A pyme comercio

# Data protection for your SME at a glance.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
*"Una manera de hacer Europa"*

# Index

› Introduction 03.

› What is data protection? 04.

› Common data protection problems and errors 07.

› Applicable sanctions 08.

› Conclussions 09.

# Introduction

› Today, the use of new technologies, fed by data, is so common that almost all companies have become familiar to their daily use, and it is seen as something normal. In this scenario, **the privacy protection is a key challenge in the day-to-day work of companies.**

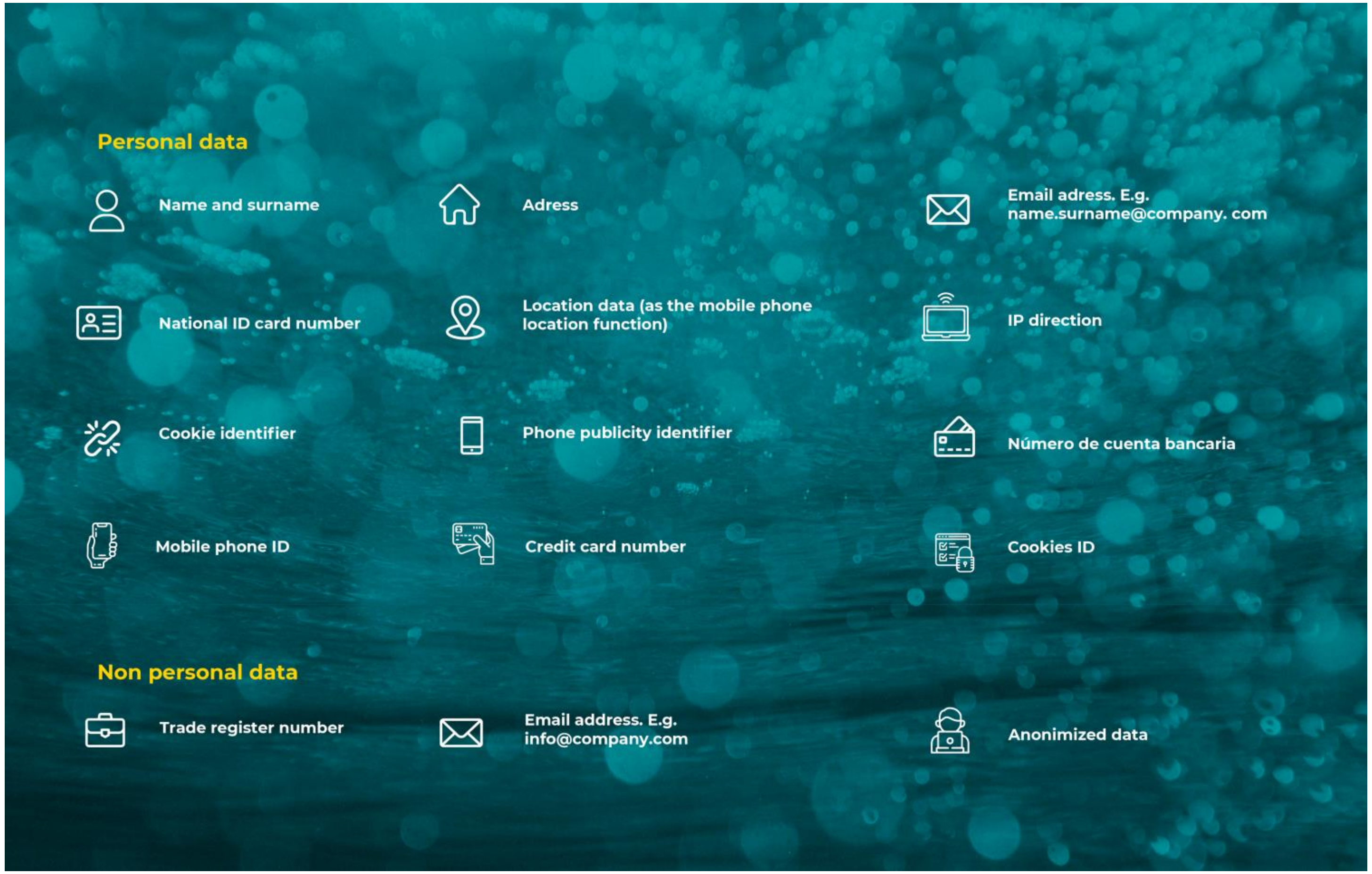
**Data are essential to improve the competitiveness of SMEs, as their correct analysis and exploitation generate opportunities to optimise business processes, support decision-making, help optimise costs and provide support in the control of business expenses.**

# What is data protection?

> Data protection is a fundamental right of all natural persons, which imposes a number of obligations and principles on companies to protect the personal data of their customers/suppliers/employees.

