This document is a courtesy machine translation by the AEPD of the original legal report. In the event of any inconsistencies between the Spanish version and this English courtesy machine translation, please note that the Spanish version shall prevail.

As stated in the Report of Regulatory Impact Analysis (MAIN) presented together with the draft Royal Decree, Law 28/2022, of 21 December, on the promotion of the ecosystem of start-ups foresees in its articulation the creation of controlled testing environments for limited periods of time with the aim of evaluating the usefulness, feasibility and impact of technological innovations. In particular, Article 16(1) thereof provides that *public authorities are to promote, by regulation, the creation of controlled environments, for limited periods of time, to assess the usefulness, feasibility and impact of technological innovations applied to regulated activities, to the supply or provision of new goods or services, to new forms of provision or provision thereof, or to alternative formulas for their supervision and control by the competent authorities,* specifying paragraph 4 of that provision, specifying the principles to which the creation and development of controlled test environments must be adjusted.

Similarly, Annex I to the draft Royal Decree states that the European Commission has adopted a proposal for a Regulation laying down harmonized standards in the field of artificial intelligence (Artificial Intelligence Regulation) on 21 April 2021. That Commission proposal aims to ensure that AI systems placed on the Union market and used in the Union market are secure and comply with existing legislation on fundamental rights and Union values, to ensure legal certainty to facilitate investment and innovation in artificial intelligence and to improve governance and effective enforcement of existing legislation on fundamental rights and security, as well as to facilitate the development of a single market for legal, secure and reliable AI applications and to avoid market fragmentation, a list of areas of AI systems that are considered to be of high specific risk is laid down in Annex II.

I

The draft Royal Decree "*establishing a controlled testing environment for testing compliance with the proposal for a Regulation of the European Parliament and of the Council establishing harmonized standards in the field of artificial intelligence*" aims, as set out in Article 1 'Objective', *paragraph*1, to verify the design, validation and monitoring requirements to be laid down in the

development of artificial intelligence systems that may pose risks to the safety, health and fundamental rights of individuals:

> *Article 1. Object*
> *1. This Royal Decree aims to create an experience to verify the requirements in which different entities chosen by means of a public call participate, which selects, as a test, some artificial intelligence systems that may pose risks to the safety, health and fundamental rights of individuals, with the aim of developing the experience that can subsequently facilitate to all European organizations the implementation of the principles governing the design, validation and monitoring of artificial intelligence systems, and which will help to mitigate those risks.*

As stated in Article 5 "Eligibility Requirements for Access" of the Draft Royal Decree, participation in the controlled testing environment is open to providers of artificial intelligence systems (hereinafter "AI systems") and, as participating users, legal entities making use of a high-risk artificial intelligence system, general purpose systems or foundational models, provided that the provider of such systems also accesses the controlled testing environment:

> *Article 5. Eligibility requirements for access.*
> *1. Participation in the controlled testing environment is open to those AI suppliers and users resident in Spain or who have a permanent establishment in Spain, or are part of a group of entities, where the representative of the group or sole agent being a member of it, is the applicant entity and whose domicile or principal establishment is necessarily in Spanish territory for the purposes of Article 9 of Royal Legislative Decree 1/2010, of 2 July, approving the consolidated text of the Capital Companies Law.*
> *2. This environment, as a participating user, can be accessed by private legal entities and public sector entities in Spain that make use of a high-risk artificial intelligence system, general purpose systems, or foundational models, provided that the AI provider of that system also accesses the environment.*

Therefore, the controlled testing environment will be related to "AI systems" and also to the use of AI systems in treatments of certain users.

II

With regard to the processing of personal data, Article 3 of the Draft Decree lays down in paragraph 3 the definition of "artificial intelligence system":

> *'Artificial intelligence system' means: system designed to operate with a certain level of autonomy and which, based on input data provided by machines or people, infers how to achieve a set of established goals using machine learning strategies or based on logic and knowledge, and generates output information, such as content (generative artificial intelligence systems), predictions, recommendations or decisions, that influence the environments with which it interacts.*

It must be borne in mind that an AI system will be formed by an AI algorithm and other elements that will allow the implementation and effective operation of the algorithm, and that will be able to condition the operating parameters of the system in multiple aspects. In short, through incoming data, and through the application of the system algorithm, get output information, with the purpose -he adds- of achieving a set of established objectives using machine learning strategies or based on logic and knowledge.

