URÍA
MENÉNDEZ

# Main conclusions of the AEPD Guidelines for the "Conformity with the GDPR of processing of personal data using Artificial Intelligence"

March 2020

# Purpose and scope

The purpose of the Spanish Data Protection Authority (the "**AEPD**") guidelines for the "*Conformity with the GDPR of processing of personal data using Artificial Intelligence*" (the "**Guidelines**") is to be an "*initial approach*" to the alignment with the General Data Protection Regulation (the "**GDPR**") of processing of personal data carried out using artificial intelligence ("**AI**"). Thus, the AEPD does not intend to carry out an exhaustive review of what has been established in the GDPR, but rather address doubts regarding the processing of personal data and highlight the most significant aspects of the AI-GDPR relationship that should be taken into account during design and implementation of personal data processing that includes AI.

In particular, in the Guidelines, the AEPD provides criteria regarding:

- The **information** that must be delivered to the data subjects whose data is processed in an AI system.
- The **roles** assumed by the different stakeholders participating in the creation, development and use of an AI system.
- The **technical and organisational measures** to be applied by the data controllers to mitigate or eliminate certain risks inherent to the use of AI systems.

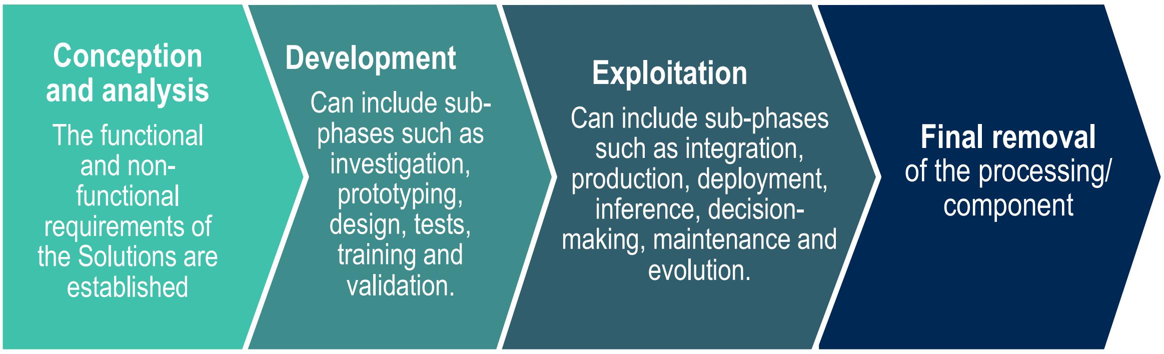
# Questions and general definitions about AI technology

**Analysis of weak AI.** The AEPD sets out certain preliminary considerations about the definition, concept and main characteristics and kinds of AI (e.g. machine learning). It distinguishes between three categories: strong, general and weak AI, and highlights that the Guidelines focus on dealing with the conformity with the GDPR of processing that incorporates weak-AI components (i.e. technological solutions that able to solve a specific and delimited problem).

**Involvement of personal data (or not).** The AEPD recognises that AI components processing natural persons' data (e.g. a marketing profiling model) can be distinguished from those that do not imply personal data processing (e.g. weather-prediction models).

Regarding solutions that process personal data, different kinds are mentioned, such as those that can make predictions about a subject, those that perform an evaluation of the subject's current status, or even those that decide on the performance of a set of actions. It is also noted that when it comes to decision making, AI can adopt two roles: (i) one where it provides assistance to the decision-making process in order for a human to adopt the final decision, and (ii) one where it adopts and (autonomously) executes the decision.

The Guidelines highlight that, generally, the AI component will not operate in isolation, rather it will be a part of a broader processing and may connect with other technologies or acts of processing such as big data, IoT or 5G, and that all human and technological elements must be taken into account to determine the implications of carrying out data processing that incorporates an AI solution.



**Conception and analysis**
The functional and non-functional requirements of the Solutions are established

**Development**
Can include sub-phases such as investigation, prototyping, design, tests, training and validation.

**Exploitation**
Can include sub-phases such as integration, production, deployment, inference, decision-making, maintenance and evolution.

**Final removal**
of the processing/ component

**Ethical challenges**. Lastly, the AEPD highlights the ethical – and not only legal – challenges that may arise from the use of this technology, such as discriminatory biases or the risks of acceptance of results without critical thinking, and the need to evaluate this ethical dimension throughout the whole life cycle of an AI solution.

