SME Guide to EU Compliance Volume II: **Data Protection and Privacy**

Spark Legal and Policy Solutions

12 March 2026

Spark
Legal and Policy Solutions Ltd

Table of Contents

Foreword

Have you ever come across terms such as GDPR, DPIA, ROPA, or DPA, and felt a headache coming on? Data protection and privacy can seem like a complicated and overwhelming part of running a business. However, as digital landscapes evolve, understanding the "how" of data management is no longer optional: it is a crucial competitive advantage for any scaling SME.

The vast majority of businesses recognise GDPR compliance as an important obligation.[1] However, reports show that 44% of small businesses are uncertain that the way they process customers' data is fully lawful.[2] A further 22% affirm that their business does not implement any technical measures to protect personal data at all.[3] When asked why they face difficulties in meeting data protection rules, businesses cite regulatory uncertainty and lack of internal resources as the biggest problems.[4]

Small and medium-sized businesses (SMEs) are placed in a particularly difficult position in this regard. While they enjoy some exemptions from the full data protection ruleset, compliance is still costly and time consuming. But it doesn't have to be this way: Volume II of our SME Guide to EU Compliance aims to break down the most important data protection obligations into clear, accessible, and actionable guidance. That way, you and your business are equipped with all the information necessary to master the basics, and one step closer to hitting the ground running.

Effective compliance with data protection requirements starts with getting the fundamentals right. By investing time upfront in designing and implementing workable structures and protocols, SMEs can put themselves on solid footing. Once these foundations are in place, compliance becomes less about constant reinvention and more about regular monitoring, training, and ensuring that these protocols are consistently followed across the organisation.

We hope this Guide supports SMEs in laying these foundations by clarifying what is required and how to approach it in practice. Data protection compliance ultimately brings about many positive outcomes – builds trust in your brand, saves you time and resources in the long term,

[1] Ceko, E., Komina, P. and Karras, D. (2025), *The Importance of GDPR Compliance and a Documentation Framework*. Available at: https://link.springer.com/chapter/10.1007/978-3-032-07370-9_23 (Accessed: 9 March 2026).
[2] GDPR.eu (2019), *GDPR Small Business Survey - Insights from European small business leaders one year into the General Data Protection Regulation*. Available at: https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf (Accessed: 3 March 2026).
[3] GDPR.eu (2019), *GDPR Small Business Survey - Insights from European small business leaders one year into the General Data Protection Regulation*. Available at: https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf (Accessed: 3 March 2026).
[4] Usercentrics (2025), *Two-thirds of European businesses doubt their compliance with data protection laws.* Available at: https://usercentrics.com/press/usercentrics-research-european-businesses-doubt-their-data-compliance/ (Accessed: 3 March 2026).

prevents loss of confidential information of your own company, and more.[5] Perhaps most importantly of all, data-compliant businesses help to protect people's privacy and create a safer online environment for everyone.

For those seeking additional support beyond this Guide in keeping oversight, monitoring compliance, or ensuring that these protocols are effectively implemented across the organisation, contact Spark Solutions at solutions@sparklegalpolicy.eu to see how we can help.

Now let's roll up our sleeves and dive into the wonderful world of data protection and privacy!

- *Esther Tenge, Principal Consultant for Digital and Technology at Spark.*

Background to Spark's SME Guide

The SME Guide is designed to bridge the gap between complex legal frameworks and practical business operations. We break down the law for entrepreneurs without legal expertise, highlighting key action points needed to ensure compliance while alerting you to critical upcoming legislative changes. Our goal is to make legal compliance a tool for growth, not a barrier.

Released in six Volumes, it contains the following:

- An overview of the **key legal areas** affecting SMEs based in the EU, across industries.
- A description of the **key legislative instruments** within those areas, and what they mean for businesses.
- Checklists of the **key action points** businesses must take to ensure compliance.
- A description of **key upcoming changes** in the law for businesses to look out for.
- **Notes and thoughts** from Spark's in-house legal experts.
- Accessible **explanations** of specialised concepts and terminology.
- **Summaries** of each Volume so you can capture the basics at a glance.