Furthermore, Article 2(1) 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 and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) sets out the material scope of that rule *in the context of 'processing of personal data'*, not in systems, technologies or technical infrastructures:

> *1. This Regulation applies to the entire or partially automated processing of personal data, as well as to the non-automated processing of personal data contained or intended to be included in a file.*

A *processing* shall be defined, as set out in Article 24(1) GDPR, by its nature, its scope, context and purposes:

> *Taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the controller shall apply appropriate technical and organizational measures to ensure and be able to demonstrate that the processing complies with this Regulation. Those measures shall be reviewed and updated where necessary.*

The nature of a *treatment* assumes the way in which such treatment is effectively implemented. The implementation of a processing can be divided into different processing operations, as stated in Article 4.2 of the GDPR:

> *"treatment" means: any operation or set of operations carried out on personal data or sets of personal data, whether or not by automated means, such as collection, registration, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of enabling access, collation or interconnection, limitation, erasure or destruction;*

Processing operations in turn can be manual or automated, in whole or in part. Automated deployment can be done using different systems, such as mobile systems, local storage systems, cloud systems, encryption systems, video surveillance *systems or AI systems.*

In the case at hand, and as explained in the article published by the AEPD Artificial Intelligence: System vs treatment, means vs purpose[1], April 2023, the same treatment may include one or more AI systems in a specific implementation of such treatment. Therefore, in itself an AI system is not a treatment, but, in its case and not always, could be part of a treatment.

III

An AI system may not be part of the processing of personal data or in its design/development, such as in its distribution by a provider, as in its operation in the framework of a processing, or in its evolution.

For example, an AI system operating in an industrial production environment, such as an assembly line, where no personal data has been used for its development and which has no interaction or decision in relation to human operators would not be involved in a processing of the scope of the GDPR material (hereinafter GDPR processing).

However, there are several GDPR treatments in which one or more AI system could be involved as explained in the guide

1https://www.aepd.es/es/prensa-y-comunicacion/blog/inteligencia-artificial-sistema-vs-treatment-medium-vs-purpose

from the AEPD Adequacy to the GDPR of treatments incorporating Artificial Intelligence [2] published in February 2020.

First, an AI system may be involved in a GDPR processing whose purpose is the design and development of an automated system. In the event that a decision has been made to develop such automated system using AI technology, and that AI technology requires the use of *personal* data for its development (e.g. a machine learning AI system or certain rule systems) we would be in the case of GDPR processing. It should be noted that the decision on how to develop such an automated system could have opted for solutions other than AI or AI requiring personal data.

Second, an AI system could *itself* contain data from identified or identifiable individuals. This does not always occur in an AI system, nor is it unique to AI systems, but it could occur. In that case, the distribution by a provider of an AI system with such characteristics could involve the *communication of personal data*, (i.e. processing of personal data) where there is data of identifiable persons that can be *extracted from* the AI system.

Third, a *processing* may implement one or more of its operations using *one or* more AI systems to automatically process personal data, to make decisions concerning natural persons, or to profile an individual. For example, when in a recruitment process an AI system is used in the selection operations to implement a pre-filter of the most interesting curriculum vitae, which will involve processing of personal data and automated decision-making with legal effects or that could significantly affect in a similar way. It would already be a choice of the controller to add qualified human supervision in such processing.

Finally, a fourth *processing* can occur when some AI systems have the characteristic that they can evolve during the execution of the controller's processing using personal data of the processing. In relation to the treatment of evolution of AI systems, the following cases could occur: either the processing is carried out by a third party to fulfill its own purposes, either by said third party to fulfill the purposes of the controller, or by the controller himself for his own purposes.

