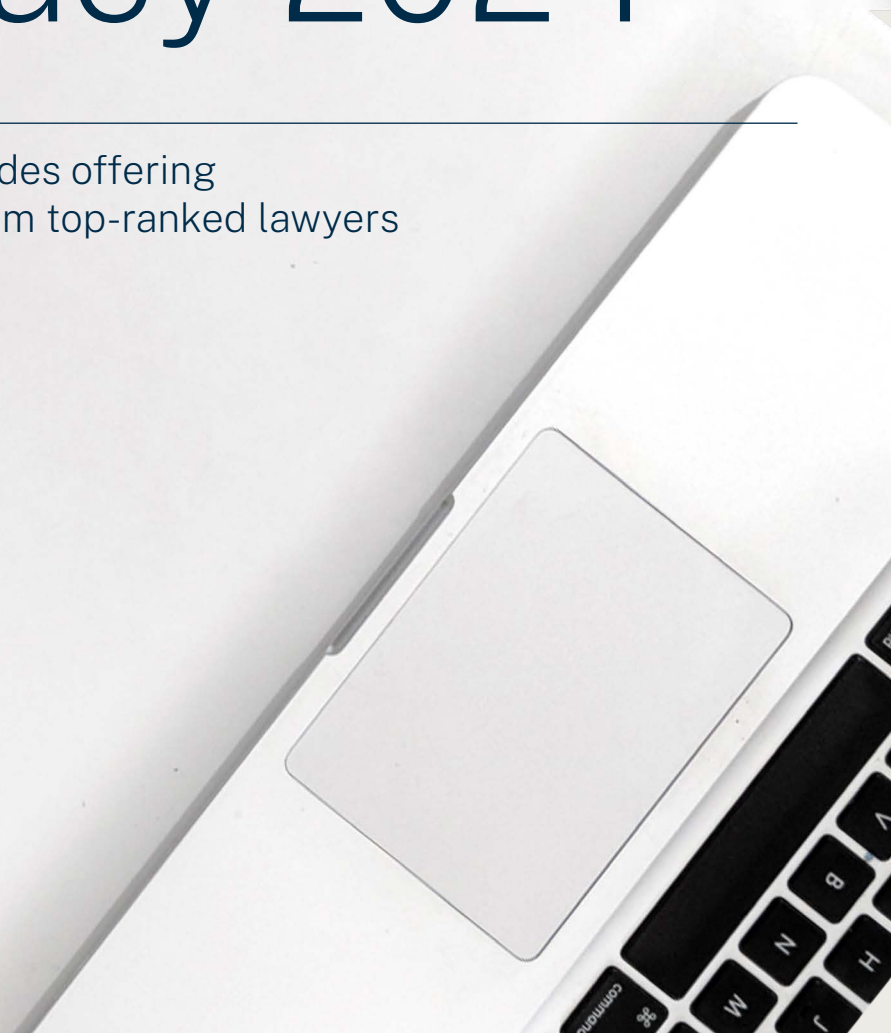
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

# Data Protection & Privacy 2024

Definitive global law guides offering
comparative analysis from top-ranked lawyers

**Contributing Editor**
Alan Charles Raul
Sidley Austin LLP



Chambers

Global Practice Guides

# Data Protection & Privacy

Contributing Editor

Alan Charles Raul

**Sidley Austin LLP**

2024

# Chambers Global Practice Guides

For more than 20 years, Chambers Global Guides have ranked lawyers and law firms across the world. Chambers now offer clients a new series of Global Practice Guides, which contain practical guidance on doing legal business in key jurisdictions. We use our knowledge of the world's best lawyers to select leading law firms in each jurisdiction to write the 'Law & Practice' sections. In addition, the 'Trends & Developments' sections analyse trends and developments in local legal markets.