# Identification of processing and roles

Having made these preliminary considerations, the Guidelines focus on analysing the personal data processing that may be realised in an AI solution, as well as identifying the roles (controller vs processor) of the different participants in the development and/or management of an AI considering the different phases of its life cycle.

### WHAT PERSONAL DATA PROCESSING OCCURS THROUGH USE OF AN AI?

| | |
|---|---|
| **Training** | definition / searching and obtaining of the data set / pre-processing (processing of non-structured data, cleaning, weighing, selection, transformation) / splitting of the data set for its verification / traceability and auditing. |
| **Validation** | may imply data processing if real data are used to ascertain the goodness of fit. |
| **Deployment** | may imply data communication if the AI solution is distributed to third parties including personal data or if there is a way to obtain them. |
| **Exploitation** | • Inference: when the data of the data subject are used to obtain a result, when third-party data are used with the same purpose or when data and inferences of the data subject are stored.<br>• Decision-making: making a decision regarding a data subject is data processing.<br>• Evolution: if data and results of the data subjects are used to refine the AI model. |
| **Removal** | can have effects on processing that amounts to local, centralised or distributed erasure of data, as well as on the portability of the service. |

The AEPD notes that not all AI solutions process personal data throughout their life cycle but warns that if it is considered that they do not process personal data (e.g. because they were eliminated or anonymised), then **the effectiveness of those procedures must be proven and the risk of re-identification evaluated.**

## WHAT ROLES DO THE PARTIES INVOLVED IN THE USE OF AI HAVE?

During the exploitation phase of the system incorporating the AI solution we can encounter various different situations:

1 The owner of the AI gives Access to the solution to all data subjects who underwent the AI processing (e.g. an AI tool that carries out a psychological evaluation of the users of a social network).

2 The owner of the AI transfers the rights of use of the AI solution to a third party.

3 An entity decides on the purposes of an act of data processing, and hires the owner of the AI to execute one or several phases of that processing (data controller – data processor).

The entity that takes the decision to use, within the scope of a processing of personal data, an AI solution, will be considered the **data controller** due to being the entity that "*determines the means and purposes of the processing*".

The decision of using a technical solution based on an AI is taken by the data controller and, for this reason, the data controller must decide if opting for one technological solution or another. Therefore, data controllers must be diligent when choosing an AI solution and know how it functions and the data processing that will occur within that solution, not being able to hide behind a lack of information or technical knowledge. In consequence, the AEPD does not find acceptable that the data controller transfers the responsibility to the own system.

### WHAT ROLES PARTICIPATE IN THE DIFFERENT PHASES OF AN AI COMPONENT'S LIFE CYCLE?

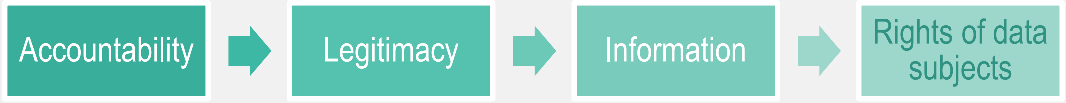
Leaving aside and without evaluating possible cooperative network models and joint-responsibility models, the AEPD determines that the roles of the different participants in the different steps of an AI's life cycle can be summarised as follows:

| PHASE | CONTROLLER | PROCESSOR |
|---|---|---|
| **Development / Training** | • Entity defining the AI's purposes and deciding which data are going to be used to train the AI.<br>• Entity developing the AI if it adopts decisions for its own purposes over the data to be used for its training. | • Third party contracted for the training or development of the AI if the contracting party determines the main terms and characteristics of the processing (irrespective of the origin of the data: whether provided by the contracting party or collected by the contracted party). |
| **Validation** | | |
| **Deployment** | • Entities selling and buying the AI solution containing personal data (data communication), except if the solution is sold to a natural person for his or her personal use (application of the domestic exception). | • Entity providing the AI solution to a third party for its use in the scope of a provision of services and that does not process the data for its own purposes. |
| **Inference / profiling** | • Entity processing the data contained in the AI solution for its own purposes, except if the processing is performed by a natural person within the scope of an exclusively personal or domestic activity. | • Entity providing the AI solution to a third party for its use in the scope of a provision of services and that does not process the data for its own purposes. |
| **Decision-making** | • Entity adopting automated decisions over the data subjects for its own purposes. | • Entity providing the AI solution to a third party for its use in the scope of a provision of services and that does not process the data for its own purposes. |

| PHASE | CONTROLLER | PROCESSOR |
|---|---|---|
| **Evolution** | • Entity communicating to a third entity the users data.<br>• Entity determining the development of the AI. | • Contracted entity processing the data within the AI system for the purpose of providing a service. |