If you or your business needs legal assistance beyond this Guide, contact Spark Solutions at solutions@sparklegalpolicy.eu to see how we can help. Our in-house expertise combined with

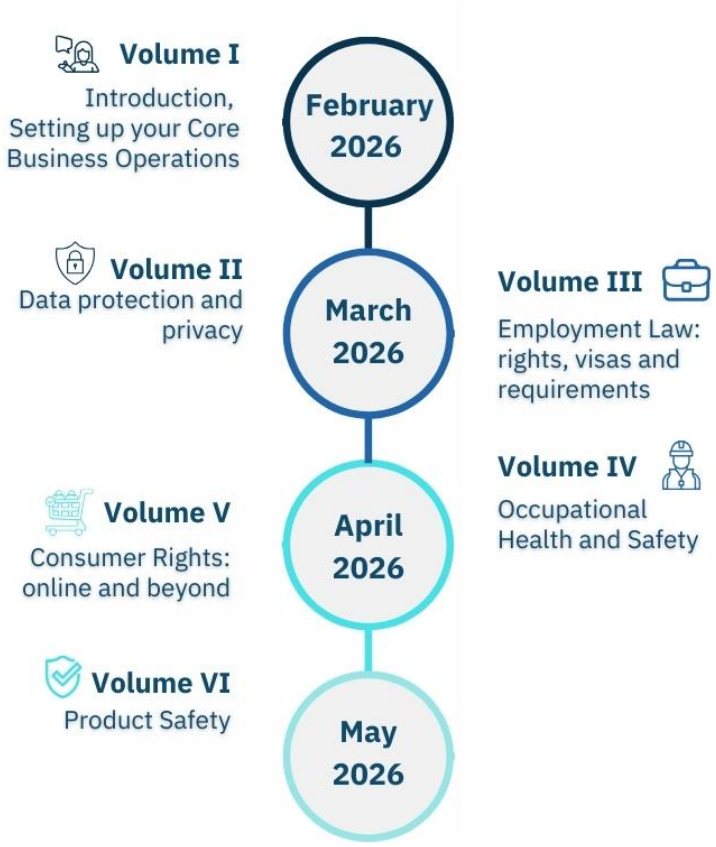
[5] Ullagaddi, P. (2024), *GDPR: Reshaping the Landscape of Digital Transformation and Business Strategy*. Available at: https://www.researchgate.net/profile/Pravin-Ullagaddi/publication/382969062_GDPR_Reshaping_the_Landscape_of_Digital_Transformation_and_Business_Strategy/links/66b5588251aa0775f275026d/GDPR-Reshaping-the-Landscape-of-Digital-Transformation-and-Business-Strategy.pdf (Accessed: 5 March 2026).

our network of over 3,000+ national legal experts ensures that your compliance needs are met at EU and national level, with a plan, budget, and schedule that works for you.

Go beyond the Guide: get in touch with **Spark Solutions** at solutions@sparklegalpolicy.eu today!

Note: This Guide is intended to act as a broad starting point for understanding compliance, rather than a comprehensive toolkit for navigating the full scope of EU law. It does not cover sector-specific regulations, such as medical regulations or transport regulations. It also does not address country-specific regulations.

Publication Roadmap



This Guide is intended for general informational purposes only and does not constitute legal or professional advice. Please note that the law may have changed since publication. Spark is not a law firm and is therefore not regulated by the Barreau de Bruxelles, or by equivalent authorities in other jurisdictions. Our services are designed to provide clients with high-quality legal research, drafting, and analysis, alongside any work of regulated legal professionals. We work with partner law firms across the EU and beyond where specific legal advice is required (e.g. contracting, litigation)

1. Introduction and Volume Checklist

In today's digital world, SMEs use many different tools and online platforms to run their daily operations. In doing so, most SMEs engage in activities that require them to comply with data protection and privacy regulations. Data protection legislation can be challenging to navigate, but understanding both the rules and their practical application is crucial for compliant digital business practices.

Spark's SME Guide aims to help businesses do exactly that, by addressing both the law and its practical application. As such, we help SMEs understand how data protection works in day-to-day business, and how they can meet their responsibilities in a clear and manageable way.

Part 2 of this Volume breaks down the core elements of the GDPR, including key definitions, the legal bases for processing, the documents businesses must maintain, how to handle data breaches, and how to uphold individuals' rights. Part 3 sets out the main obligations under the e-Privacy Directive, focusing on electronic communications, cookie rules, online marketing, and confidentiality requirements. Finally, Part 4 highlights upcoming regulatory changes that may affect SMEs and outlines the potential practical implications of these developments.

