-risk AI system presents risks affecting the health, safety or fundamental rights of persons [16] the distributor shall inform the provider of the system or, where applicable, the importer. [17]
- As long as the high-risk AI system is under their responsibility, distributors shall ensure that storage or transport conditions, where applicable, do not jeopardise the system's compliance with the requirements of the Regulation.
- Where a distributor considers or has reason to consider, on the basis of the information in its possession, that a high-risk AI system is not in conformity with the requirements set out in Section 2, it shall not

[16] It should be recalled that, as clarified in footnote 5, such a risk is considered to be present to a degree beyond what is considered reasonable and acceptable in relation to its intended purpose or under normal or reasonably foreseeable conditions of use of the system in question, including the duration of its use and, where appropriate, its commissioning, installation and maintenance requirements.

[17] While it should be understood that refusal to distribute the product here reduces the risk, it would be prudent to impose an obligation on the distributor to inform authorised representatives and market surveillance authorities.

make the high-risk AI system available on the market until the system has been brought into conformity with those requirements.

- Where the high-risk AI system presents a risk affecting the health, safety, or fundamental rights of persons,[18] the distributor shall immediately inform the provider or importer of the system and the competent authorities for the high-risk AI system concerned and shall provide details, in particular, of the non-compliance and any corrective measures taken.
- Upon a reasoned request from a relevant competent authority, distributors shall provide that authority with all the information and documentation regarding their actions necessary to demonstrate that the system complies with the requirements of the Regulation.
- Distributors shall cooperate with the relevant competent authorities in any actions taken in relation to a high-risk AI system made available on the market by the distributors, in particular, to reduce or mitigate the risks posed by it.

5.2. *Sanctioning instruments to ensure compliance with the obligations of distributors*

Once again, the Regulation guarantees compliance with the obligations of distributors by subjecting them to the same sanctioning system that applies to providers since, as operators, they consciously assume compliance with essential obligations to guarantee the security of high-risk AI systems, both in that they must ensure that they distribute in the EU a system that meets the requirements of the Regulation, and, like importers, in that they assume custody of the high-risk AI system while it is within their sphere of responsibility.

6. *Deployers*

6.1. *Concept and obligations of the deployers of high-risk AI systems*

Deployers are all natural or legal persons, or public authorities, bodies, or

[18] In the sense of footnote 5.

agencies using an AI system under its authority, except where the AI system is used during a personal, non-professional activity.[19]

The obligations of deployers are particularly extensive, and this is because the risks of applying the AI system may manifest themselves in this deployment phase without their existence having been foreseen in the development phase.[20] In its final version, the Regulation has greatly developed the obligations of these operators that in the initial version were clearly insufficient, as the doctrine was careful to highlight,[21] although the impact assessment requested by these authors has only been established for some sectors of activity and is not a general obligation as established by article 35 of 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.

The catalogue of general obligations for these operators is extensive:

- The deployers of high-risk AI systems shall take appropriate technical

---

[19] Concept established in article 3(4) of the Regulation.

[20] This is rightly argued in recital 93 of the Regulation: '*Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the persons or groups of persons likely to be affected, including vulnerable groups.* (...)'.

[21] In this regard, for example, M. Ebers, V.R.S. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, in *J Multidisciplinary Scientific Journal*, 4, 2021, pp. 589 to 603 (www.mdpi.org), p. 597: 'it seems conspicuous that the AIA requires the providers (developers) of an AI system to perform a risk assessment, whereas under the GDPR, the user (as defined under the AIA) acts as the 'data controller' who takes on the task of risk assessment. This shift of roles has the effect of removing 'users' from any responsibility for risk assessment under the AIA. Consequently, the AIA should provide an obligation for high-risk AI system users to carry out an AI impact assessment similar to the one carried out under Art. 35 GDPR, Art. 39 EUDPR or under Art. 27 LED (p. 9)'.

and organisational measures to ensure that they use such systems in accordance with the instructions for use accompanying the systems.