In short, an AI system can be found within the framework of four treatment groups: design/development, distribution, operation and evolution. Each of them could involve different responsibility. The same system of

2 https://www.aepd.es/documento/adecuacion-rgpd-ia-en.pdf

AI could be in the framework of the four treatments, three, two, one or none.

IV

The draft Royal Decree establishes in Annex II a list of areas of high-risk AI systems, a concept that should be qualified in relation to the definition of high risk in the GDPR.

In relation to the *high risk*, Article 35 GDPR "*Data Protection Impact Assessment*" (DIA) provides that *the controller must establish whether a processing is of high risk to the rights and freedoms of natural persons taking into account* the nature, scope, context and purposes of the processing, in particular whether new technologies are used. The existence of a high risk in a processing is determined in a non-exhaustive manner in paragraphs 35.3 and 35.4 lists of Article 35 GDPR, in the cases of Article 32(2) or Recital 75 of the GDPR, in the cases of Article 28.2 of Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD), in the cases and examples of the WP248 Guidelines of the Article 29 Group (now the European Data Protection Board-ECDPB). in the specific legislation requiring a Data Protection Impact Assessment (DIA), in the specific cases and conditions described in the guidelines published by the EDPB for specific processing, in the specific cases and conditions described in the codes of conduct in accordance with Article 40 and in the certification mechanisms in accordance with Article 42 GDPR.

In short, the risk classification established in the draft Royal Decree complements, **but does not displace**, the risk assessment for personal data processing established in the GDPR. It complements it in the sense that it determines the high risk of those processing operations that use such systems. Specifically, in the different treatments in which an AI system is involved, it will be necessary to carry out a risk management taking into account not only the nature of one of its operations (one or several AI systems), but it will also have to take into account the risk to the rights and freedoms that imply the **joint use of all the systems that implement the treatment**, the scope or extent of said processing, the context in which it is developed and the purposes, as well as the uncertainty that may introduce the use of new technologies.

V

In the draft Royal Decree, in article 5 "*Eligibility requirements for access*", referred before, the participation of different agents is established

, such as AI providers and users, both private legal entities and members of the public sector.

In the proposals submitted, **the legal positions of each of the parties involved in the processing of personal data must be clearly defined,** whether as controllers, joint controllers, processors or sub-processors, in accordance with the GDPR, whose observance is not displaced, but reinforced by the draft Royal Decree (Article 16, Protection of Personal Data).

> *1. Participating AI providers and participating users in the controlled testing environment shall respect the applicable data protection provisions.* ***The regime for the protection of personal data in the actions carried out in the framework of this controlled testing environment is that provided for in Regulation*** *(EU) 679/2016 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 (****GDPR****) and in Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and the Guarantee of Digital Rights (****LOPDGDD****), all personal data processed in the private systems of the participating AI providers or, where applicable, participating users should remain as appropriate to verify the requirements included under that protection.*
>
> *2.* ***Acceptance of participation in the controlled testing environment will imply recognition of compliance with data protection legislation****.*

VI

Article 1(1) of the draft Royal Decree, *referred* to above, states that the aim is to draw experience on the principles that will subsequently be applied at European level for the design, validation and monitoring of AI systems:

> *...the objective of developing the experience that can subsequently facilitate for all European organisations the implementation of the principles governing the design, validation and monitoring of artificial intelligence systems, and which will help mitigate those risks.*

On the other hand, Article*4(*2) provides that AI systems are not exempted from compliance with their specific legislation, not by design but once placed on the market. In addition, provided that it has not been previously placed on that market:

Where an AI system is regulated by sector-specific legislation and has not been placed on the market or put into service prior to the request for participation in the controlled testing environment, its participation in it does not exempt from compliance that the AI system has to pass the conformity assessment in accordance with the specific legislation once the AI system is placed on the market.