See below our checklist of practical action points a company should take in order to be compliant with the rules laid out in this Volume:

General Data Protection Legislation (GDPR)

- ✓ Ensure you rely on the correct legal grounds for processing personal data, as listed in GDPR Article 6. These most commonly include legitimate interest, contract, or consent, but consent is a less stable legal ground as it can be withdrawn.
- ✓ At the time when data is collected, provide notice of this to the data subjects with full information. The most appropriate way to do this is usually by including a privacy notice on your website and prompting users to read it before their data is collected.
- ✓ Keep an internal record of the data you collect and why (Record of Processing Activities).
- ✓ Sign agreements with all companies/service providers that process data for you (Data Processing Agreement).
- ✓ Before using personal data in a way that could be high-risk to the individuals concerned, conduct a Data Protection Impact

Assessment (DPIA). High-risk cases often involve the use of new or innovative technologies, as highlighted in GDPR Article 35.

- ✓ In the event of a data breach, inform your Data Protection Authority and the persons affected (including data subjects) within 72 hours.
- ✓ Where an individual makes a request with regard to accessing, updating or deleting their data in your systems, respond to their request within one month, free of charge.

e-Privacy Directive

- ✓ Obtain explicit consent from all users who visit your website where the cookies are non-essential.
- ✓ Include a clear cookie banner and a Cookie Policy on your website.
- ✓ Enable users to change or withdraw cookie choices at any time.
- ✓ For marketing emails/SMS messages, ensure that the user actively consents and include a straightforward option to unsubscribe.

Upcoming legislative changes

- ✓ Stay alert with regard to the Digital Omnibus package as it rolls out and changing AI rules.
- ✓ Contact Spark at solutions@sparklegalpolicy.eu to see how we can help you stay ahead, and stay complaint!

2. General Data Protection Regulation (GDPR)

2.1 Introduction to the GDPR

The General Data Protection Regulation (EU) 2016/679 (GDPR) is the cornerstone of data protection law in the EU.[6] It sets out the rights that individuals have in relation to their personal data, and the responsibilities of organisations to ensure those rights are protected. Indeed, any organisation that processes data related to EU citizens or residents, regardless of size, must comply with the GDPR.[7]

The GDPR applies ***extraterritorially*** – this means that even non-EU companies handling EU data must comply with the rules. "EU data" means personal data about individuals located in the EU, for example a Turkish company collecting information from customers in Belgium.

The GDPR includes two broad categories of rules that SMEs must comply with:

- **Data Protection:** Keeping personal data safe from unauthorised access, loss, or breach.
- **Data Privacy:** Empowering individuals to make informed decisions about who processes their personal data and for what purpose.

WHY IT IS VITAL FOR SMES TO COMPLY WITH THE GDPR:

- To prevent reputational damage.
- To maintain customer trust and competitiveness.
- To avoid financial penalties.
- To reduce risks of identity theft and fraud affecting customers.
- To avoid losing business opportunities.
- To meet legal obligations across the EU.
- To help protect people's privacy and make the internet a safer place for everyone.

[6] 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', OJ L 119, 4.5.2016, Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed: 26 February 2026).

[7] European Commission (n.d.) *Who does the data protection law apply to?* available at: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en (Accessed: 26 February 2026).

Consequences for non-compliance: fines for SMEs

SMEs can receive GDPR fines for simple mistakes, such as missing a Privacy Notice, failing to sign a DPA, not responding to data-subject requests on time or even accidental data breaches such as sending an email with a personal-data attachment to the wrong recipient. These fines are issued regularly across EU Member States and can range from a few hundred euros to several thousand, depending on the severity of the issue. While the GDPR allows fines up to €20 million or 4% of global turnover, most SME-level cases involve smaller albeit significant penalties that are easily avoidable with basic compliance. [8]

Since its enforcement in 2018, GDPR fines have been plentiful. Large companies have been fined in the billions: in May 2023, Meta was fined €1.2 billion for unlawful EU-US data transfers.[9] TikTok was fined €345 million for violating the special protection requirements for children's data.[10] Smaller companies have also faced significant penalties. The French Data Protection Authority in January 2025 alone fined an insulation company €15,000, an apprentice training centre €10,000, a road haulage company €8,000, and an energy brokerage company €4,000, all for failing to comply with the GDPR.[11]

[8] Regulation (EU) 2016/679, Articles 83(4-6).
[9] European Data Protection Board (2023) *1.2 billion euro fine for Facebook as a result of EDPB binding decision.* Available at: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (Accessed: 11 March 2026).
[10] Data Protection Commission (2023) Irish Data Protection Commission announces €345 million fine of TikTok. Available at: https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok (Accessed: 11 March 2026).
[11] Commission Nationale de l'Informatique et des Libertés (2026) Sanctions issued by the CNIL. Available at: https://www.cnil.fr/en/investigation-powers-cnil/sanctions-issued-cnil (Accessed: 11 March 2026).