**GPG Director** Katie Burrington
**Content Management Director** Claire Oxborrow
**Content Manager** Jonathan Mendelowitz
**Senior Content Reviewer** Sally McGonigal, Ethne Withers
**Content Reviewers** Vivienne Button, Lawrence Garrett, Sean Marshall, Marianne Page, Heather Palomino, Deborah Sinclair, Stephen Dinkeldein and Adrian Ciechacki
**Content Coordination Manager** Nancy Laidler
**Senior Content Coordinator** Carla Cagnina
**Content Coordinator** Hannah McDowell
**Head of Production** Jasper John
**Production Coordinators** Genevieve Sibayan, Pete Polanyk and Paul Cummings

Published by
**Chambers and Partners**
165 Fleet Street
London
EC4A 2AE
**Tel** +44 20 7606 8844
**Fax** +44 20 7831 5662
**Web** www.chambers.com

# CONTENTS

# CONTENTS

# CONTENTS

# SPAIN


## Trends and Developments

**Contributed by:**
Miguel Geijo Castany and Alicia Coloma Duato
**Broseta Abogados**

**Broseta Abogados** was founded in 1975 and provides a full range of services and multidisciplinary advice. With over 300 professionals, it offers its clients deep technical expertise and a consolidated geographical presence in Spain, Portugal and Switzerland. The firm is agile and flexible, with a structure that allows it to adapt to the most complex environments with proactivity, and to react to any contingency with the efficiency that the market and the client demand. Broseta Abogados puts its team of partners at the head of all its projects. These are professionals with an average of 30 years of experience, who are accessible, proactive and involved in every decision relevant to the client. The firm promotes transformation as the basis for growth and rejects static and standardised solutions. Each client is a challenge and their needs define the firm's service proposal. It aims to grow the value of its clients based on a differentiated way of doing things.

## Authors

**Miguel Geijo Castany** is a partner and head of corporate and commercial law at Broseta Abogados. Miguel has extensive experience in information technology law, and is an expert in personal data protection and privacy, as well as biotechnology and pharmaceutical law. He is considered one of the best in the practice of privacy and data protection, and is the author of numerous articles on the subject. He is a Master's degree lecturer at the Complutense University of Madrid and ISDE, and a regular speaker at conferences. He has also been a member of the Spanish Confederation of Business Organizations, Data Protection Committee, among others.

**Alicia Coloma Duato** is a senior associate in the IT, privacy and digital environments department at Broseta Abogados. She has a degree in Law from the University of Valencia (2011) and a Master's degree in Intellectual Property from the Universidad Pontificia Comillas (2012). Her experience focuses mainly on providing specialised advice to national and international companies (technology, pharmaceutical, insurance, retail, etc) on projects with implications in the areas of intellectual property, data protection, e-commerce and information technology. She is a participant in important commercial transactions related to technological assets and drafting and reviewing all types of commercial contracts. She is currently working as a privacy specialist lawyer with 12 years of experience.

**Contributed by:** Miguel Geijo Castany and Alicia Coloma Duato, **Broseta Abogados**

## Broseta Abogados

Goya, 29
28001
Madrid
Spain

Tel: +34 914 323 144
Fax: +34 934 145 300
Email: info@broseta.com
Web: www.broseta.com

### Trends and Position of the AEPD in Sanction Procedures for Personal Data Breaches

The Spanish Data Protection Agency ("AEPD", or the "Agency") has initiated several sanction procedures in the past few months, in relation to the infringement of Articles 5.1.f, 32.1 and 25.1 of Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

Specifically, the AEPD has been implementing sanctions for (i) the infringement of the principle of confidentiality and data integrity; (ii) the absence of security measures according to an appropriate risk evaluation; and (iii) the failure to implement appropriate privacy by design. All the resolutions follow the same trend: the aforementioned articles are considered autonomous as they have a different obligational content, pursue different purposes and, therefore, they are classified differently in the GDPR. Regarding their statutes of limitation, the Spanish Organic Law 3/2018, of 5 December 2018, on the Protection of Personal Data and Guarantee of Digital Rights, also considers them as autonomous obligations.

In summary, the AEPD sets forth:

- Article 5.1.f of the GDPR is infringed when there is a loss of confidentiality or integrity, whether or not there is an absence/deficiency of security measures;
- Article 32.1 of the GDPR establishes the obligation to implement appropriate technical and organisational security measures to ensure a level of security according to an appropriate risk evaluation. This means that it only refers to security and does not make any reference to any other measures, such as organisational ones; and
- Article 25 of the GDPR is infringed when the appropriate technical and organisational measures have not been adopted to effectively apply the principles of privacy by design.

Moreover, the obligations arising from these three articles constitute an obligation of means and not of results, this being a well-established view in case law. However, the application of the resolutions analysed is generating certain controversies.

It should also be noted that the deadline for the notification of a personal data breach to the competent supervisory authority has been

interpreted by the Agency in a very strict manner. The AEPD considers that for the notification of a personal data breach it will be sufficient that there is any likelihood and any risk to the rights and freedoms of natural persons. It is also relevant to point out that, according to the Agency, the notification of the breach must be made at the time when the data controller detects that the breach has occurred, without waiting for a detailed examination of the situation.

