DIGITAL PACT FOR THE PROTECTION OF PEOPLE

Spanish Data Protection Agency,

INTRODUCTION

In 2019, the Spanish Data Protection Agency (AEPD) published the document Social Responsibility Framework, with an action plan of 103 initiatives in areas like children's education, gender equality, innovation and enterprise, the environment, good governance and transparency, and workers. These initiatives are fully aligned with the Sustainable Development Goals (SDGs) of the 2030 Agenda, especially SDGs 5, 12, 16 and 17.

Our commitment to Society is rooted in our role as public body with the mission of upholding a fundamental right. Starting from this premise, we assume a responsibility with citizens and regulated bodies that is defined in our Social Responsibility Framework under two key concepts:

- Combating violence on the Internet, especially against women.
- Fostering innovation in the field of privacy and data protection so that it is not an obstacle to the development of the digital economy.

The measures to combat digital violence include the creation of a Priority Channel to request the urgent removal of sexual or violent content from the Internet. With this initiative, pioneering at global level, the Agency aims to provide citizens with a rapid and efficient institutional response to the issue of digital violence, which is becoming increasingly common and damaging to the private lives of women who survive this such experiences, especially young women, but also in other particularly serious situations such as racism and homophobia.

Similar measures have also been promoted in the business environment, where other possible responsibilities can be deduced, such as those arising from the omission of prevention or protective measures or the failure to adequately assess the workplace risks to staff who provide services for the company.

These actions are a clear example of the preventive focus and proactive responsibility established in the General Data Protection Regulation. The GDPR opts for a dual strategy of prevention and flexibility that requires a change of mentality in the form of compliance.

The initiative of this Agency must be framed in this context, geared towards promoting a grand pact for coexistence among citizens in the digital sphere under the title DIGITAL PACT FOR THE PROTECTION OF PEOPLE, placing the emphasis on privacy as an asset for public and private organizations.

With this initiative, we want to strengthen rights in the digital sphere, and raise awareness of the fact a right might be accompanied with a corresponding obligation. To do so, it is necessary for all stakeholders involved in the digital sphere, citizens, and organizations to be aware of the consequences that might arise in the lives of those affected by the dissemination of particularly sensitive materials and the liabilities that

may be incurred by the persons distributing them (civil, criminal, administrative and, where applicable, educational and employment).

In terms of the specific scope of the initiative, it is worth pointing out that signing up to the pact means assuming a series of commitments that are detailed across the three main documents.

Through the Charter Letter, the signatory entity commits, firstly, to implement within their respective organizations the principles and recommendations covered in the other two documents that make up the Pact and, secondly, assumes additional commitments to introduce a Priority Channel for their staff and users to request the urgent removal of sexual and violent material from the Internet, along with the other resources and tools that the AEPD has made available to public and private sectors and citizens to help raise awareness of the value of privacy and the importance of processing personal data, also in the workplace. Tools and resources with which we want to extend our policy of zero tolerance in cases of digital violence to all the signatory organizations.

In general, it is sought that signatories to this initiative assume a firm commitment in their sustainability policies and respective business models, not just because it is a fundamental right of the people who must be adequately protected but also, at the same time, it is increasingly considered an asset of the public and private organizations and a distinctive element of competitiveness.

The second document -the Commitment to Responsibility in the Digital Sphere- contains the specific obligations of the organization in the digital sphere, promoting its dissemination within their organization and with third parties.

It is important to note that it is not intended for the signatory organizations to assume obligations beyond those legally binding but to state a specific commitment in the digital sphere which must be subject to special diligence on the part of the signatory organizations.

As a correlation with these obligations, the document lists the liabilities that may be incurred by signatories in the event they fail to comply with them, especially behaviour relating to so-called “digital violence”: from administrative breaches for infraction of the data protection regulation or employment and health and safety regulations, civil and criminal liabilities, and even disciplinary liabilities in the educational sector in the case of behaviour such as harassment to students.