- Deployers shall assign human oversight, as defined in Article 14 of the Regulation, to natural persons with the necessary competence, training, and authority. [22]
- They shall also ensure that the input data is relevant and sufficiently representative given the intended purpose of the high-risk AI system.
- Deployers shall monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with the framework of the post-market monitoring system.
- Where deployers have reason to consider that using the high-risk AI system in accordance with their instructions may result in that AI system presenting a risk affecting the health, safety, or fundamental rights of individuals, [23] they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority and suspend the use of that system.
- Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. [24]
- They shall keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control for a period appropriate to the intended purpose of the high-risk AI system of at

---

[22] Compliance with these first two obligations does not affect other obligations imposed on deployers by national or Union law, nor their freedom to organise their own resources and activities in order to implement the human supervision measures indicated by the provider.

[23] In the sense nuanced in note 5.

[24] This obligation to provide information has, however, two important nuances:

• This obligation shall not cover sensitive operational data of deployers of AI systems, which are law enforcement authorities.

• For deployers that are financial institutions subject to requirements regarding their internal governance, arrangements, or processes under Union financial services law, the monitoring obligation shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes, and mechanisms pursuant to the relevant financial service law.

least six months,[25] unless provided otherwise in applicable Union or national law, in particular in Union law on the protection of personal data.[26]

- Where applicable, deployers of high-risk AI systems shall use the information provided under Article 13 of the Regulation (instructions for use and information that allows for proper interpretation of the output results) to comply with their obligation to carry out a data protection impact assessment.
- Deployers shall cooperate with the relevant competent authorities in any action those authorities take in relation to the high-risk AI system in order to implement the Regulation.

In addition, specific obligations are foreseen for some sectors:

- In case of putting into service or using high-risk AI systems at the workplace

Deployers shall, before putting into service or using a high-risk AI system at the workplace, inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. This information shall be provided in accordance with the rules and procedures laid down in Union and national law and practice of workers and their representatives.

- In the case where the deployers of high-risk AI systems are public authorities or Union institutions, bodies, offices, or agencies

The public deployers of high-risk AI systems shall comply with the registration obligations referred to in Article 49.

In the case of high-risk AI systems in the areas of law enforcement, migration, asylum, and border control management, these obligations,

---

[25] We must insist here on the considerations we made in the case of the similar obligation of providers.

[26] The deployers that are financial institutions subject to requirements regarding their internal governance, arrangements, or processes under Union financial services law shall maintain the logs as part The Regulation imposes in Article 26(10) the obligation to request a judicial or administrative authority whose decisions are binding and subject to judicial review on deploying officers to use a high-risk AI system for delayed remote biometric identification in the framework of an investigation aimed at the targeted search for a person suspected or convicted of having committed a criminal offence. Of the documentation kept pursuant to the relevant Union financial service law.

however, are reduced, in accordance with Article 49 of the Regulation, by reducing the data to be provided to the register and by making the register in a non-public section of the database accessible only to the Commission and the national authorities designated for the control of the systems in these areas.

When such deployers find that the high-risk AI system that they envisage using has not been registered in the EU database, they shall not use that system and shall inform the provider or the distributor.

-Specific obligations for the use of high-risk AI systems for delayed remote biometric identification in the criminal sphere

The Regulation imposes in Article 26(10) that the deployer of a high-risk AI system shall request authorisation by a judicial authority or an administrative authority whose decision is binding and subject to judicial review for the use of that system in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, and for post-remote biometric identification.

However, the initial identification of a possible suspect on the basis of objective and verifiable facts directly linked to the offence is exempted from the authorisation.

The obligation to request authorisation must be fulfilled ex ante or without undue delay and no later than 48 hours, and each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence.

In the event that the authorisation is rejected, the use of the post-remote biometric identification system linked to that requested authorisation shall be stopped with immediate effect, and the personal data linked to the use of the high-risk AI system for which authorisation was requested shall be deleted.