2.2 Key Definitions

Before looking at the specific legal requirements, there are several key concepts set out in the GDPR that SMEs should understand:

- Personal Data: Any information relating to an identified or identifiable natural person. A person is considered 'identifiable' if they can be identified, directly or indirectly, by reference to an identifier such as a name, an ID number, an IP address etc. [12]

  Examples: Customer name, email, phone number, ID number, location, IP address, customer number, photos, financial data.

- Data Subject: An identified or identifiable person. Only individuals can have personal data; data relating to companies or organisations is not considered personal data.[13]

  Examples: A costumer, an employee, a website visitor, a job applicant.

- Data Processing: Data Processing is a broad concept under the GDPR; however, it can be briefly defined as any action a business takes with personal data.[14]

  Examples: Collecting, storing, sending, editing, deleting, analysing, sharing. Even keeping data in your email inbox counts as processing.

- Data Controller: Any entity that decides why and how personal data is processed.[15] Most SMEs are data controllers with regard to their client/customer data.

  Examples: Collecting names and email addresses of your clients to communicate with them or collecting the IP addresses of your website visitors to optimise your marketing.

- Data Processor: Any entity that processes personal data on behalf of a data controller without using it for their own purposes.[16]

  Examples: If you upload your clients' customer lists into an email-sending tool so it sends newsletters on your behalf, the email-sending tool is a data processor.

- Data Breach: Any incident that leads to the loss, disclosure, theft, alteration, or unauthorised access to personal data, accidental or intentional.[17]

  Examples: lost laptop, hacked email, file sent to the wrong person.

[12] Regulation (EU) 2016/679, Article 4(1).
[13] Regulation (EU) 2016/679, Article 4(1).
[14] Regulation (EU) 2016/679, Article 4(2).
[15] Regulation (EU) 2016/679, Article 4(7).
[16] Regulation (EU) 2016/679, Article 4(8).
[17] Regulation (EU) 2016/679, Article 4(12).

2.3 Legal Requirements for Lawful Data Processing

Personal data can only be processed when there is a legal basis under the GDPR.[18] Having understood the key concepts of the Regulation, this section now outlines the lawful grounds that SMEs must rely on to ensure their data processing activities remain compliant and justified.

Legal grounds listed under the GDPR

A. Lawfulness, fairness and transparency

Personal data must be collected and used in a lawful way, treated fairly, and explained clearly to data subject. First, SMEs must always rely on a **valid legal ground** for processing personal

[18] Regulation (EU) 2016/679, Article 5(1)(a).

data, as defined in Article 6 of the GDPR.[19] The lawful bases permitted under GDPR are listed in Article 6 and include the following:

i. **Performance of a contract**: Processing is necessary to fulfil contractual obligations.[20]

Example: If an online shopper purchases a book from an online bookstore, the bookstore must process the shopper's address in order to deliver their book.

ii. **Legal obligation:** The organisation must process the data to comply with the law.[21]

Example: You may be legally required to process employee salary information in order to comply with tax and social-security laws.

iii. **Vital interests**: Processing is necessary to protect life or prevent serious harm, particularly in crises or emergencies.[22]

Example: You may need to share a person's health information with paramedics to protect their life.

iv. **Public interest:** Processing is necessary to perform a task carried out in the public interest or by an official authority.[23]

Example: You may need to share a person's information with the police to assist them in arresting a suspect.

v. **Legitimate interest:** Processing is necessary for a clear and sensible business purpose, as long as this does not unfairly affect the person's privacy or rights.[24]

Example: You may collect information about how people use your website to see which pages perform well and improve the user experience, as long as this does not unfairly affect anyone's privacy. Businesses can comply with this by offering a clear Cookie Policy where users can easily choose which cookies they accept.

vi. **Consent of the personal data subject**: The data subject actively consents to their data being processed. Consent of the data subject must be freely given, specific, informed, and expressed through a clear and unambiguous indication of their wishes.[25]

Example: if you ask your customers to tick a box confirming they agree to receive your newsletter, that ticked box counts as consent.