# Compliance with the regulations: accountability, legitimacy, information and rights of data subjects

The AEPD sets out a series of conditions to be fulfilled in order to guarantee that the processing carried out through an AI solution complies with the data protection regulations, among which it highlights the need for compliance with the following key elements:



Particularly worthy of attention is the fact that the AEPD establishes, within the Guidelines, that an AI solution will not be mature and therefore will not be able to comply with the principle of accountability, transparency and lawfulness if it does not guarantee certain technical elements such as (i) precision, accuracy and measurement of error; (ii) predictability of the algorithm, or (iii) consistency of the results of the inference procedure.

### ON WHAT LEGAL GROUNDS CAN DATA PROCESSING BE CARRIED OUT WITHIN AN AI?

The legal basis that will usually legitimate the processing of personal data within an AI solution are the following ones:

**More common**

- Need to process the data to perform an agreement or apply pre-contractual measures (e.g. establishing an agreement with a data subject for the use of his or her data in the AI's training).
- Legitimate interest.
- Consent, considering that subsequent removal of the consent will not affect the processing carried out up until that moment. The withdrawal of consent will not have retroactive effects in relation to the results obtained by the processing carried out.

**Unusual**

- Protection of vital interests.
- Reasons of substantial public interest on the basis of EU or Member State law.
- Compliance with legal obligations set out in an EU or Member State law.

If **third parties' data sets** are used to train the AI, the data controller must demonstrate that it has exercised the required diligence to check the lawfulness of the origin of the data acquired (e.g. that the agreement with the third party which provided the data set includes clauses in which the data controller requests evidence and warranties about that lawfulness).

Regarding the processing of special categories of personal data, the AEPD notes that the GDPR determines that decisions based solely on automated processing will not be based on special categories of personal data, except (i) if the data subject has provided his or her consent to do so, or (ii) if the processing is necessary for reasons of substantial public interest.

Finally, the AEPD highlights the possibility that the personal data can be processed for different purposes to those for which the data were initially collected as long as the data controller complies with all the requirements to carry out a lawful processing of those data.

## HOW CAN THE DATA CONTROLLER COMPLY WITH THE TRANSPARENCY PRINCIPLE? WHAT INFORMATION MUST BE PROVIDED TO DATA SUBJECTS?

The AEPD places particular emphasis on the transparency principle, establishing that this is a critical aspect as the information provided to data subjects must allow them to understand the impact of the use of AI solutions in the processing of their personal data. Such information should not only be provided at a precise moment but dynamically throughout the processing of personal data. For this reason, in the Guidelines, the AEPD establishes certain criteria regarding how to be transparent with data subjects that exceed the usual conception of "transparency", implying that data controllers must make an additional effort to comply with the transparency principle while processing personal data in an AI solution.

**Information to supply during the training phase**. The AEPD highlights the necessity to clearly inform the data subject about the possibility that he or she may be reidentified through the data included in the model.

**Certification**. One of the key problems is confidentiality to protect industrial property. Certification mechanisms can be used to enhance transparency regarding the processing of personal data.

**First layer of information**. Data subjects must be informed about the processing of their personal data according to Articles 13 and 14 of the GDPR, with it being necessary to adapt the information to the peculiarities of each phase of the life cycle of the AI in which the processing is taking place.

The AEPD emphasises that the first layer of information must contain, in addition to the information set out in article 11 of the LOPDGDD, information about the compiling of profiles or about automated decision making, with it being obligatory to inform about (i) the right to object to such processing, (ii) the logic involved and (iii) the envisaged consequences of such processing for the data subject.

Regarding information about the logic involved, the AEPD considers that the data subject must be provided with information that makes him or her conscious about the processing that is being carried out with his or her data and that provides him or her with certainty and confidence regarding the results adopted through the algorithms used. As an example, the AEPD highlights that the information that might be relevant for the data subject could be the following:

- Details of the data used in the decision making and the importance of each of them in the process of making such decisions.
- Quality of the training data and the patterns used.
- Profiles used and implications.
- Precision or error values according to an adequate metric to measure the goodness of fit.
- Existence – or not – of qualified human supervision.
- Reference to audits and certifications of the system.
- If the AI system contains third-party data, the prohibition of processing such information without a legal basis and the consequences of doing so.

