G A _ P

Gómez-Acebo & Pombo

The new Spanish Data Protection Act What must I do?

Isabela Crespo Vitorique
Senior Associate, Intellectual Property and Information Technologies Practice Area, GA_P
Privacy and Technology Industry

Bárbara Sainz de Vicuña Lapetra
Senior Associate, Intellectual Property and Information Technologies Practice Area, GA_P
Privacy and Technology Industry

Following the application of the General Data Protection Regulation as per Article 99 thereof, a new Data Protection Act has been passed and is awaiting publication to adapt the Spanish legal system to the aforementioned EU regulation and thereby ensure legal certainty.

The new Data Protection and Digital Rights Guarantee Act (LOPD) is here to stay. The LOPD will enter into force the day after its publication in the Official Journal of Spain in order to complete the adaptation of the Spanish legal system to the EU General Data Protection Regulation (GDPR). The LOPD comprises ninety-seven articles structured around ten titles, twenty-two additional provisions, six transitional provisions, one repealing provision and sixteen final provisions.

It is now up to establishments to check that their activity conforms to the new rules. By way of a list, the main aspects or changes that such establishments, as data controllers or data processors, should take into account in respect of the provisions of the new LOPD are:

1. **Guarantee of digital rights.** If we start at the end as far as the location of the content of the LOPD is concerned, the great change thereof is the content of Title X aimed at information society service providers and Internet service providers as persons responsible for helping to ensure the application of these rights. Title X undertakes the task of recognising and safeguarding a

number of citizens' digital rights in accordance with the mandate provided in the Constitution. In particular, the rights and freedoms associated with the Internet environment, such as network neutrality and universal access or the rights to digital security and education, as well as the rights to be forgotten, to portability and to the digital will, are the subject matter of regulation. The recognition of the right to digital disconnection in the framework of the right to privacy in the use of digital devices in the workplace and the protection of minors on the Internet occupies an important place. Finally, the guarantee of freedom of expression and the right to the clarification of information in digital media is noteworthy.

2. **Processing of children's personal data.** Whereas the GDPR establishes a minimum age of sixteen (16) years for the processing of children's data based on the child's own consent, the LOPD, pursuant to the enablement provided in the GDPR itself - according to which Member States may provide by law for a lower age provided that such lower age is not below thirteen (13) years - sets the age of the child at fourteen (14) years for the processing of data based on the child's consent.

3. **Processing of personal data relating to criminal convictions, offences, proceedings and related provisional and protective measures.** The processing of such data for purposes other than the prevention, investigation, detection or prosecution of criminal offences or enforcements may only be carried out when covered by a rule with statutory force and effect or by EU law. In other cases, processing of such data may only be carried out by lawyers and procurators, provided that the purpose of the same is to collect the information provided by clients for performance of their functions.

4. **Processing of individual employers and freelancers' contact data.** The processing of contact data and, where appropriate, data relating to the function or position of natural persons providing services within a legal person, shall be understood as forming part of the legitimate interest pursued by the controller or a third party when two requirements are met:

   (a) The processing relates only to data necessary for professional location.
   (b) The purpose of the processing is exclusively to maintain relations of any kind with the legal person in which the data subject provides his or her services.

   The same shall be presumed in the processing of data relating to individual entrepreneurs and freelancers when the data refer to such capacity and are not processed to maintain a relationship with them as natural persons.

5. **Data processing related to the carrying out of certain commercial transactions. I**n the absence of proof to the contrary, the processing of personal data, including prior communication thereof, arising from a company's structural changes or a contribution or transfer of undertaking, business or part of undertaking or business, shall be lawful, provided such processing is necessary for the successful outcome of the transaction and guarantees, where appropriate, continuance in the provision of services. If the transaction in question is not concluded, the transferee must immediately delete the data, the obligation to block not applying.

