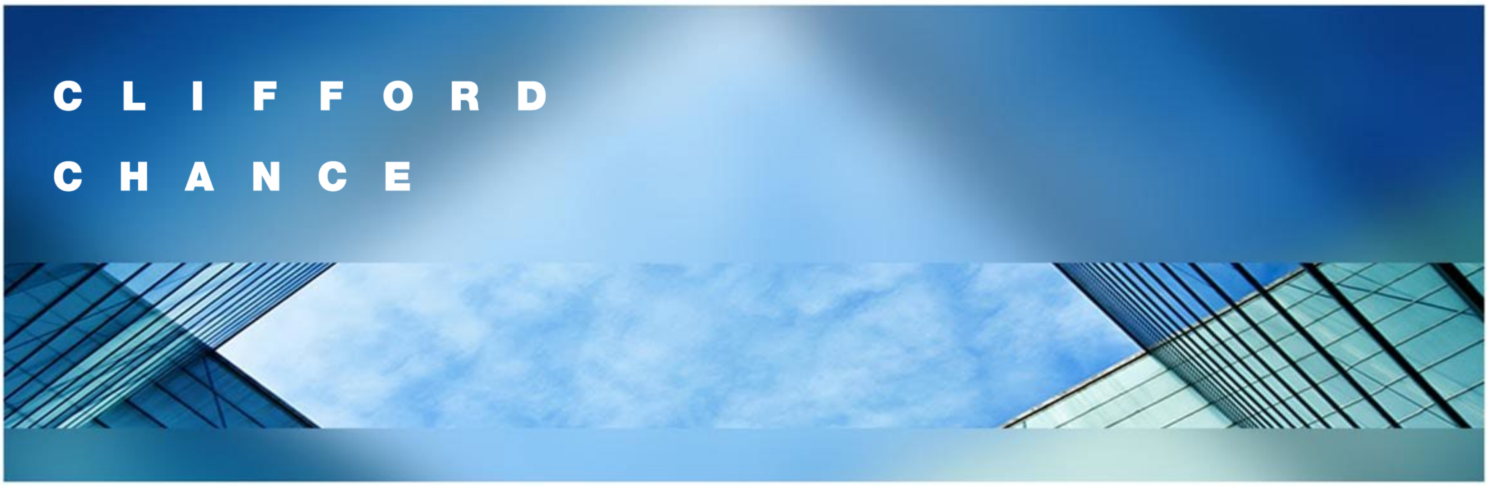

DATA PROTECTION AND ARTIFICIAL INTELLIGENCE: THE NEW AEPD GUIDELINES

The Spanish Data Protection Agency ("**AEPD**") has published new guidelines on compliance by processing techniques that use artificial intelligence with the General Data Protection Regulation ("**GDPR**"), in which the AEPD seeks to highlight the most relevant aspects in the relationship between artificial intelligence and personal data protection.

Last February, the AEPD published the guidelines entitled "GDPR Compliance of processing that uses Artificial Intelligence. An introduction" (the "**Guidelines**"), which is accessible in its entirety at: Guidelines

The Guidelines are directed at data controllers that use components of artificial intelligence ("**AI**") in processing, as well as the developers and processors who provide support.

The Guidelines focus on processing that uses components known as weak AI (which refers to solutions able to resolve a specific, limited problem), omitting strong AI and general AI solutions (those which go beyond human abilities – or superintelligence – and those able to resolve any intellectual task that can be resolved by human beings, respectively).

As the AEPD recognises, despite their length, the Guidelines do not intend to provide an exhaustive analysis of the relationship between data protection and AI.

Below are some aspects of the Guidelines that we deem to be of greatest interest.

1. COMPREHENSIVE VISION OF PROCESSIG WITH AN AI SOLUTION

The Guidelines adopt a comprehensive vision of possible personal data processing with an AI solution, highlighting that there can be personal data processing in all stages of the AI solution's lifecycle, starting with the "training" phase of the system, continuing through the "validation", "roll-out" and "operation" stages, and finishing with the service "withdrawal" phase (the "**Stages**").

Key points

- **AI is here to stay**: in addition to these Guidelines, in January 2020 an international conference on data protection and AI was held in Brussels, organised by the *Computers, Privacy & Data Protection* platform, and it has just been a few days since the European Commission published its White Paper on AI, which contains numerous references to data protection.
- **Duties of information are enhanced**: the first layer should include "*meaningful information about the logic involved*" and "*the significance and the envisaged consequences*".
- **Under no circumstances can the AI system itself be held responsible.**
- Moreover, the Guidelines include an Annex with a non-exhaustive list of the **AI-based services currently being provided**: product recommendation based on customer profiling and the analysis of purchases, intelligent assistants or appliances (*IoT*), or the monitoring of transactions to detect fraudulent activities based on consumer habits.