Finally, the document incorporates a number of principles that, from an ethical and data protection perspective, must be considered when it comes to designing and implementing new technological developments. Among the more significant ethical principles relating to privacy are those relating to fostering the greatest possible transparency for users, knowing what data are being collected, when to register them and what they are used for; promoting gender equality, the protection of children and women who are survivors of gender-based violence and persons in situations of vulnerability, or guaranteeing that technologies do not perpetuate bias or increase

existing inequality, avoiding algorithmic discrimination on grounds of race, origin, beliefs, religion or gender, among others.

The third document that comprises this initiative of the AEPD is the Ten Golden Rules of Good Privacy Practice for Media Outlets and Organizations with In-house Media Channels, with which the Agency wishes to promote the fight against digital violence both among the media and all organizations with in-house media channels providing content of interest to their audience, whether through social media, corporate magazines, and bulletins.

To tackle a challenge of this nature with guarantees it is essential to forge alliances with the principal associations, foundations and business and retail organizations among whom, from the outset, we have encountered great enthusiasm to sign up this initiative and to participate actively in its definition and content. Equally, the Agency has been fully receptive to incorporating suggestions and comments it receives, and we believe that the documents faithfully reflect the objectives we set when we agreed to implement this strategic initiative to position the Agency and its stakeholders on the front line of the fight against digital violence.

Consequently, it would be remiss of us not to thank the signatory organizations of this initiative for their support and trust in our institution.

Mar España Martí

DOCUMENTS OF THE PACT

I. CHARTER LETTER: DIGITAL PACT FOR THE PROTECTION OF PEOPLE

The signatory entity publicly declares its commitment to people through the fundamental right to the protection of their data and privacy, both as customers and/or the users and their staff, and with responsible and ethical use of technologies and shall therefore promote, within its sphere of activity, the initiatives to achieve that objective.

Consequently, through this CHARTER LETTER, the signatory entity signs up to:

- The "Commitment to Responsibility in the Digital Sphere" containing the specific obligations of organizations in the digital sphere and the liabilities it may incur in the event of failure to comply with those commitments, fostering dissemination within the organization and with third parties to promote adequate coexistence conditions on the basis of respect for privacy in the digital environment.

- The "Ten Golden Rules of Good Privacy Practice for Media Outlets and Organizations with In-house Media Channels"

Furthermore, it also assumes the following COMMITMENTS for the protection of personal data and privacy, innovation, and sustainability:

- To disseminate, based on the media available, the information on the Priority Channel that has been launched by the Spanish Data Protection Agency to help citizens in urgent and serious cases to prevent digital violence that mostly affects girls and women.

- To promote a working environment free of harassment, especially in the digital sphere, tackling head-on the use and dissemination of personal data for illegal purposes that may violate the right privacy of its staff. The principles of equality, dignity, non-discrimination, and the right to physical and moral integrity are universal legal principles, enshrined in the Spanish Constitution, which assigns the public authorities the responsibility of promoting the conditions necessary for equality and non-discrimination to be effective. To do so, it shall promote the Recommendations of the AEPD for the prevention of digital sexual harassment in the workplace .

- To promote innovation and digital transformation from an approach based on ethics, responsibility, and transparency in relation to those products and services that conduct large-scale data processing, both in terms of the number of persons and the extension of the data on each person, particularly those that encompass Artificial Intelligence (AI).

- To establish working-from-home guidelines that respect privacy, especially for their own employees, that guarantee minimal intrusion in the personal sphere.

- To disseminate, within their area and based on the resources available, the materials from the list attached to this Charter Letter, that the AEPD has made available to both the public and private sector and citizens to help raise awareness of the value of privacy and the importance of personal data and respect for privacy.

- To drive information campaigns, based on the resources available, focussed on training and raising awareness in relation to privacy and personal data protection, in order to reduce inequality in the digital sphere ("digital gap"), especially in more vulnerable sectors of the population.