Finally, the AEPD has also ruled on sensitive data, considering not only the special categories of personal data provided for in Article 9 of the GDPR, but also that data, the disclosure of which causes immediate harm or distress to the data subject. These include national identification numbers or financial data, which require strengthened technical and organisational measures to ensure the authentication, confidentiality and integrity of personal data.

In view of the above, the purpose of this article is to analyse the approach that has been taken into account to jointly sanction the three aforementioned infringements, with special reference to determining whether the obligations of implementing security measures refers to an obligation of means, the consideration of sensitive data and the deadline for the notification of the personal data breach.

## Notable Trends in Personal Data Breaches

### *Concurrence of infringements*

#### *Non bis in idem*

In the resolutions analysed for this article, the AEPD has developed a trend in which it sanctions companies for infringement of Articles 5.1.f and 32.1 of the GDPR. This could mean that the same act (the insufficiency of security measures) constitutes two infringements of the same protected legal right (the adequate guarantee of the rights and freedoms of the data subjects). In other words, the same facts constitute an infringement of the principle enshrined in Article 5.1.f of the GDPR and, in turn, of the materialisation or concretisation carried out in Article 32 of the same legal text. As indicated by the AEPD, it can even be concluded that we are dealing with two equivalent precepts, one with a general approach, and the other with a more specific content.

In addition, in some resolutions, the AEPD also sanctions the infringement of Article 25.1 of the GDPR. It could be considered that any infringement of data protection legislation by a data controller would necessarily entail a breach of the principle of privacy by design, since such a breach would derive from inadequate compliance with this obligation.

A situation in which the same act (not having security measures) is sanctioned in terms of three different offences could imply an infringement of the non bis in idem principle. This principle "prevents the same subject from being sanctioned twice for the same act based on the same grounds, the latter being understood as the same legal right protected by the sanctioning rules in question" (SAN 23 July 2021 (rec.1/2017)). Although this is a principle specific to criminal law, it also applies to the sanctioning power of the administration in its material and procedural aspects.

When we are faced with this concurrence, there is a different criterion in case law for these situations: (i) the application of the special rule over the general rule or (ii) the application of the most severe sanctioning rule. However, the AEPD disagrees with this perspective, because it considers that these are complementary dispositions,

each of them having to be taken into account independently.

As explained above, the Agency considers that the three Articles in the GDPR each pursue a different purpose. The AEPD states that Article 5.1.f of the GDPR "only determines the manner through which confidentiality and integrity can be maintained". Therefore, compliance is ensured through the application of appropriate technical and organisational measures, which do not have to be security related. In this regard, Article 32 of the GDPR may be infringed regardless of whether the loss of confidentiality does not materialise, since it is the absence itself that is sanctioned, regardless of whether the personal data breach occurs.

In addition, with regard to the possible concurrence of infringements of Articles 25 and 32 of the GDPR, the Agency also clarifies that the measures referred to in Article 25 are not exclusively security measures, reiterating in several of its resolutions that there are multiple technical and organisational measures. However, it does not always provide examples of which kind of measures can be considered as pertaining to such categories.

The AEPD points out in some resolutions that Article 25 of the GDPR intends that the company has integrated within it, in its orderly operation, the protection of personal data. This means that it is a matter of adopting internal policies and implementing measures that comply, in particular, with the principles of privacy by design and by default, within the meaning of Recital 78 of the GDPR.

Having stated the above, economic operators could choose to allege, in the alternative, that the articles are very closely related, making it extremely likely that when one is infringed, the others will be infringed (concurso medial). In other words, even if there is not total duplication, it could be argued that they are all reciprocally consequential.

In our opinion, it could be considered that the infringement of Article 5.1.f of the GDPR would necessarily and inseparably be caused by the alleged lack of careful implementation of the measures required in Article 32 of the GDPR. At the same time, it could be interpreted that the lack of application of these measures would be the consequence of an alleged lack of design of the measures at the time of determining the means and ends for the processing.

However, in the Agency's view, the interpretation in this matter is clear: Article 32 of the GDPR, although related to Article 5.1.f of the GDPR, does not comply with the principle of confidentiality in its entirety, since situations may be encountered in which there are inadequate measures without a loss of confidentiality and integrity. At the same time, there may be situations in which confidentiality is lost without the cause being the absence or deficiency of strict security measures. Consequently, the Agency considers that the lack of security measures does not necessarily result in the loss of confidentiality.