In this case, it should be noted **that the provisions of the Royal Decree cannot displace the obligations of compliance with the GDPR and the LOPDGDD in the treatments in which the AI system is involved**. In particular, that the processing of personal data must be appropriate ***from the design*** of the personal data, which implies "before" their placing on the market. That is, it cannot be understood that an AI system that 'has not yet been placed on the market' can comply with the rules on the processing of personal data 'once it is placed on the market', since the GDPR is mandatory 'from the design of the AI system'.

As participation in the controlled testing environment does not exclude the obligation to comply with data protection regulations, for reasons of legal certainty an express reference should be made to Article 16 of the draft Royal Decree, amended in accordance with the observations included in this report, and even its express inclusion in Article 4.2 of the Project, or in a specific section below.

VII

Article 7 of the draft Royal Decree "*Request for access to the controlled environment of evidence*" establishes in paragraph 3 the obligation to submit a responsible declaration in relation to compliance with the regulations on the protection of personal data:

3. Applications submitted must be accompanied by: a technical report covering the content set out in Annex II; a responsible statement accrediting compliance with the regulations relating to the Protection of Personal Data; and of that documentation that was established in the call.

Unlike the technical report, which is included in Annex II to the Royal Decree, the responsible declaration does not appear in it. For legal certainty, it is suggested that the text of this declaration should appear in an Annex to the Royal Decree together with a descriptive annex to the documentation proving the principle of proactive responsibility in the same way as the technical report. This Annex must be clearly reflected,

among others, the clear identification of the treatments and the roles responsible/in charge in them in relation to the design/development, distribution, operation and evolution, the legitimacy of the treatments and, in case of high risk of the processing in accordance with **the GDPR, the favorable overcoming of the impact assessment for data protection (EIPD).**

VIII

Article 8 of the draft Royal Decree, '*Assessment of applications*', sets out in paragraph 2 the elements of the requests for access to the controlled test environment to be evaluated:

> *2. Applications for access to the environment will be evaluated for each of the AI systems received as follows:*
>
> *a) Degree of innovation or technological complexity of the product or service.*
>
> *b) Degree of social, business or public interest impact presented by the proposed artificial intelligence system.*
>
> *c) Degree of explainability and transparency of the algorithm included in the artificial intelligence system presented.*
>
> *d) Alignment of the entity and the artificial intelligence system with the Charter of Digital Rights of the Government of Spain.*
>
> *e) High risk typology of the artificial intelligence system, looking for a varied representation of typologies in the selection.*
> *f) In the case of general-purpose artificial intelligence systems, their potential to be transformed into a high-risk artificial intelligence system shall also be assessed.*
>
> *g) In the case of founding models of artificial intelligence, the deployment and utilisation capacity as well as the relative or absolute impact on the economy and society shall be assessed.*
>
> *h) The degree of maturity of the artificial intelligence system, considering that it has to be sufficiently advanced to be put into service or on the market within the time frame of the controlled testing environment or at its completion. A varied representation of maturity of artificial intelligence systems will be sought.*

i) The quality of the technical memory.

j) The size or typology of the applicant AI supplier, according to number of employees or annual turnover, the status of start-up, small or medium-sized enterprise being positively assessed to ensure a greater diversity of types of participating undertakings. A varied representation of AI supplier size and typology will be sought in the selection.

k) The participation of public sector entities, both as an AI provider and as a user, will also be positively assessed.

l) In the case where the artificial intelligence system is subject to compliance with sector-specific legislation and is on the market, a report from the Competent Authority on its correct compliance will be requested. If the report is unfavorable, a ground for refusal of the application may be deemed to exist.

m) The sector-specific compliance plan that has been implemented or designed to bring the AI system concerned into compliance with the regulations in force.

In this sense, and in relation to what is established and analysed in Article 7 of the draft Royal Decree, it is considered that, for legal certainty, it would be necessary for the evaluation procedure to include **the evaluation of the responsible declaration proving compliance with the regulations relating to the protection of personal data, and the assessment of the documentation accrediting the statements that should be attached to the responsible declaration**, as indicated above.