- To promote digital awareness campaigns for minors to ensure they use digital devices and information society services in a balanced and responsible way in order to guarantee their personal development. To prevent risks of abusive use of technologies, the resources and materials in the attached list are provided.

- To incorporate data protection into the design of sustainability and social responsibility policies, including actions geared specifically towards guaranteeing compliance with this fundamental right as an asset of public and private organizations and as a distinguishing element of competitiveness. In this regard, it is considered good practice to include in the Principles of Responsible Business or Ethical Code of the company, the categorical opposition to any practice that suggests behaviour or practices constituting workplace or sexual harassment or discrimination in the digital environment (digital harassment and cyber-harassment).

The Spanish Association of Foundations (AEF), the foundations and other tertiary sector entities, in fulfilling their social mission in accordance with the resources available to them, assess and look favourably on the initiatives of the AEPD in the area of services, defence and protection of society, especially less advantaged sectors of society. The AEPD is particularly mindful, in the application of this initiative, that it requires the adaptation of those commitments to the needs and characteristics of these entities.

This commitment is valid for one year, automatically renewed, unless the signatory entity withdraws.

II. COMMITMENT TO RESPONSIBILITY IN THE DIGITAL SPHERE.

The protection of people in relation to the processing of personal data is a fundamental right.

The Spanish Constitution guarantees the right to honour, personal and family privacy and one's own image. It recognises the right to self-determination of data and digital freedom as a fundamental right, which is the right to protect one's personal data, complementary

to the above but not restricted solely to one's intimate data, but encompassing all those data that identify or allow for the identification of the person, may serve for the construction of an ideological, racial, sexual or other type of profile or which serve any other purpose that, in certain circumstances, might constitute a threat to the individual (STC 292/2000).

The principles of equality, dignity, non-discrimination, and the right to physical and moral integrity are universal legal principles, enshrined in the Spanish Constitution, which assigns the public authorities the responsibility of promoting the conditions necessary for equality and non-discrimination to be effective.

Article 8, section 1 of the Charter of the Fundamental Rights of the European Union, and Article 16 section 1 of the Treaty on the Functioning of the European Union establish that everyone has the right to the protection of their personal data.

The General Data Protection Regulation (EU) 2016/679 (GDPR) - and Organic Law 3/2018, of 5 December, on personal data protection, and guaranteeing digital rights (LOPDGDD) jointly configure the development of the fundamental right to the protection of personal data.

The most significant new element of the European Regulation is the development of a model based on control; from primarily formal methods, such as compliance with the data protection regulation, to the principle of active responsibility, requiring a preliminary assessment on the part of the data controller or data processor, of the risk that might arise from the processing of personal data. Based on this assessment, they shall adopt the necessary measures. As a general rule, the data controller must therefore apply appropriate and efficient measures and demonstrate the compliance of processing activities with the applicable regulations (GDPR and LOPDGDD), including the efficiency of the measures adopted, which shall be reviewed and updated where necessary. These measures must consider the nature, scope, context and purposes of processing, and the risk to the rights and freedoms of natural persons (Articles 24.1 GDPR and 28 LOPDGDD).

The data controller must, therefore, adopt a proactive attitude, incorporating the value of privacy in their ordinary activity, guaranteeing compliance with this right as an asset of the organization and a distinctive element of competitiveness in the market.

Accordingly, for the full development of the fundamental right to personal data protection and privacy, the signatory organizations assume the commitment to diligently comply with the following obligations:

SPECIFIC OBLIGATIONS IN THE DIGITAL SPHERE

To inform users of the processing of the data and the exercise of their rights.

The organizations inform users, clearly and simply, on the most important aspects of data processing identifying who processes them, the legal basis, the purpose and how they can exercise their rights. The exercise of these rights cannot be denied in the event that

the citizen wishes to exercise them through a procedure or different channel that that offered (Articles 13 and 14 GDPR and 11 LOPDGDD).

In particular, they shall inform the users of the measures and tools to guarantee privacy in a prominent manner.

