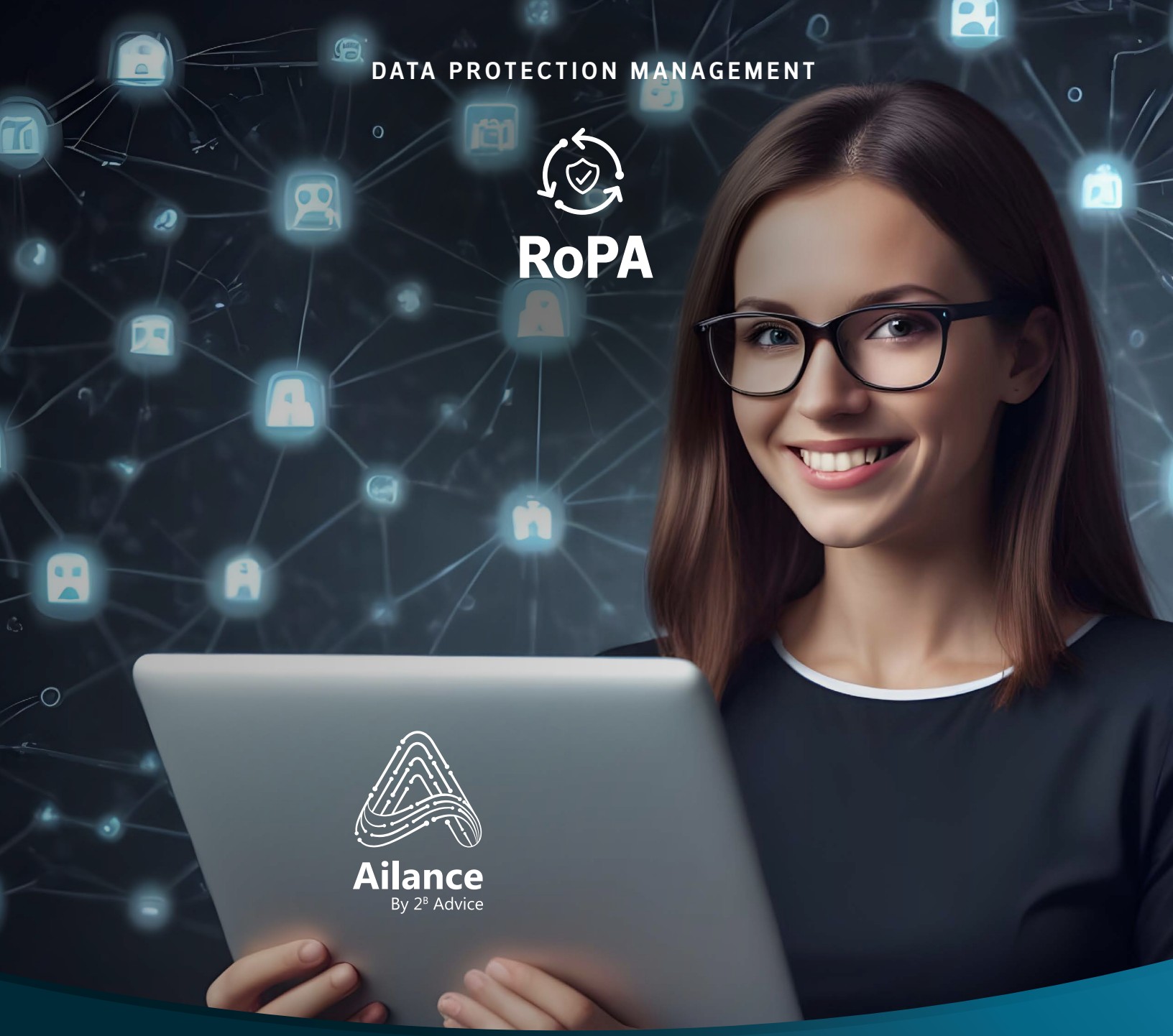

Data protection in SMEs

7 costly mistakes and how to avoid them

Serious risk instead of trivial offense:

Mistakes in data protection management with critical consequences

Fines of several tens of thousands of euros, customer terminations, loss of trust and damage to image. All due to supposedly minor errors in data protection management?

You may think: "This happens so rarely, nothing will happen." That's what the companies we worked with after these data protection shocks thought too.

Over the past 20 years, we have worked with more than 4,500 clients on data protection, including many SMEs. In the process, certain mistakes that companies made before we started working with them on data protection have occurred time and again.

We have compiled the 7 most common mistakes in this report so that you can avoid them, act with legal certainty and strengthen the trust of your business partners.

Find out on the following pages which data protection mistakes you should not make as an SME and how you can effectively avoid them.

The challenges in data protection management for SMEs

1,277 million €
is the amount of fines imposed for violations of the GDPR in 2021. This corresponds to an increase of 742% compared to 2020 (Enforcementtracker).

78%
of companies see a major challenge in the uncertainty surrounding the specific requirements of the GDPR (Bitkom 2024)

77%
think that the GDPR makes business processes more complicated.

Data protection is becoming increasingly complex.
There are always adjustments and additions that require new measures.

The challenge therefore lies in this:

- Keep track of all your obligations.
- To have the certainty of complying with the regulations.
- To keep your own data protection management costs as low as possible.