In turn, paragraph 2(d) of Article 8 requires an *alignment of the entity and the artificial intelligence system with the Charter of Digital Rights of the Government of Spain.* In Title X, "Digital Rights Guarantee" of the LOPDGDD (Articles 79 to 97) digital rights are established as an organic law, except for articles 79, 80, 81, 82, 88, 95, 96 and 97, which are ordinary law. Taking into account the prevalence of the rule on a non-regulatory declaration, **such as the Charter of Digital Rights of the Government of Spain, it is suggested that reference should also be made to that title of the legislation of the LOPDGDD.**

Article 12, '*Development of tests by participants*', of the draft Royal Decree, in paragraph 2, states:

> *Adapting these artificial intelligence systems to compliance with the requirements* ***does not imply*** *potential risks to the protection of consumers, users and third parties that might be affected.*

As that paragraph is worded, it could be understood that an aprioristic risk assessment ('does not involve risks') is carried out in the Royal Decree unless it is to be interpreted as meaning that the adaptation of such AI systems *should* not involve risks. If this were the latter case, the wording should be clarified. If this were not the case, and as explained in the beginning of this report, the Royal Decree would not be able to make an aprioristic assessment of the risk to the rights and freedoms established by the GDPR of a processing in which an AI system is (or is) involved. It is the responsibility of data controllers, in accordance with the GDPR, to analyse risks and assess data protection impacts (arts. 24, 25, 32, 35, etc. GDPR) by taking the necessary measures, and even demonstrating the compliance with this Regulation of the measures envisaged to address the risks taking into account the rights and legitimate interests of the data subjects and of other persons concerned (Article 35(7)(d) GDPR).

X

Article 16 of the Draft Royal Decree, Protection of Personal Data, establishes:

> *1. Participating AI providers and participating users in the controlled testing environment shall respect the applicable data protection provisions. The personal data protection regime in the actions carried out in the framework of this controlled testing environment is that provided for in Regulation (EU) 679/2016 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 (RGPD), and in Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD). all personal data processed in the private systems of the participating AI providers or, where applicable, participating users should remain as appropriate to verify the requirements included under that protection.*

The principle of lawfulness of processing (Article 5.1.a) GDPR, the principle of proactive responsibility (Article 5.2 GDPR) and the principle of data protection by design (Article 25.1 of the GDPR), state, as already mentioned, that compliance with the GDPR in the processing of personal data must be established and guaranteed before the start of the processing.

On the other hand, the principle of minimisation (Article 5.1.c of the GDPR) and the principle of retention (Article 5.1.e of the GDPR) state that the data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and maintained in a way that allows the identification of data subjects for no longer than is necessary for the purposes of the processing of personal data; personal data may be kept for longer periods provided that it is processed exclusively for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1) GDPR, without prejudice to the application of appropriate technical and organisational measures imposed by this Regulation in order to protect the rights and freedoms of the data subject.

In this case, the adequacy of the personal data used in the processing, for example, for the processing of development through training of an AI system, must be evaluated before the start of the processing, and duly accredited, where appropriate, by third parties. If it were not possible in some exceptional case, which would have to be adequately justified before the start of the project, it would have to be determined that a treatment that by design prevents such an assessment has not been implemented. This, where appropriate, could lead to a breach of data protection regulations. In another case, it would be necessary to establish, among others, the legitimacy of that conservation, the proper management of the risk to the rights and freedoms, and the application of privacy measures such as those of selecting a significant sample, if possible anonymised, with specific retention periods, or with synthetic data.

Likewise, within the framework of the GDPR it will be necessary to assess whether the operation of the AI system in an AI processing preserves the principle of accuracy (Article 5.1.d GDPR) of the decisions, profiles or values inferred. In this case, it applies what is stated in the previous paragraph.

Therefore, the wording of the article should be clarified that all processing of personal data carried out in the context of the controlled test environment has to comply with data protection regulations, in particular the GDPR and the LOPDGDD, and the applicable sectoral regulations. In addition, such compliance must be ensured prior to the processing of personal data.