**Proper privacy management will bring numerous benefits to businesses, such as improved reputation, increased competitiveness, and above all, guaranteed compliance with regulations so as not to be fined and/or sued.**

> **We distinguish between two types of data: personal data and non-personal data.**



**Personal data**

- Name and surname
- Adress
- Email adress. E.g. name.surname@company. com
- National ID card number
- Location data (as the mobile phone location function)
- IP direction
- Cookie identifier
- Phone publicity identifier
- Número de cuenta bancaria
- Mobile phone ID
- Credit card number
- Cookies ID

**Non personal data**

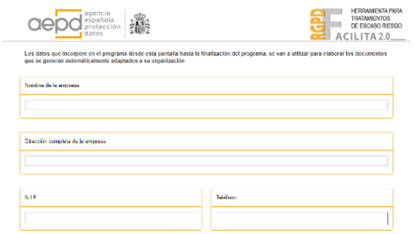
- Trade register number
- Email address. E.g. info@company.com
- Anonimized data

# What is data protection?

**› The Spanish Data Protection Agency aims to guarantee the privacy and data protection of citizens, as well as compliance with the General Data Protection Regulation (GDPR) and the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPD-GDD).**

The AEPD provides free tools for citizens to help them understand and assess their level of compliance with data protection regulations:

### Facilita RGPD



aepd agencia española protección datos
RGPD
HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO
FACILITA 2.0

Los datos que incorpore en el programa desde esta pantalla hasta la finalización del programa, se van a utilizar para elaborar los documentos que se generan automáticamente adaptados a su organización

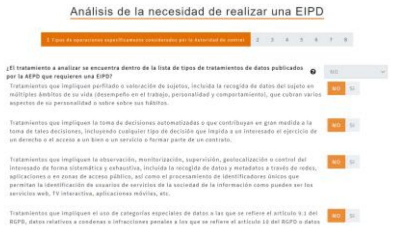
Nombre de la empresa

Dirección completa de la empresa

N.I.F.

Teléfono

### Gestiona EIPD



Análisis de la necesidad de realizar una EIPD

1 Tipos de operaciones específicamente considerados por la Autoridad de control
2
3
4
5
6
7
8

¿El tratamiento a analizar se encuentra dentro de la lista de tipos de tratamientos de datos publicados por la AEPD que requieren una EIPD? NO

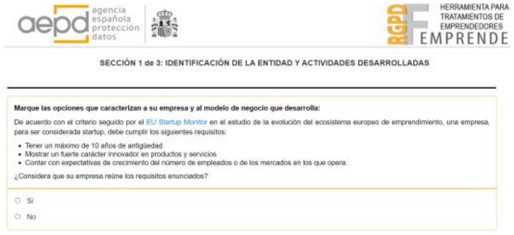
Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos. NO SI

Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato. NO SI

Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc. NO SI

Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos NO SI

### Facilita EMPRENDE



aepd agencia española protección datos
RGPD
HERRAMIENTA PARA TRATAMIENTOS DE EMPRENDEDORES
FEMPRENDE

SECCIÓN 1 de 3: IDENTIFICACIÓN DE LA ENTIDAD Y ACTIVIDADES DESARROLLADAS

**Marque las opciones que caracterizan a su empresa y al modelo de negocio que desarrolla:**

De acuerdo con el criterio seguido por el EU Startup Monitor en el estudio de la evolución del ecosistema europeo de emprendimiento, una empresa, para ser considerada startup, debe cumplir los siguientes requisitos:

- Tener un máximo de 10 años de antigüedad
- Mostrar un fuerte carácter innovador en productos y servicios
- Contar con expectativas de crecimiento del número de empleados o de los mercados en los que opera.

¿Considera que su empresa reúne los requisitos enunciados?