In order to ultimately realize the benefits of effective data protection management:

- **Increase compliance:** By reliably fulfilling all data protection regulations and thus protecting yourself from high fines.
- **Strengthen trust:** By demonstrating your compliance, you create trust with customers and business partners.
- **Prevent cyber attacks:** By reducing the attack surface for hackers and securing sensitive data.

The big question: How can we now effectively realize these benefits and overcome the current challenges?

7 costly mistakes in data protection management and how to avoid them

1 Missing or inadequate privacy policy

A clearly defined privacy policy is the basis for effective data protection management. Its absence can lead to uncertainties in the handling of personal data and jeopardize compliance with the General Data Protection Regulation (GDPR). Attention: Data protection declarations available online are not sufficient in many cases!

Example: A medium-sized company from the financial sector did not have a written privacy policy. The supervisory authority criticized this during a data protection audit - which resulted in severe penalties.

7 costly mistakes in data protection management and how to avoid them

2 Insufficient response to data breaches

The GDPR stipulates that notifiable data breaches must be reported within 72 hours. A late or inadequate response can not only result in high fines, but can also significantly damage the trust of those affected and the public.

Example: A retailer was the victim of a hacker attack in which customer data was stolen. Due to a lack of precautions and uncertainty about reporting obligations, the retailer did not inform those affected and the supervisory authority for two weeks. This not only damaged the retailer's image, but also resulted in a fine of 50,000 euros.

7 costly mistakes in data protection management and how to avoid them

3 Missing processing directory

Most companies are obliged to keep a record of processing activities. This register is not only used for internal control and management of data protection measures, but is also required for audits by the supervisory authorities. The absence of a record of processing activities can result in sanctions.

Example: A medium-sized software company had no overview of its data processing procedures. An audit by the data protection officer revealed considerable deficiencies, which led to high fines and conditions.

Manage processing activities efficiently

A digital tool allows you to quickly create and easily manage your processing directory.
The latest version of our software has recently been launched: Ailance™ RoPA.
With automations, soon-to-be-available AI features and unlimited customization options, even complex data protection management becomes a breeze.

RoPA
By 2B Advice

Find out more now
and test it free of charge for 14 days

7 costly mistakes in data protection management and how to avoid them

4 Insufficient technical and organizational measures

The security of personal data through appropriate technical and organizational measures is a central element of the GDPR. Companies that are negligent in this area are more susceptible to data leaks and cyberattacks.

Example: A medium-sized industrial company had outdated firewall systems and no encryption of emails containing customer data. Sensitive data was stolen in a hacker attack, which led to damage to the company's image and warnings from customers.

7 costly mistakes in data protection management and how to avoid them

5 Lack of data protection impact assessment

Processing operations that pose a high risk to the rights and freedoms of natural persons must be subject to a data protection impact assessment. Failure to carry out such an assessment can result in high fines and reputational damage for customers in the event of a data breach. However, if you carry out a data protection impact assessment, you can identify data protection risks at an early stage and implement appropriate measures.

Example: A medium-sized company introduced a new customer loyalty program with extensive profiling without a data protection impact assessment to be carried out. Following a customer complaint, this was objected to by the supervisory authority and a fine of EUR 30,000 was imposed.

7 costly mistakes in data protection management and how to avoid them

6 Insufficient training of employees

Employees play a crucial role in data protection management. Inadequately trained staff can cause unintentional data breaches. Regular training is therefore essential.

Example: In a medium-sized retail company, employees were not trained in the correct handling of customer data. As a result, data was sent unencrypted by email, which led to a data leak. The supervisory authority imposed a fine of 20,000 euros for inadequate employee training.

Ailance
By 2B Advice

7 costly mistakes in data protection management and how to avoid them

7 Inadequate client separation in data processing

In environments in which data from different clients is processed, strict separation of this data is of the utmost importance. Errors in implementation can lead to unwanted data access and thus to data breaches.

Example: A medium-sized IT service provider processed data from several customers on the same server environment. Due to configuration errors, employees were able to access the data of other customers. This led to contractual penalties and customer terminations.

Secure data protection management made easy

Effective data protection management is more than legal certainty.

By avoiding the 7 mistakes described and following the tips, you will have your data protection management properly under control.

That means:

- You act with legal certainty and do not allow high fines to be imposed on you.
- You protect yourself against cyber attacks.
- They strengthen the trust of customers, interested parties and business partners.

Data protection management with minimum effort?

Is it important to you to comply with data protection regulations, but do you not have the necessary expertise or resources internally?

At 2B Advice, we have been supporting companies worldwide in data protection management for over 20 years, including as external data protection officers.

Find out here how we solve data protection management for you securely and efficiently with Ailance DPO:
https://2badvice.de/ailance-dsb/

Do you have individual questions about your data protection management or would you like to find out how you can make your data protection management more efficient with our external data protection officers?

Then secure your free data protection check with one of our experts here:

Andreas Ingala

E-mail address:
andreas.ingala@2b-advice.com
Telephone number::
+49 151 53289737

About 2B Advice

The Integrated Risk Management Benchmark

For more than 20 years, 2B Advice has specialized in corporate solutions in data protection, compliance and risk management.
Over 450 international clients already use 2B Advice's external data protection consultants, among others.

It is particularly important to us to find the right solutions.
From start-ups to international corporations - we can offer the right strategy & implementation!