While not all AI solutions will process personal data in some (or all) of the Stages of their lifecycle, it will be necessary – in line with the principle of data protection by design and by default– to carry out an analysis and determine in advance what specific personal data processing is to be carried out.

2. THE ROLE OF EACH OF THE ACTORS INVOLVED IN THE AI SOLUTION

The Guidelines offer examples of the different (controller/processor) actors that intervene in each of the Stages. Thus, at the training phase, the role of the controller will correspond to the entity that defines the purposes of the AI component and decides what personal data is to be used for training the system, while the entity hired to assist with the training will generally be considered the processor.

3. THE LEGITIMATE PURPOSES OF THE PROCESSING

As with any processing, the first step will consist of establishing a legal basis for legitimacy, which may vary depending on the Stage in question, the most common being (i) performance of an agreement, (ii) legitimate interest (in which case there will have to be a mandatory prior assessment which, according to the Guidelines "*requires a greater degree of commitment, formality and competence of the controller*"), or (iii) consent of the interested parties.

Particular attention must be paid to special data categories, as well as to automated individual decisions based solely on automated processing (without human intervention), and profiling.

4. THE ENHANCED DUTY OF INFORMATION

With regard to the duty of information, the Guidelines follow the two-layer approach (article 11 of the Organic Law on Data Protection and Safeguarding Digital Rights), but with greater demands in the first layer. A technical reference to the implementation of the algorithm in question will not be sufficient. Instead, information supplied must make it possible to understand the behaviour of the processing by means of the inclusion, for example, of (i) details of the data used and its age; (ii) its respective importance for adopting the decision: (iii) its quality and they type of patterns used: (iv) profiling carried out and implications thereof; (v) whether or not there is qualified human supervision; (vi) a reference to audits carried out of the AI system; (vii) as well as whether the AI system contains information on identifiable third parties, the prohibition on unlawful processing that information and the consequences of doing so.

5. THE BLOCKING OF DATA: PARTICULARITIES

The Guidelines indicate that there is a specific obligation to block data relating to the inference process ("*at least entries and results obtained*") when an AI solution is selected or developed.

6. DECISION-MAKING BASED SOLELY ON AUTOMATED PROCESSING

In AI solutions it will often be possible to adopt decisions that affect individuals and that are based solely on automated processing, but it will be mandatory for at least one of the exceptions envisaged in article 22.2 GDPR to apply (including explicit consent of the data subject).

In the event the explicit consent is chosen, the Guidelines recommend designing processing in such a way as to protect the freedom of choice of users (and therefore, that it can be considered to have been freely granted).

The Guidelines strongly recommend that AI-based processing always be subject to human supervision, giving the option for a human operator to ignore the algorithm at a particular point.

7. DATA CONTROLLER PERSONNEL

The Guidelines also envisage that controllers will be obliged to provide their personnel with "*precise information and specific training*" on the limits of the AI system.

It will be necessary to avoid personnel (human element) acting as a "*mere conveyor belt*" of the inferences carried out by the AI solution and to prevent errors of interpretability on the part of operators. Information and training are a manifestation of the accountability principle on which the GDPR is based.

8. BIAS AND ACCURACY

The accuracy of data is essential in the context of AI solutions, meaning that the controller must ensure that the data processed and, above all, that generated and linked with the interested party, is accurate.

With a view to avoiding any risks in this regard, the controller must implement techniques designed to examine and determine the possible existence of bias in the algorithms used (*Algorithmic Impact Assessment*).

9. SPECIFIC SECURITY THREATS

As with any processing, controller and processor are obliged to adopt the appropriate security measures to ensure a level of security appropriate to the risk.

Nonetheless, the measures will have to be appropriate for AI systems, which have specific risks and "*defined types of attack and defence*" (adversarial pattern poisoning, inclusion of backdoors during the AI development process, adversarial machine learning attacks, etc…).

10. AUDIT

Finally, also in line with the accountability principle, it will be necessary for controllers and processors to carry out an audit to determine whether the AI solution is in line with GDPR requirements and verify the validity of the processing based on these solutions.

All in all, the Guidelines represent a gradual approach to one of the most important legal challenges of our times: how to ensure that the benefits associated with the use of AI are compatible with respect for fundamental rights.

CONTACTS

Josep Montesfusco
Partner

T +34 93 344 22 25
E josep.montefusco
@cliffordchance.com

Fernando Irurzun
Counsel

T +34 91 590 41 20
E fernando.irurzun
@cliffordchance.com

Manel Santilari
Associate

T + 34 93 344 22 84
E manel.santilari
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, Av. Diagonal 682, 08034
Barcelona, Spain

Clifford Chance, S.L.P.U.

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.