○ Sí

○ No

**› These tools generate the key documents that companies must have up to date in order to legally comply with regulations, so that they can be accredited to the authorities.**

In addition, and without being a tool in itself, the Oficina de Seguridad Internauta (OSI), of INCIBE, provides the possibility of identifying any type of security incident for your data, related to botnets, with the AntiBotnet service.

# What is data protection?

**These are the companies that must comply with the GDPR:**

- **EU-based companies, whether or not data processing is carried out in the EU.**
- **If the behaviour of EU citizens is monitored.**
- **If they offer goods or services to people in the EU.**

**How to comply with the regulation?**

- Identify whether the processing of the data is high-risk data
- Risk evaluation.
- Develop a procedure for verification, evaluation and assessment of the implementation of the measures developed for data protection.

**Depending on whether they are high or low risk treatments, different actions should be taken:**

### High risk

- Registration of activities involving treatment.
- Appointing a Data Protection Officer.
- Carry out an impact analysis of data processing.

### High + low risk

- Establish appropriate procedures.
- Review Data Protection Officer contracts.
- Establish policies to ensure data processing.
- Conduct employee training.

# Common data protection problems and errors

1. Lack of awareness of the **legal obligations on personal data protection**, as laid down in national legislation.

2. **Documents** with confidential and sensitive information should be **kept out of sight**.

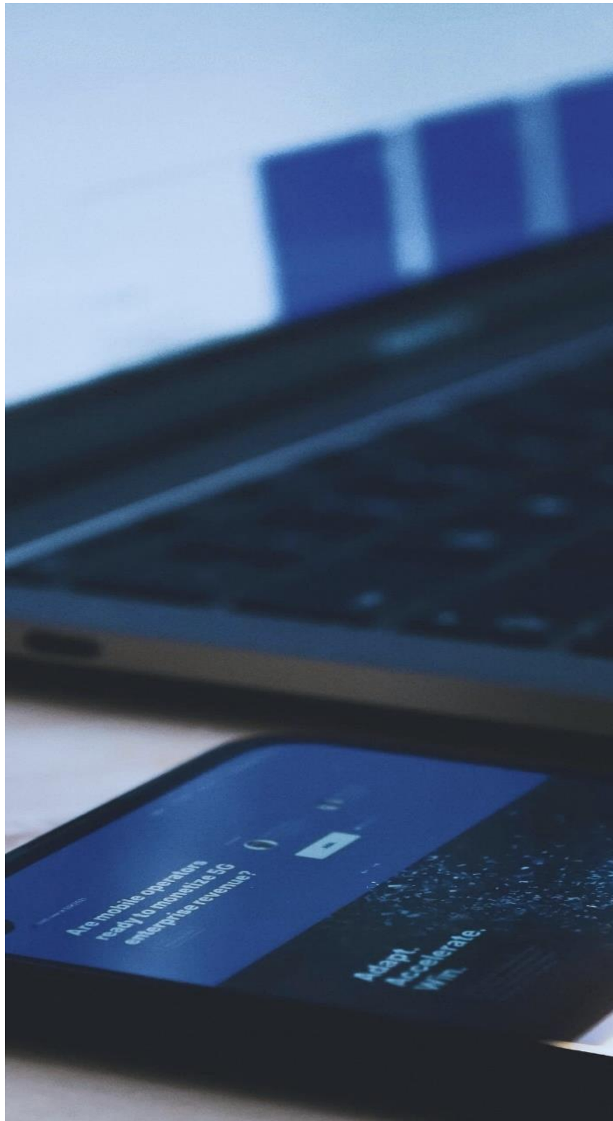
3. The use of **single contact forms** is another common mistake.

4. **Recruitment of employees who have a database of contacts,** as these contacts are often requested to be added to the database of the new company.

5. In some cases, **e-mail marketing campaigns or the sending of advertising** by post are also not permitted without the consent of the recipients.