Apply the principles relating to processing.

The organizations must apply, in the processing of the data of their customers, staff, suppliers and citizens, the principles of lawfulness, fairness, transparency, purpose limitation, minimization, accuracy, storage limitation, integrity, confidentiality and proactive responsibility with the given scope of Article 5 of the GDPR.

Guarantee the lawful processing.

The organizations shall be obliged to guarantee the lawful processing of customers', employees' and citizens' data based on the grounds considered in Article 6 and also, in the case of special categories of personal data (health data, data regarding political or trade union affiliation, data relating to sex life, etc.) in Article 9, both of the GDPR.

Appoint a Data Protection Officer (DPO)

Private organizations must, in the cases legally required, and public sector entities in all cases, appoint a Data Protection Officer who shall have the appropriate level of qualifications, ensuring they have the resources necessary for the exercise of their duties in an independent manner, duly informing the Spanish Data Protection Agency of the appointment (Articles 37 to 39 GDPR, and 34 to 36 LOPDGDD). In particular, in appointing the DPO, special attention shall be paid to those with accredited qualifications and the professional capacity required for their work.

The appointment of Data Protection Officers shall be encouraged in cases where it is not legally compulsory, provided that the circumstances or process make it advisable or where the organization has the resources to do so.

The organization shall offer the DPO all the necessary support so that they have the best resources to respond to all complaints from citizens where they opt for this route before lodging a complaint with the AEPD, or in cases where the AEPD decide to transfer it to the data controller prior to admission to procedure (Article 65.4 LOPDGDD).

To apply privacy "from design" and "by default".

Organizations must, therefore, when it comes to determining the means of processing and in the act of processing itself, that they have, "from design", implemented appropriate technical and organizational measures, and integrate the necessary guarantees into the processing, for the purpose of efficiently complying with legal obligations and protecting data subject rights (Article 25.1 GDPR).

Furthermore, they shall promote the application of the appropriate technical and organizational measures that, by default, are only subject to the processing of the personal data necessary for each of the specific purposes of processing. This obligation

shall apply to the amount of personal data collected, the extent of their processing, the period of storage and their accessibility (Article 25.2 GDPR).

Failure to comply with these specific obligations could lead to the following:

RESPONSIBILITIES IN THE DIGITAL SPHERE

Administrative responsibility for infraction of the data protection regulation.

The acts constituting an infraction of data protection regulation and which would, therefore, be susceptible to sanction, include:

- Failure to provide the information to allow users to ascertain who is processing their personal data and why.
- Obtaining the personal data of a person in an illegal, misleading, or fraudulent way, in particular through identity theft.
- Using a person's personal data or communicating them to third parties with no legal basis, in particular in the case of sensitive data such as ideology, religion, belief, ethnic origin, health, sex life and sexual orientation.
- Using a person's personal data for purposes other than those compatible with those for which they were collected.

Survivors of gender-based violence enjoy special protection that covers the use, access, and dissemination of their personal data, to ensure they are not exposed to new risks of a similar nature. In particular, the dissemination of especially sensitive personal data (in contents such as images, audio, or video of a sexual or violent nature that allow them to be identified) published through different Internet services without content shall be considered illegal processing of personal data subject to sanction by the Spanish Data Protection Agency, with fines in the most serious cases reaching 20 million euros or 4% of the company's global turnover (Article 83.5 GDPR).

Civil liability.

The persons responsible may have to deal with compensation to their victims for material and psychological damages arising from illegal conduct in the area of personal data protection.

Criminal liability.

The evolution of information technologies and the communication and extension of their use through Internet services and applications, such as social media, instant messaging, and email on smart devices, has seen them used as a common method not only for offences in under data protection, but also those typified as criminal offences.

The Criminal Code typifies certain conducts in the digital sphere as crimes such as those that constitute an attack on moral integrity, discovery and disclosure of secrets, threats,

coercion, harassment, slander and libel, gender-based violence, identity theft and computer damage, among others.

