ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Legal Note – Constitutional Act 3/2018, of 5 December, on Personal Data Protection and Guarantee of Digital Rights.

Madrid, January 10, 2018

By means of this legal note we analyse the most significant points brought in by the newly adopted **Constitutional Act 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights (hereinafter, "LOPDGDD")** which aims to realign the Spanish legal regime with the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, with regard to the processing of personal data and on the free movement of such data (hereinafter, "GDPR").

- **Personal data of deceased persons**

The relatives, civil partners and heirs of the deceased person are granted a right to exercise the rights to access, rectify and erase the personal data of the latter before the controller or the processor, unless forbidden by the deceased person or by law.

- **Accuracy of personal data**

Under the GDPR, personal data must be accurate and, where applicable, updated, though the controller shall not be responsible for the compliance of this principle where the personal data have been collected from the data subject by means of a mediator or intermediary, from another controller through the exercise of the right to data portability or from a public registry.

- **Child's consent**

Only persons over fourteen years-old shall be able to provide a valid consent. As for the persons under fourteen, consent shall be given by the holders of the parental authority and the custody of children.

- **Transparency and information**

The controller is granted the possibility to provide information through layers: a first layer including the identity of the controller (and representative, where applicable), the purpose(s) for processing and the rights of the data subjects.

Where personal data have not been obtained from the data subject, the first layer shall also include information on the categories of the processed personal data and the origin of such data.

- **Processing of contact data, freelances and independent professionals**

On the basis of legitimate interest, the controller shall be able to process contact data of natural persons who work for legal persons or entities where such data are used only for

professional location and for keeping a relationship of any kind with the legal person to whom the data subject renders services. Likewise, the prior assumption applies to freelances where they are contacted in the mentioned conditions, and not as natural persons.

- **Information systems on solvency and credit worthiness**

Processing of personal data concerning breaches of monetary, financial and credit obligations shall be lawful where personal data have been provided by the creditor and the debts to which they refer are truthful, overdue and enforceable and where the creditor has informed the debtor in the agreement or when issuing prior claim for payment of the possibility to inclusion into said systems.

- **Processing for surveillance purposes**

The controller is provided with the possibility to inform through an informative device which consists in a first layer informing on the existence of processing, identity of the controller and rights of the data subjects. This device may also include a connection code or an Internet address leading to such information.

- **Advertising exclusion systems**

Controllers who intend to carry out commercial communications must check the advertising exclusion systems (e.g. the Robinson List) to exclude those data subjects who do not wish to receive commercial communications, unless the data subject has provided the controller with his or her consent to receive commercial communications.

- **Data blocking**

Controllers shall block personal data at the end of processing by keeping such data under technical and organisational measures to avoid longer processing activities and permitting their disclosure only where required by the competent authorities.

- **Penalty regime**

Responsible subjects: controllers, processors, representatives thereof, certifying entities and/or entities accredited for supervising codes of conduct.

Infringements: classification of infringements in very serious (e.g. failure to comply with the duty of information, international transfers without safeguards, failure to comply with the duty to block personal data under LOPDGDD, etc.), serious (e.g. hampering or repeated failure to attend the rights of the data subjects, engagement by a processor of other processors without the authorisation of the controller, etc.) and minor (e.g. uncomplete security breach notifications to the Spanish Data Protection Agency, not to publish the contact details of the DPO, etc.)

- **Limitation periods of infringements**

Very serious: 3 years; **serious:** 2 years; **minor:** 1 year.

- **Limitation periods of sanctions**

    - **Sanctions equal or under 40,000 euros:** 1 year.
    - **Sanctions between 40,001 and 300,000 euros:** 2 years.
    - **Sanctions over 300,001 euros:** 3 years.

This limitation periods commence the day after the one the resolution becomes enforceable.

- **Digital rights**

Right to Internet neutrality: Right to obtain from the internet services providers a transparent service offer without discrimination for technical or economic reasons.

Right to universal access to the Internet: Right to access a universal, affordable, solid and non-discriminatory Internet service for the entire community.

Right to digital security: Right of users to the security of their communications through the Internet.

Right to digital education: The education system shall guarantee the full integration of the students into the digital society and the learning of a use of the digital means that is safe and respectful towards the constitutional ethos, fundamental rights and freedoms and personal and domestic privacy. In this regard, the Spanish Autonomous Communities shall include in the scholar program a subject relating to digital competence, which shall include, in particular, a study on the risks derived from an inadequate use of the digital means.

