# First measures for compliance with the General Data Protection Regulation: the Spanish Agency takes the first step

**Data Protection Area, Gómez-Acebo & Pombo**

*The Spanish Data Protection Agency (AEPD) takes the first step and publishes a package of documents consisting of two guides and guidance that are issued as guidelines for action by small to medium-sized enterprises to comply with the provisions of the General Data Protection Regulation (GDPR).*

The new documentation package published by the AEPD is aimed at SMEs so that they are aware of the impact that the Regulation will have on the way they must process data and they adapt their processes to the new legislation, taking into account the change in the model of compliance as well as the requirement of a more active commitment. Needless to say, although SMEs are the objective scope, the three documents also serve as guidelines for those considered large enterprises.

The issue of the above-mentioned three documents has been accompanied by the AEPD's announcement of the measures it is working on: the creation of a section specific to the GDPR on the AEPD's website, the preparation of an online self-assessment tool so that companies can quickly and easily assess if their data processing is high or low risk, and the new Data Protection Bill.

*General Data Protection Regulation Guide for controllers*. The first paper is as an open, non-exhaustive and non-definitive document that includes, in this order, a series of interpretations, proposals and recommendations that didactically guide the controller and processor in the identification of the measures to be taken. As the AEPD itself points out, some recommendations or interpretations can be implemented almost immediately, a case in point being the manner in which consent is to be obtained. In other cases, the GDPR must apply before some measures can be taken.

This Guide includes issues such as the legitimate grounds for data processing, transparency in the duty to provide information, rights and procedures to be followed, the controller-processor relationship, accountability measures, international data transfers and the processing of a child's data. In addition, the last two points of the Guide, under the headings of "Checklist" and "Simplified

Checklist", provide a questionnaire with which the controller and processor can self-assess their situation against the main obligations under the GDPR. It should be noted that in the case of the so-called Checklist, the AEPD refers to organisations and in the case of the Simplified Checklist, the AEPD refers to SMEs; the foregoing corroborates what was mentioned above concerning the scope of application of these documents.

Considering the content of the Guide, it would seem that the work of adapting to the GDPR would commence from the end; that is, by answering the questions included in the Checklist.

*Guide to comply with the duty to provide information*. In the second of the published documents, by way of recommendations and practical solutions, the AEPD aims to guide SMEs in their compliance with the duty to provide information, which has been hardened by the introduction of new information requirements in respect of data subjects under the GDPR (arts. 13 and 14). The AEPD, in tune with other Data Protection Authorities, proposes to implement a "layered" information model similar to the one already proposed for compliance with the duty to provide information regarding the use of cookies. Thus, in a first layer the data subject would be offered certain basic or summarized information in the form of a synoptic table (similar to that of nutritional information on food products) in connection with the most important headings (controller, purpose, legitimate interests, recipients and rights). This layer would refer to a second layer of additional information where the information required by the GDPR would be provided in detail.

Hence, traditional privacy policies may not be sufficient to meet the requirements under the GDPR, making it necessary to examine and synthesise its contents so as to enable interested parties to gain quick and clear understanding of the same.

*Guidance in drawing up contracts between controllers and processors*. The GDPR lays down the obligation to regulate in a contract (data processing contract) the relationship between the controller and processor. The guidance issued by the AEPD sets out the minimum content that these contracts must include in order to comply with the requirements under the GDPR. Among other novelties, the GDPR requires that these contracts clearly state whether it is the responsibility of the processor to handle and respond to requests for exercising the data subject's rights, or if the processor's only obligation is to communicate to the controller that such right has been exercised. The GDPR further requires that the parties define in the contract the final destination of the data. The contract must therefore specify whether, after completion of the processing, the processor should return or delete the personal data, as well as the manner and time limit in which such obligation must be fulfilled. Therefore, envisaging both options in the contract, leaving the choice of one or the other for a later time, is not possible. The guidance includes as an Annex an example of contractual clauses for those cases where the processor processes the data on his premises and exclusively through his systems. In addition, said guidance answers ten basic questions concerning the regulation of the processor, his relationship with the controller and the scope of application of the GDPR. It is important to note that the GDPR will apply not only to data processing carried out by a processor established in the Union, but also, on certain occasions, to the processing performed by a processor not established in the Union.

It is therefore the responsibility of the SMEs to work, as soon as possible, on identifying processors who currently access their personal data and to review the current data access contracts/clauses signed with them for the purpose of verifying whether such contracts are consistent with the guidance. Likewise, the drawing up of a new data access agreement template that includes the required minimum content is advisable for SMEs.

*For any questions please contact:*

**Isabel Crespo Vitorique**
*Senior Associate, Madrid*
Tel.: (+34) 91 582 91 00
icrespo@gomezacebo-pombo.com