Overall, in the opinion of the AEPD, the safeguarding of the principle of confidentiality and integrity is directly linked to the implementation of security measures appropriate to the risks. This principle, enshrined in Article 5 of the GDPR, also covers measures of an organisational nature, the fulfilment of which is independent and autonomous from the obligation set out in Article 32 of the GDPR.

In light of the foregoing, it should be borne in mind by economic operators that a sanction procedure is likely to result in the concurrence of infractions. Therefore, special attention must be paid to comply with the general principle of confidentiality and integrity, through security, technical and organisational measures, and above all, by establishing an adequate and sufficient design protocol even before the processing of personal data takes place.

### *Obligation of means, not of results*

As the Spanish Supreme Court ruled in its judgment of 15 February 2022, the obligation to adopt technical and organisational measures to guarantee confidentiality is an obligation of means and not of results. This means that the infallibility of the measures adopted is not an enforceable obligation. It is important to note that, according to such criteria, the alleged breach of Article 32 of the GDPR may not be linked to the production of the result that may occur as a result of a series of unforeseeable factors.

However, the AEPD points out that, it is in itself an infringement, if at the time of the incident there were adequate technical measures not implemented. To this end, attention must be paid to the due diligence of data controllers and processors and, above all, to the nature, scope, context and purpose of the processing, as well as the level of risk. It is understood that greater due diligence is required for certain companies, due to the fact that their activity and the development of their business involves a continuous and abundant processing of personal data on a large scale.

With regard to this due diligence, the AEPD highlights the importance of ensuring that the measures adopted are sufficient in response to the risks and must include the same actions not only of a reactive nature, but also of a preventive nature. This means that it is not enough to apply measures to immediately solve a personal data breach, but it is necessary to have prior measures to prevent such a breach from occurring. Consequently, the AEPD refers again to privacy by design, highlighting that confidentiality is guaranteed above all with preventive measures, which seems inconsistent with the arguments relied upon by the agency when imposing the sanctions relating to security measures.

The AEPD's approach for deciding whether the obligation of means established in Article 32 of the GDPR has been complied with is that the economic operator can justify that the security measures are in accordance with the "state of the technology and in relation to the nature of the processing carried out and the personal data in question, reasonably prevent their alteration, loss, processing or unauthorized access" (STS 15 February 2022).

The AEPD has come to consider that the need to adopt reactive measures highlights an inadequacy or insufficiency of the measures, implicitly implying an acknowledgement of the existence of deficiencies in its approach to security. This shows that the Agency considers the duty to design security measures to be an obligation of result. Notwithstanding this, the AEPD has also considered the application of these corrective measures as mitigating factors. Therefore, the Agency's approach could raise some concerns.

In short, Article 32 of the GDPR establishes an obligation of means to prevent a result from occurring, and this obligation consists of having the appropriate technical or organisational measures, while Article 5.1.f of the GDPR enshrines precisely the result that is intended to

be achieved with such means, which is to guarantee the security and integrity of the data.

### Sensitive Data

In some of the resolutions analysed, the AEPD has ruled in relation to sensitive data, indicating it is not limited to Article 9 of the GDPR, since the types of data that deserve special protection are those whose disclosure causes immediate harm or distress to the data subject, such as location data, data about private communications, national identification numbers, or financial data, such as transaction statements or credit card numbers.

It is worth mentioning that Recital 75 of the GDPR mentions that the processing of certain personal data may result in physical, material or non-material damage. This may give rise to "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage".

Likewise, the AEPD mentions that even though financial data is not considered sensitive data under the GDPR, its processing requires special guarantees that ensure the accuracy and security of such data. Particularly, due to the type (transactional data) and amount of data which are processed through electronic payment systems, they need to incorporate data protection measures, for instance, privacy by design and by default.

The AEPD establishes that this mention by the GDPR does not exclude that other financial data, different from electronic payment systems, may require special guarantees. In fact, the AEPD's Guide on Risk Management and Impact Assessment in the processing of personal data differentiates between three types of financial data that must be carefully assessed when determining the level of risk of a given processing: (i) data related to the economic situation, (ii) data related to the financial statement and (iii) means of payment data. The first two are assigned a medium risk and the last a high risk. This means that "high-level security measures" should only be relevant if data related to payment methods is processed.