Protection of children in the Internet: Parents, guardians and legal representatives shall ensure that children under their responsibility make a balanced and responsible use of digital devices and information society services. Additionally, Public Prosecutor shall intervene in those cases of unlawful intrusion by means of the use or disclosure of images or personal information concerning children in social media or in information society services.

Right to rectification in the Internet: Right to freedom of speech on the Internet is established. Moreover, social media, digital platforms and information society services managers or controllers shall adopt protocols for exercising the right to rectification in the Internet, this is, the right to rectify content on the Internet which violates any person's right of honour, personal and familiar privacy or to communicate or receive truthful information. In this sense, digital communication media attending such requests shall publish in a visible place of their digital

archives a warning indicating that the original news does not reflect the real situation of an individual.

Right to the update of information in digital communication media: Right to request digital communication media, on a justified basis, the inclusion of a warning of an update in a visible spot to indicate that the original news does not reflect the current situation of the individual as a consequence of subsequent circumstances. The prior right shall also apply to police or judicial actions subsequently modified by resolutions of the competent authority which benefit the data subject.

Right to privacy and use of digital devices in the workplace: Right to privacy in relation to digital devices at the employees' disposal.

Furthermore, the LOPDGDD reminds the right of the employer to access the content in the digital devices at the employees' disposal for the purpose of controlling their compliance with the employment relationship and for guaranteeing the integrity of said devices. In this sense, the employer must implement a policy for the use of digital devices which observes the minimum privacy standards, where employees' representatives must be involved in the drafting.

The right to digital disconnection in the workplace: Right to be have non-labour time respected, including leaves and holidays, as well personal and familiar privacy.

In this regard, the employer must draw up an internal policy setting out the ways of exercising this right, as well as training actions aimed at making staff aware of the use of technological tools. This policy shall be drafted jointly with employees' representatives.

Right to privacy related to the use of video-surveillance and sound recording devices in the workplace: In relation to this right, the following must be taken into account:

- the employer may use a video-surveillance system to monitor employees in accordance with Article 20(4) of the Workers' Statute. For this purpose, the employer must inform employees in advance and, where appropriate, to the employees' representatives. The duty to inform shall be fulfilled through the use of the distinctive sign approved by the Spanish Data Protection Agency in cases of commission of an unlawful act by the employees.
- video-surveillance systems or sound recording systems may not be used in the employees' recess or recreation areas (changing rooms, toilets, dining rooms, etc.).
- Sound recording systems may only be used when they are relevant for the security of installations, goods and persons, taking into account, in any case, the principle of proportionality, of minimum intervention and the guarantees provided by the foregoing rights.

Right to privacy when using geolocation systems in the workplace: In this regard, employers may use geolocation systems for labour control when employees have been clearly and expressly informed beforehand, as well as of the possible exercise of the rights of access, rectification, limitation of processing and erasure.

Digital rights in collective bargaining: Collective agreements may provide additional safeguards with regard to the processing of employees' personal data and digital rights in the workplace.

Protection of children's data on the Internet: Educational centres, as well as any other natural or legal persons carrying out activities involving the participation of children, shall ensure the protection of the children's or minor's best interests, in particular with regards to their personal data.

The right to be forgotten in Internet searches: Right to obtain from Internet search engines the removal of inappropriate, inaccurate, irrelevant, out-dated or excessive personal data from the lists of results.

Right to be forgotten in social media and similar services: It refers to the right of any person to request the erasure of the personal data he or she has provided to or published on social network services or in any other information society service.

Right to portability in social media and similar services: Right to data portability to which the GDPR refers, specifically applied to social media.

Right to a digital testament: This right to access to digital content concerning deceased persons shall be governed as follows:

- Persons related to the deceased person (relatives and civil partners) may access to digital content concerning him or her and provide instructions regarding such data (use, destination or deletion). This possibility will be vetoed if the deceased has expressly indicated otherwise.
- Where a testament exists, the executor or any other person appointed by the deceased person may conduct the aforesaid actions.
- Where the deceased person is an underage or a person with disability, these powers may be exercised by his or her legal representatives or by Public Prosecutor.

We remain at your disposal for any doubt or question that may arise.

Yours sincerely,

Privacy and Data Protection Area of ECIJA
info@ecija.com
+34 917 81 61 60