**Personnel of the data controller**. The data controller must provide clear information and specific training to its personnel about the limitations of the AI. Moreover, if the AI system is used as a tool to assist with the taking of decisions, the data controller must implement information, training and audit measures to manage the risk of the personnel merely following the automated decision.

**Data Protection Officer ("DPO").** Even if in certain cases it may not be mandatory for the data controller, the AEPD highlights that appointing a DPO may be useful for companies that use AI systems or develop AI solutions.

## HOW TO ENSURE THAT THE RIGHTS OF THE DATA SUBJECTS ARE RESPECTED

The AEPD places particular emphasis on data controllers establishing mechanisms and procedures to manage data subjects' requests starting from the design phase of the processing or AI system.

Moreover, if the AI solution contains personal data at the time it is distributed, the AEPD establishes that the data controller must do the following:

- Erase the personal data or, on the contrary, justify why it is impossible to do so.
- Determine the legal basis for carrying out the disclosure of data to third parties and inform the data subjects about that disclosure of data.
- Demonstrate that the privacy-by-design and by-default measures have been executed.
- Carry out a privacy impact assessment depending on the risks.

The AEPD also highlights the importance of implementing within the AI system the possibility of blocking (*bloquear*) the personal data relating to the inference procedure (at a minimum, the entries and results obtained) that are necessary to handle a claim by a data subject.

The AEPD also includes a series of points regarding three particular data protection rights:

- **Right to rectification**. Inaccurate data may exceptionally be processed if they are used to anonymise and prevent the reidentification of data subjects as long as such processing of inaccurate data does not have any effects on the data subject.
- **Right to data portability**. The data controller must evaluate and document whether the processing of personal data is subject to the right to data portability.

- **Right to not be subject to a decision based solely on automated processing**. The data controller must always provide the option for a human operator to ignore the algorithm used. For this reason, the AEPD recommends documenting incidents and questions received from data subjects regarding automated decisions in order to be able to assess and detect situations in which human intervention may be necessary.

Finally, the Guidelines highlight that automated individual decision-making can only be used in relation to the **personal data of minors** when (i) it is essential to protect the minor's well-being, **and** (ii) the adequate guarantees have been implemented.

# Risk management

In the Guidelines, the AEPD emphasises the importance of implementing adequate and proportional technical and organisational measures to ensure an adequate level of security, and which should be determined through a risk analysis. This analysis consists in two differentiated phases:

(i) A **first phase** in which the threats are identified and the level of the intrinsic risk that exists is evaluated.

(ii) A **second phase** in which the proportional and adequate technical and organisational measures are implemented in order to eliminate or mitigate that risk.

## 1. IDENTIFICATION OF THE THREATS

The data controller should be capable of identifying the additional risks that may arise from using and implementing an AI. As privacy impact assessments ("**PIAs**") must be carried out when the data controller carries out profiling activities or automated individual decision-making, and through those PIAs the data controller will established the specific and concrete measures to manage the risk .

## 2. DETERMINING THE TECHNICAL AND ORGANISATIONAL MEASURES

After carrying out the relevant risk analysis, the data controller must determine the necessary technical and organisational measures to eliminate or mitigate the risk. In relation to the use of AI systems, the AEPD highlights the following measures:

| | |
|---|---|
| **Transparency principle** | See measures established in section "***How can the data controller comply with the transparency principle? What information must be provided to data subjects?***" |

| | |
|---|---|
| **Accuracy principle** | **Factors.-** Three factors affect the accuracy of data:<br>• There are systems which, due to their own implementation, can include errors in the system, others where errors are included through external elements (e.g. through biometric readers) and, finally, ones where errors can be introduced through programming or design errors.<br>• Errors contained in the training or validation data set.<br>• Biased evolution of the AI model.<br>**Biometric information.-** Due to their special nature, particular importance must be assigned to the accuracy of biometric data (e.g. facial recognition, fingerprints, voice). |
| **Minimisation principle** | **Limitations.-** Minimisation includes implementing the following limitations from the conception of the AI solution:<br>• Limiting the extent of the types of data processed to those necessary in each phase.<br>• Limiting the level of detail or accuracy of the information.<br>• Limiting the number of data subjects whose personal data are processed.<br>• Limiting the accessibility of different categories of personal data to the personnel or the final user in each and every one of the phases.<br>**Techniques.-** Different data-minimisation techniques exist, out of which must be highlighted (i) the erasure of non-structured data or unnecessary information collected during the pre-processing of the information, (ii) data aggregation, and (iii) anonymisation and pseudonymisation.<br>**Inclusion of third-party data in the distributed AI solution.-** In the event that the AI solution is distributed with third-party data, the data controller must (i) formally assess which personal data will be contained in such solutions (i.e. to what extent persons are identifiable); and (ii) apply technical, organisational and legal measures to minimise the identification or to reduce the extent of the identification to the minimum number data possible. |