Any use of such systems, regardless of the purpose or deployer, shall be documented in the relevant police file and made available, upon request, to the relevant market surveillance authority and national data protection authority, excluding the disclosure of sensitive operational data related to law enforcement. [27]

[27] Which is to be understood, without prejudice to the powers conferred on supervisory authorities by 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

In addition, deployers shall submit annual reports to the relevant market surveillance authority and the national data protection authority on their use of delayed remote biometric identification systems, although disclosure of sensitive operational data related to law enforcement is excluded, and reports may be aggregated to cover more than one deployment.

The whole of this authorisation regulation leaves a lot of doubts open, as the wording is too open, allowing both ex-ante and ex-post authorisations, granted both in judicial and administrative proceedings, which makes this authorisation a lax mechanism, however, Member States are allowed to establish stricter rules for the use of this type of high-risk AI systems, and, in an excessively generic statement, 'shall ensure' that law enforcement authorities cannot take any decision that produces adverse legal effects for an individual solely on the basis of the output results of such delayed remote biometric identification systems. The reasonable thing to do, in accordance with the general principles of law common to the Member States, would be to have expressly stated that any conviction or restrictive measure against the individual based solely on the use of such systems would be null and void.

The Regulation does, however, clearly prohibit the use of high-risk AI systems of delayed remote biometric identification for law enforcement purposes in an untargeted way, without any connection to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or to the search for a specific missing person.

Nevertheless, it is worrying, however, that this prohibition leaves open uses of these systems beyond the targeted search for a person suspected or convicted of having committed a crime, which is the purpose requiring authorisation. This could be interpreted to mean that these systems can be used without authorisation for other purposes of crime prevention or searching for missing persons unless prevented by other EU [28] or Member State rules.

---

of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

[28] Article 26(10) itself states that this provision is without prejudice to Article 9 of Regulation (EU) 2016/679 and Article 10 of Directive (EU) 2016/680 for the processing of biometric data. This means that the prohibitions laid down in these rules on the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the

- Obligations to inform natural persons imposed on certain deployers

Those deployers of high-risk AI systems referred to in Annex III [29] who make decisions or assist in making decisions relating to natural persons shall inform those natural persons that they are exposed to the use of high-risk AI systems. In the case of high-risk AI systems used for law enforcement purposes, Article 13 of Directive (EU) 2016/680 [30] shall apply.

6.2. *In particular, the fundamental rights impact assessment for high-risk AI systems*

The first thing to clarify is that the obligation for deployers to subject the high-risk AI system to an impact assessment is not general, having both objective and subjective limitations.

From an objective point of view, the obligation to assess the system refers to high-risk AI systems listed in Annex III, except for those relating to critical infrastructures (insofar as it is understood that they will not affect fundamental rights).

From a subjective point of view, the following deployers are obliged to carry out an impact assessment:

---

processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person shall apply.

[29] Annex III identifies as high-risk specific AI systems in the areas of biometrics, critical infrastructure, education and vocational training, employment, management of workers and access to self-employment, law enforcement, migration, asylum and border control management, administration of justice, and democratic processes.

[30] This provision allows Member States to adopt legislative measures delaying, limiting, or omitting to make available to the data subject certain information, including the collection of data without his or her knowledge, as long as such a measure constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations, or procedures;

(b) avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences or the execution of criminal penalties;

c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

- Those who are bodies governed by public law.
- Those who are private entities providing public services.
- Those using high-risk AI systems to assess the creditworthiness of natural persons to establish their credit score.
- Those using high-risk AI systems for risk assessment and pricing in relation to natural persons in the case of life and health insurance.

The assessment that these deployers are required to undertake should include the following elements:

i. Description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose.
ii. Description of the time period during which each high-risk AI system is expected to be used and the frequency with which it is expected to be used.
iii. Identification of the categories of natural persons and groups of persons likely to be affected by its use in the specific context.
iv. Identification of the risks of specific harm that may affect the categories of natural persons and groups concerned, taking into account the information provided by the provider in compliance with the Regulation.
v. Description of the implementation of human oversight measures in accordance with the instructions for use.
vi. Identification of measures to be taken in case such risks materialise, including internal governance arrangements and grievance mechanisms.

The assessment may be waived in the cases provided for in Article 46 of the Regulation, i.e., for exceptional reasons of public safety or in order to protect human life and health, the environment, or critical industrial and infrastructure assets.