Spanish Agency data protection

Article 29 of the Project "*Participation of private legal persons and public sector entities as users of an artificial intelligence system*" states in paragraph 2:

> *The private legal person or public sector entity, when acting as participating users, shall cooperate by implementing the measures specified in the guides provided by the competent body for monitoring after the implementation of the artificial intelligence system.*

To the extent that the processing involving the AI system processes personal data, decisions about persons or profiles, the legal position of the user GDPR should be defined in relation to the developer, system provider or system evolver. That circumstance should be reflected in that section, making a reference to what has been observed on the Responsible Declaration and the accreditation of the declaration. With regard to the evolution of the AI system, the roles are more complex, we could enter a scenario of responsible-responsible communication or responsible-in charge situations, in which case the provisions of Article 28 must be taken into account specifically.

XII

Annex II "*List of areas of specific high-risk artificial intelligence systems*" lists a set of AI systems that the Royal Decree establishes of high risk.

As noted in section IV of this report, the risk classification set out in the Draft Royal Decree complements, but does not displace, the risk assessment for personal data processing set out in the GDPR. In particular, in the different processing of personal data in which an AI system is involved, it will be necessary to carry out a risk management taking into account not only the nature of one of its operations (one or several AI systems), but also the risk to the rights and freedoms involved in the **joint use** of all the systems that implement the processing, the scope or extent of such processing, the context in which it is developed and the purposes, as well as the uncertainty that may introduce the use of new technologies. To the extent that the processing is of high risk of processing in accordance with the GDPR, it will be necessary to overcome the Data Protection Impact Assessment (DIA) prior to the execution of such processing.

All this without prejudice to the fact that any of the high-risk systems that could participate in the controlled test environment, such as the one described in section 7a "*artificial intelligence systems intended for use by the*

competent public authorities or on their behalf as polygraphs and similar tools, or to detect the emotional state of a natural person;" in which there is no restriction of their use to their use for the purpose of, for example, investigation of criminal offences, or 8a "*artificial intelligence systems intended for use by a judicial authority or on its behalf for the interpretation of facts or the law to apply the law to a specific set of facts*" should have a **prior analysis of the lawfulness** of the processing.

XIII

Annex IV to the draft Royal Decree, within the '*Technical Documentation to be submitted at the end of the implementation of the requirements*', states in point 3:

> *Detailed information on the supervision, operation and control of the artificial intelligence system, in particular with regard to: their capabilities and performance limitations, including the degrees of accuracy for the specific individuals or groups of persons on whom the system is intended to be used and the overall level of accuracy envisaged in relation to their intended purpose; sources of risk to health and safety, fundamental rights and discrimination in view of the intended purpose of the artificial intelligence system; the necessary human oversight measures in accordance with Article 11 and the guides provided by the competent body for that purpose, including technical measures put in place to facilitate the interpretation of the output information from artificial intelligence systems by system users; specifications on input data as appropriate;*

With regard to the processing of personal data, the aspects indicated in this point should be established according to the impact they may have on the user's processing, or the intended purposes and specific contexts of operation, for which the system is validated. In particular, performance metrics, which should be selected according to the purposes and contexts of operation and evaluated in relation to the risk that they may entail for the rights and freedoms of citizens in the framework of the processing of personal data carried out by a user.

XIV

Finally, and in the light of all the above, it is not shared, and in the opinion of this Agency should be amended to express that the treatments derived from the project can be considered to be of high risk in terms of data protection, and to establish how this

circumstance in the text, as expressed in paragraph 8, *Consideration of other impacts*, of the MAIN, which states:

> *There are no other impacts. Since personal data provided by companies will not be accessed and, in any case, the specific regulations related to Data Protection will be respected. (...)*

Precisely, the risk would not only occur "if the data provided by companies were accessed", but also that companies access "high-risk" data as data controllers. Certainly, as stated above, the Royal Decree cannot exempt from compliance with data protection regulations, and from the design, but that does not mean that in those processes there are not some "high risk" (in particular, all those provided for in Annex II, from the perspective of the draft Royal Decree), but also those that result in having such a consideration of the application of the GDPR directly.