| | |
|---|---|
| **Security** | **Specific threats.-** Specific threats exist for AI systems, out of which the AEPD highlights the following:<br>• Accessing and manipulation of the training data set.<br>• Inclusion of Trojans or back doors within the code or development kits.<br>• Manipulation of users' APIs in order to access the model and alter the parameters, filters and carry out attacks on integrity and availability.<br>• Filtration and accessing of the logs that result from the inferences generated through interaction with the data subjects.<br>**Logs.-** Collection of logs makes up a part of the strategies for complying with the accountability principle. Data controllers must provide the following evidence:<br>• Determine who and in which circumstances the personal data included in the model are accessed.<br>• Provide traceability regarding the updating of the inference models, communications of users' APIs with the model and detection of intrusion or abuse attempts.<br>• Provide traceability in order to allow governance of the disclosure of data between the parties participating in the AI solution.<br>• Track the inference quality parameters when the AI is used for decision-making or for procedures to help with decision-making.<br>**Legal basis for the creation and maintenance of logs.-** The AEPD highlights that the possibility of processing the personal data contained in these types of files has a basis in different legal grounds set out in Article 6 of the GDPR, with the most important ones being (i) the existence of a legitimate interest in guaranteeing the security of the network and information, and (ii) compliance with legal obligations (e.g. those deriving from Spanish Law 10/2010 of 28 April on the prevention of money laundering and financing of terrorism). |

| | |
|---|---|
| **PIAs** | **High risk and weighting.-** The AEPD places special emphasis on the fact that processing of personal data within the context of an AI solution may imply a “high risk” for the rights and freedoms of the data subjects. For this reason, it highlights data controllers’ obligation to assess the possibility of carrying out such processing using another solution through which the same functionality can be achieved (with an acceptable performance margin) and that poses less risk for the rights and freedoms of data subjects. In conclusion, the data controller must carry out this weighting and may use the AI solution if more benefits and advantages are produced for public interest and society than harm to the rights and freedoms of data subjects. |
| **Audits** | Throughout the entire life cycle of the AI solution the data controller must carry out data processing audits in order to verify the conformity of that processing with the data protection regulations. Moreover, it must be determined whether the AI solution is being used for the purpose for which it was designed and, if it has been purchased from a third party, it must be analysed whether collateral functions that may have regulatory implications are being carried out by the AI solution (e.g. the AI system carries out parallel processing of personal data different from those managed by the data controller, such as analytical functions). |

# International transfers

There are several scenarios in which cross-border flows of personal data can be carried out while using an AI system, such as when the development or deployment of the system is cloud based, when the personal data are disclosed to third parties for the evolution of the AI model, or when the AI component is distributed with third-party personal data. In this regard, the AEPD highlights the importance of such transfers complying with the obligations set out in the GDPR, in particular (i) the duty to inform, and (ii) the guarantees set out in Chapter V of the GDPR.

# Contact lawyers

**Leticia López-Lapuente**
*Partner*
+ 34 91 586 01 31
leticia.lopez-lapuente@uria.com

**Reyes Bermejo**
Managing associate
+34 96 352 91 91
reyes.bermejo@uria.com

**Laia Reyes**
Senior associate
+34 91 586 01 31
laia.reyes@uria.com

**Carolina Moniz Pina**
Senior associate
+34 91 586 01 31
carolina.monizpina@uria.com

**Lidia Gimeno Rodríguez**
Junior associate
+34 91 586 01 31
lidia.gimeno@uria.com

BARCELONA
BILBAO
LISBOA
MADRID
PORTO
VALENCIA
BRUXELLES
LONDON
NEW YORK
BOGOTÁ
CIUDAD DE MÉXICO
LIMA
SANTIAGO DE CHILE
BEIJING

www.uria.com

This newsletter provides general information and does not constitute legal advice