The AEPD establishes a criterion in which "the documentary support related to the origin of a fund in a bank account contains data related to the economic situation and financial status of customers, which make it possible to determine the financial situation or the patrimonial solvency of a person, so they require a greater protection in view of the risks to the rights and freedoms of the natural persons".

That criterion follows from the fact that Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, infers that even if some of the data considered in isolation does not appear to be capable of revealing important information about the private life of the people concerned, the fact remains that, taken together, that data is capable of revealing, among other things, a complete travel itinerary, travel habits, relationships between two or more people, as well as information on the economic situation of air passengers, their eating habits or their state of health, and could even provide sensitive data about such passengers.

Overall, according to the AEPD, the analysis and adoption of measures must not be carried out solely by virtue of the nature or purpose of the processing or exclusively by virtue of the type of data processed, as if they were exclusion-

ary aspects, but must be carried out taking into account all the aspects that the processing in question may involve.

On the other hand, the AEPD has stressed that an ID number, together with a verification character corresponding to a tax identification number, undoubtedly identifies a natural person. For this reason, it should be borne in mind that, in the opinion of the AEPD, it should be considered as sensitive data – regarding the security measures to be implemented – when its processing is not accompanied by the necessary technical and organisational measures to ensure that the person identified with it is really its owner. This is because, otherwise, a third party could easily act in the place of the person's identity leading to identity fraud, with the risks that this entails for the privacy, honour and assets of the person affected.

In summary, economic operators must take into account that there is data which, when processed together, entails a severe risk if it allows the identity of the person to be identified or impersonated directly. Therefore, when companies process such data, they must ensure reinforced technical and organisational measures, carrying out an analysis to ensure compliance with data protection principles.

### *Notification deadline*

Both Article 33 and Recital 87 of the GDPR establish the requirements regarding whether a data breach should be notified to the authorities and the deadline within such notification should be carried out.

The AEPD's criterion with respect to such notification is clear, considering that the notification of a personal data breach should not depend on the level of risk existing or the unlikelihood that such risk will materialise, but that it will be sufficient that there is a likelihood (whatever it may be) that there is a minimum risk to the rights and freedoms of natural persons. In addition, in this regard, it clarifies that it is not necessary for the risk to have been manifested for the breach to be notifiable, but it is sufficient that the risk is somewhat likely.

It is also relevant to point out that, according to the AEPD, the notification of the breach must be made at the time when the data controller detects that the breach has occurred, and in any case before the lapse of 72 hours, without waiting for a detailed examination or investigation of the situation. In this matter, the full risk assessment can take place in parallel with the notification and the information thus obtained can be provided in phases without undue delay. With regard to the way in which the communication is made to the data subjects, the AEPD does not object to it being done in phases, as long as the information provided is clear, complete and truthful.

In addition, the AEPD reiterates the importance of notifying as soon as it becomes aware of the existence of the likelihood of risk to the rights and freedoms of natural persons derived from the personal data breach. The Agency considers that, from that moment, the loss of confidentiality of the data may already be occurring, regardless of whether or not there is an improper access to it.

In view of the above, economic operators must equip themselves with protocols and tools to ensure the correct assessment of risk in the event of personal data breaches, taking into account factors such as the volume of data affected, its sensitive nature, the internal or external impact of the incident, among other matters. In conclu-

sion, as soon as there is a minimum likelihood or risk of a breach, the competent data protection supervisory authority must be notified.

## Conclusion

In short, the recent resolutions of the AEPD show a clear tendency to jointly sanction for the infringement of Article 5.1.f with either Article 32.1 or Article 25.1 of the GDPR, and even with both of them, considering that each one pursues a different purpose and must be evaluated independently.

On the other hand, despite the fact that the obligation to implement technical and organisational measures should be considered an obligation of means, taking into consideration the AEPD's criteria, it may be difficult for economic operators to clearly determine the level of adequacy of the measures which should be implemented taking into account the state of the art.

As for the definition of sensitive data, it goes beyond the provisions of Article 9 of the GDPR, including data whose disclosure results in the likelihood and severity of the high risk to the rights and freedoms of data subjects, capable of causing material or non-material physical damage.

Finally, the AEPD strictly interprets the deadline for notification of personal data breaches, as well as the approach that must be followed when making the decision to carry out such notification. Basically, the notification must be made as soon as there is a probability and risk to the rights and freedoms of the interested parties.