Once the assessment has been carried out, the deployer shall notify its findings to the market surveillance authority, which shall develop for this purpose a model questionnaire using an automated tool, in order to facilitate a simplified way for the deployer to fulfil its obligations. [31]

[31] This technique is also used in other regulatory areas to standardise operators' self-assessments within the EU. The most typical example is the European Single Procurement Document (ESPD) which was regulated in the Commission Implementing Regulation (EU) 2016/7 of 5 January 2016 establishing the standard form for the European Single Procurement Document (ESPD).

The assessment obligation shall apply to the first use of the high-risk AI system so that, in similar cases, the deployer may rely on previously conducted fundamental rights impact assessments or existing impact assessments conducted by providers.

If the system already fulfils any of the obligations inherent to the assessment by having undergone the data protection impact assessment conducted under EU data protection regulations, the fundamental rights impact assessment for high-risk AI systems will complement the data protection impact assessment, thus re-enshrining the idea of the autonomy of such regulations. [32]

The assessment seems to be conceived as a dynamic instrument because if, during the use of the high-risk AI system, the deploying officer considers that any of the elements of the assessment have changed or are no longer up to date, he will take the necessary steps to update the information, which cannot lead to any other outcome, in our view, than a new assessment.

6.3. *Sanctioning instruments to ensure compliance with the obligations of deployers*

Article 99(4)(d) of the Regulation guarantees compliance with the obligations of the deployers by subjecting them to the same system of penalties that applies to providers, which is particularly justified here because of the importance of the obligations that these operators must fulfil and because, as has been pointed out, the risks of the high-risk AI system will not always be identifiable in the development phase and will often manifest themselves in the implementation phase, with these deployers being the operators who are in the best position to assess, detect and mitigate these risks or incidences.

7. *Trade-offs between operators' obligations. Responsibilities along the AI value chain*

The Regulation, as noted above, takes into account the fact that

[32] Idea highlighted in the doctrine by M. Ebers, V.R.S. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, cit., p. 600.

throughout the chain of marketing and implementation of high-risk AI systems, changes may occur in the position of operators which should lead to a reordering of their obligations.

In section 2.1 of this chapter, we have already analysed two cases: the transformation of other operators into providers and the conditions under which the manufacturer of a product that incorporates a high-risk AI system as a safety component can also be considered a provider for the purposes of the application of the Regulation. Two further scenarios remain to be analysed: the position of providers of high-risk AI system providers and the possibility that the same operator may fulfil several conditions and have to comply with obligations for all of them.

7.1. *The position of providers of high-risk AI system providers*

The Regulation obliges any third party supplying the provider of a high-risk AI system, tools, services, components, or processes that are used or integrated into that system to specify, by written agreement with the provider, the information, capabilities, technical access, and other assistance that are necessary, based on the generally acknowledged state of the art, to enable the provider of the high-risk AI system to fully meet the obligations set out in the Regulation. [33]

This obligation does not apply to third parties making accessible to the public tools, services, processes, or components, other than general-purpose AI models under a free and open-source licence.

To facilitate compliance with this obligation, the AI Office may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties providing tools, services, components, or processes to be used or integrated in high-risk AI systems. These model clauses shall be published and be available free of charge in an easily usable electronic format.

[33] Again, this obligation is without prejudice to the need to observe and protect intellectual and industrial property rights, confidential business information, and trade secrets in accordance with Union and national law.

7.2. *Possibility for the same operator to perform several functions and shall fulfil the corresponding obligations*

Although the operative text of the Regulation does not elaborate on this with due precision, recital 83 expressly admits that, in certain situations, operators of High-Risk AI systems may perform more than one function in the value chain of these systems at the same time and therefore have to fulfil cumulatively all the relevant obligations associated with these functions. For example, an operator may act as both a distributor and an importer simultaneously, in which case it will assume all the obligations of both. However, it does not seem reasonable that the Regulation has left the compatibility regime of these figures to interpretation, an issue that should have been dealt with in a way that is more in line with legal certainty, given the intensity of the obligations at stake.