6. **Data processing for video surveillance purposes.** Natural or legal persons, public or private, may process images through a video surveillance system in order to preserve security. Images in a public thoroughfare may only be captured to the extent they are necessary for the aforementioned purpose and where needed to protect strategic property or facilities or transport-related infrastructure. It is forbidden to capture images of the interior of a private home and it is clarified that the processing by a natural person of images of his or her own home is excluded from the scope of application of the LOPD. The maximum period of data retention continues to be 30 days, except where said retention is required as evidence of acts against the integrity of persons, property or facilities. If such be the case, the images will be made available to the competent authority within 72 hours of the existence of the recording becoming known. The data controller must comply with the duty to inform by placing in a visible place a device informing on the existence of processing, the identity of the data controller and the possibility of exercising the rights provided in the GDPR or including a code or link to such information. Finally, the LOPD includes several requirements in relation to the use of video surveillance and sound recording devices in the workplace:

   - Employers may process images obtained through video surveillance systems for the performance of labour control functions, provided that these functions are performed within their legal framework and with the inherent limits thereof.
   - Workers need to be informed in advance, in an express, clear and concise manner, about this measure.
   - Video surveillance and sound recording systems are not permitted in places intended for rest or recreation such as changing rooms, toilets, dining rooms and the like.
   - The use of sound recording systems in the workplace will be admitted only when the risks to the safety of facilities, property and people are significant and always observing the principle of proportionality, the principle of minimum intervention and the guarantees provided in the LOPD.

7. **Advertising-exclusion systems.** The LOPD specifies that data processing in order to prevent the sending of commercial communications to those who have refused to receive them will be lawful, being able to create information systems with just the essential data to identify those concerned. These systems may also include services related to preferences. The establishments responsible for the advertising-exclusion systems must inform the control authority of their creation, their general or sectoral nature and the way in which those concerned can assert their preferences. It imposes an obligation on the person responsible to inform of existing exclusionary systems to those concerned who express their refusal to receive commercial communications. Those who send direct marketing communications must previously consult the advertising-exclusion systems, excluding from such processing the data of those concerned who have expressed their objection. Such consultation is not necessary where the person concerned has given consent to receiving communications to whomever intends to send communications.

8. **Information systems for internal complaints in the private sector.** The main development in relation to the previous regulation is that the LOPD allows complaints to be anonymous. Access to the data contained in these systems will be limited exclusively to those who perform the functions of internal control and compliance. Access to or communication of the same is considered lawful when required to adopt disciplinary measures or to process legal proceedings. Only when disciplinary measures could be taken against a worker, will such access be allowed to personnel with human resources management and control functions. The data controllers must adopt the necessary measures to preserve the identity and guarantee the confidentiality of the data concerning the persons affected by the information supplied, especially those of the person who brought the facts to the attention of the entity, if he or she has not done so anonymously. Details of the person making the communication and of employees and third parties should be kept in the complaints system only for the time necessary to decide whether or not to initiate an investigation into the facts complained of. In any case, three months after the entry of the data, such data should be deleted from the complaints system, unless the purpose is to have evidence of the functioning of the legal person's criminal compliance programme. If retaining the data is necessary to continue the investigation, such may continue to be processed in a different environment by the body of the establishment with which the investigation lies. When the data are no longer necessary, they must be destroyed or deleted, the obligation to block not applying to these systems.

9. **Use of digital devices in the workplace. The LOPD guarantees the right of workers and public employees to the protection of their privacy in the use of digital devices made available by their employer.** The employer must establish criteria for the use of digital devices and may only access the content derived from their use by workers in order to monitor compliance with employment or articles of association-related obligations and ensure the integrity of such devices. Furthermore, access by the employer to the content of digital devices used for private purposes will require the precise specification of authorised uses and guarantees to preserve the privacy of workers. In relation to the use of digital devices, the incorporation into the LOPD of the right to digital disconnection for public employees and workers in order to guarantee respect for their breaks, leaves and holidays, as well as their personal and family privacy. The employer must define the methods of exercising the right to disconnection in an internal policy aimed at workers, which will also establish personnel training and awareness actions for a reasonable use of technological tools in order to avoid the risk of computer fatigue. The methods of exercising this right shall take into account the nature and object of the employment relationship, subject to what is established in collective bargaining or, failing that, to what is agreed between the company and the worker representatives.

10. **New legal framework.** The new LOPD repeals the Personal Data Protection Act 15/1999 of 13 December and any provisions of equal or lesser force and effect that contradict, oppose or are incompatible with the provisions of Regulation (EU) 2016/679 and the new statute. Without prejudice to the foregoing, processing subject to 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 of the

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, shall continue to be governed by the Personal Data Protection Act 15/1999 of 13 December, particularly Article 22 and its implementing provisions, until such time as the piece of legislation incorporating the provisions of the aforementioned directive into Spanish law enters into force. Likewise, the provisions passed in application of Article 13 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which entered into force prior to 25 May 2018, and in particular Articles 23 and 24 of the Personal Data Protection Act 15/1999 of 13 December, remain in force until expressly amended, replaced or repealed.