6. Another mistake is the need to have the **company's details on its website** so that any user can consult them.

7. Ignorance of the need to **establish a contract with those responsible for the processing of their data**.

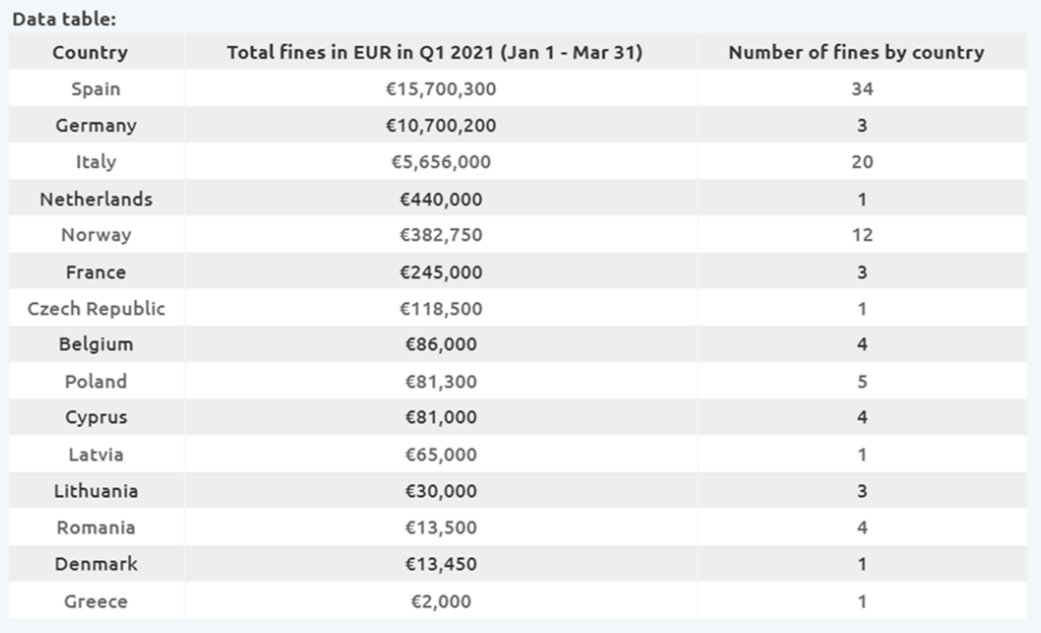


# Applicable sanctions

› **According to a study by Finbold, Spain leads in the number of fines imposed for non-compliance with the GDPR, with a total of 34 fines and more than €15 million in fines imposed by the authorities (in the first quarter of 2021).**

› **A KPMG study analyses the main reasons for sanctions, among them:**

> Failure to establish the necessary security measures for data processing.
> Lack of a legitimate basis for the processing of personal data.
> Lack of notification of security breaches and violations to users.
> Breach of the duty to inform.



Data table:

| Country | Total fines in EUR in Q1 2021 (Jan 1 - Mar 31) | Number of fines by country |
|---|---|---|
| Spain | €15,700,300 | 34 |
| Germany | €10,700,200 | 3 |
| Italy | €5,656,000 | 20 |
| Netherlands | €440,000 | 1 |
| Norway | €382,750 | 12 |
| France | €245,000 | 3 |
| Czech Republic | €118,500 | 1 |
| Belgium | €86,000 | 4 |
| Poland | €81,300 | 5 |
| Cyprus | €81,000 | 4 |
| Latvia | €65,000 | 1 |
| Lithuania | €30,000 | 3 |
| Romania | €13,500 | 4 |
| Denmark | €13,450 | 1 |
| Greece | €2,000 | 1 |

EU countries hit with over €30 million in GDPR fines in Q1 2021. Finbold. 2021.

## Sanction examples

**> In 2020, the Spanish Data Protection Agency fined a Madrid-based SME €50,000 for not having a DPO (Data Protection Officer) profile when it should have had one.**

**> Another example of a fine was for the re-use of papers with confidential data on the back by a lawyer. In this case the fine amounted to a total of €2,000.**

# Conclussions

- **The large volume of data managed by companies generated more than €2.5 billion in 2019.**

- There are multiple tools, made available by different public bodies, which aim to support companies in complying with personal data protection.

- **It is necessary to know the applicable legislation on data protection, as well as the main problems that may occur due to this lack of knowledge, since our business handles a large volume of personal data.**

**In conclusion, knowing the importance of the data, ensuring their proper treatment in accordance with the legislation and complying with the obligations established for companies are aspects that must be considered to avoid potential sanctions.**

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
*"Una manera de hacer Europa"*