Disciplinary liability for infraction in the workplace.

- ✓ *For the company.*
  - *Infractions in relation to employment relations.*
  - *Infractions in relation to workplace health and safety.*
  - *Infractions in relation to equality.*
- ✓ *For employees.*

Workers may be sanctioned for employment breach, in accordance with the extent of the offences and sanctions established in the legal provisions which, in the case of very serious offences, can be up to and including disciplinary termination of employment (2/2015 Employees' Statute).

COMMITMENT TO INNOVATION, DATA PROTECTION AND ETHICS

Privacy must be understood as a value, not as a commodity to be monetized. Digital responsibility is closely linked to respect for human rights. Thus, respect for the privacy, intimacy and confidentiality of personal data, the promotion of free and informed decision-making, equality, transparency, and accountability are all essential conditions to prevent discriminatory practices, unwanted and concealed use as well as possible asymmetries and vulnerabilities, and, especially, opacity in decision-making.

The convergence of technologies such as AI, Big Data, the Internet of Things, biometrics, block chain, 5G and genetic data should be applied in a responsible manner, first analysing the risks and ultimate impacts they may have on data subjects (as individuals, groups, and society as a whole). It is necessary, therefore, to take ethical decisions and anticipate scenarios that might generate risks to privacy, especially re-identification, and potentially increased risks as these emerging technologies converge.

To do so, it is considered good practice to provide training in ethics and privacy of the different stakeholders involved, especially those who program the algorithms and decision-makers, and digital literacy in general.

In particular, new technological developments must take the following principles into account:

- Foster maximum transparency so that users know what data is being collected, when it is registered and why it is used. To reach a significant level of transparency, people must have access to their personal data in a simple and easy-to-use manner.
- Promote gender equality, the protection of children, survivors of gender-based violence and those in situations of vulnerability.

- Guarantee that technologies avoid the perpetuation of bias or increasing existing inequality, avoiding algorithmic discrimination on the basis of race, origin, belief religion, sex, or any other reason.
- Minimum intrusion on the life and privacy of persons, ensuring processing that is proportional and necessary and the preserves individual freedoms.
- Implement mechanisms of verification, validation and accreditation that guarantee processing in good faith and accountability.

In particular, the ethical perspectives relating to Artificial Intelligence (AI) are one of the areas of greatest concern. The ethics of AI seek to uphold values like dignity, freedom, democracy, equality, individual autonomy, and justice in the face of the governance of mechanical reasoning. Reliable, human-centred Artificial Intelligence must fulfil seven key requirements: human action and supervision; technical solidity and security; management of privacy and data; transparency; diversity, non-discrimination, and equality; social and environmental well-being and accountability. These requirements must be assessed over the course of the life cycle of an AI system on a continuous basis and considering the potential collateral impact of processing in the social environment, beyond the limitations initially considered in relation to purpose, duration over time and extension. In particular, one critical aspect of AI systems is the possible existence of bias and accepting, with no critical spirit, the result of AI as correct and unwavering, assuming a “principle of authority” arising from the expectations created for said systems.

Ultimately, approaching innovation and decision-making from the perspective of respect and privacy and under the principles of ethics and digital responsibility, constituting a commitment which we must guarantee for future generations.

III. TEN GOLDEN RULES OF GOOD PRIVACY PRACTICE FOR MEDIA OUTLETS AND ORGANIZATIONS WITH IN-HOUSE MEDIA CHANNELS

Article 17 of the Istanbul Convention states that Parties shall encourage the private sector, the information and communication technology sector and the media, with due respect for freedom of expression and their independence, to participate in the elaboration and implementation of policies and to set guidelines and self-regulatory standards to prevent violence against women and to enhance respect for their dignity. Furthermore, it specifies that the skills of minors and their family and educational environments should be developed to tackle the issue degrading content of a sexual or violent nature.

The principles of equality, dignity, non-discrimination, and the right to physical and moral integrity are universal legal principles, enshrined in the Spanish Constitution, which assigns the public authorities the responsibility for promoting the conditions necessary for equality and non-discrimination to be effective. In particular, in the specific sphere of non-discrimination on the grounds of gender, Organic Law 3/2007, of 22 March, on Effective Equality of Women and Men, Article 48, section 1 states that "Companies must promote working conditions free of sexual and gender-based harassment and oversee specific prevention procedures and to provide a channel a channel for reports or complaints from those who have suffered harassment."

New technologies and the services they offer provide innumerable advantages. Nevertheless, they are sometimes used as a channel to extend and amplify the violence that takes place in the off-line world, attempting publicly humiliate women who have survived gender-based violence and violate their privacy. In this context, there are different forms of cyber-violence and digital violence mostly aimed at women, minors, persons discriminated against on grounds of sexual orientation or race, persons with disabilities or serious illness or those at risk of social exclusion. It is increasingly common for sexual or violent content featuring women who have survived gender-based violence or these other groups to be published on the Internet or disseminated through social media.

These Ten Golden Rules form part of the "Charter Letter: For a Digital Pact for the Protection of People" drafted by the Spanish Data Protection Agency. Through this Charter Letter, the Agency wishes to intensify relations with the media and with those organizations with their own media channels to inform on issues of interest to their audience. **The final objective is to promote the privacy of women who have survived gender-based violence and, in general, raise awareness of the existence of the priority channel** to request the removal of text, audio, photographic or video content of sexual or violent nature shared without the consent of the persons appearing therein.

1. The signatories of the Charter Letter shall refrain from identifying women who have survived violence or gender-based assault, acts of violent or sexual nature in their news content, and shall refrain from publishing information that, in general, might infer the identity of a survivor, especially in the case of persons with a public profile.

All of the above is without prejudice to the fact that non-public persons may be involved in newsworthy events, in which case news coverage shall be appropriate in complying with the right to information, in accordance with the specific nature of each case.

2. The information disseminated in the media shall not include images unnecessary from a purely informative point of view, qualitative or quantitative, thus avoiding the systematic repetition of images.

3. The Spanish Data Protection Agency is bound by a confidentiality clause and shall not provide information on any women who are survivors of gender-based violence or people who, while not survivors, have reported the dissemination of these sensitive content through the priority channel. It shall not contact women who are survivors of gender-based violence or those who have reported issues to inform them of the possible interest of the media in interviewing them.

4. The AEPD shall respect the data protection of those who have made reports, where they are natural persons, except where they have been made public. Once the procedure is completed, the reports published shall highlight the sanction imposed on the person recording or sharing the images, as a pedagogical tool.

5. Where the signatories of the Charter Letter offer information on the digital dissemination of violent contents, they shall attempt to provide a warning, within the possibilities of each media, on the disciplinary, civil, criminal, and administrative responsibility that may arise from such conduct.

6. The signatories shall not apologise for, or justify, in any way, the aggressor who has disseminated sensitive content of third parties without consent. Ignorance of the law is not a mitigating factor. The voluntary recording of images of a sexual nature shall not cover the subsequent dissemination of these if it is performed without the consent of the persons appearing in the images.

7. In the news stories covering the dissemination of violent or sexual content on the Internet featuring women who are survivors of gender-based violence, a systematic referral to the Spanish Data Protection Agency's Priority Channel insofar as the media allows.

8. Content published on the Internet covering digital violence shall also incorporate a referral to the Priority Channel for requesting the removal of content even if the person making does not appear in the images, audio, or text.

9. In the event that a media outlet becomes aware of the identity of a potential victim of digital violence, they shall refrain from publishing or disseminating images or contents they have obtained directly from social media sites of which the victim is a user, and from making any assessment of those images. Images from social media that have previously been disseminated through other media shall be used in compliance with the rules and principles established above.

10. The measures mentioned in the above shall apply even where the social media profiles of the victim are public.