[19] Regulation (EU) 2016/679, Article 5(1)(a).
[20] Regulation (EU) 2016/679, Article 6(1)(b).
[21] Regulation (EU) 2016/679, Article 6(1)(c).
[22] Regulation (EU) 2016/679, Article 6(1)(d).
[23] Regulation (EU) 2016/679, Article 6(1)(e).
[24] Regulation (EU) 2016/679, Article 6(1)(f).
[25] Regulation (EU) 2016/679, Article 6(1)(a).

Note: Consent is usually a last-resort legal ground for data processing, as it can always be withdrawn. The other five legal grounds are more stable.

Personal data must also be processed **fairly and transparently.** This means that individuals should clearly understand how their information is being used. Transparency requires giving data subjects the relevant information at the moment their data is collected (or obtained from a third party), and fairness requires that this information is provided in an accessible format, using clear and plain language.[26]

Example: If you collect email addresses to inform clients about products or projects, you must clearly explain how this data will be used, avoid sending unnecessary messages, and provide a straightforward way for clients to unsubscribe.

B. Purpose limitation

Personal data must only be collected where there is a **specific, explicit, and legitimate purpose** to do so. That purpose must be determined at the time that the data is collected.[27]

Example: If you collect a customer's home address for the sole purpose of delivering your product to them, you cannot later use it to send marketing materials or share it with another interested party. The data may only be used for the purpose for which it was originally collected.

C. Data minimisation

Controllers must ensure that the personal data they collect is adequate, relevant, and limited to what is necessary for the specific purpose, and processors must support this by handling only the data they are instructed to process.[28] SMEs should not collect more data than they need at the time of collection. SMEs should follow the logic of only collecting information that you ***need to know***- you must not collect information that is simply ***nice to have.***

Example: If you need to ship a product, the address and contact number are sufficient. You should not ask for further information such as date of birth, place of birth, nationality etc.

[26] Regulation (EU) 2016/679, Article 5(1)(a).
[27] Regulation (EU) 2016/679, Article 5(1)(b).
[28] Regulation (EU) 2016/679, Article 5(1)(c).

D. Accuracy

Controllers must ensure that personal data is **accurate and kept up to date**, and processors must support this by processing only the data they are instructed to.[29] It is important to review the accuracy of the data you process on a regular basis. Where data is found to be incorrect, it must be removed.

Example: If a client informs you that their address or phone number has changed, you must promptly update or remove the outdated data.

E. Storage limitation

Personal data **must not be kept longer than necessary.** SMEs should delete data once the purpose for collecting it is fulfilled. However, if SMEs wish to retain personal data for specific purposes such as archiving or research, they may do so only if the data is first anonymised (i.e., once all details that could reasonably lead to the person being identified are removed).[30]

Example: If you collect a customer's phone number only to confirm an appointment, you must delete it once that purpose is completed, unless you have another clear legal basis to keep using it (for example, if the customer has consented to receive future updates or marketing messages).

F. Integrity and confidentiality

Personal data must be **protected** against unauthorised access, misuse, and accidental loss.[31]

Example: You should secure your systems against cyber-attacks and ensure that any data collected is stored safely. Once you receive personal data, you are responsible for keeping it secure. You must also avoid sharing any personal data with third parties unless the data subject has given clear consent.

G. Accountability

Controllers are responsible for complying with all GDPR principles and must be able to demonstrate this.

[29] Regulation (EU) 2016/679, Article 5(1)(d).
[30] Regulation (EU) 2016/679, Article 5(1)(e).
[31] Regulation (EU) 2016/679, Article 5(1)(f).

When SMEs collect any personal data, they become the data controller and must show that they process data lawfully, fairly, securely, and only for the intended purpose.[32]

Example: Businesses must demonstrate accountability by in a number of ways, from making certain policies available on their website, to keeping internal records of data processing arrangements, to reporting data breaches quickly and accurately, to responding to data access requests. Each of these requirements are outlined in sections 2.4-2.6 of this Guide.

[32] Regulation (EU) 2016/679, Article 5(2).

2.4 Key Documents Your Business Must Keep for GDPR Compliance

There are several key documents that SMEs must maintain to ensure GDPR compliance. This section explains what these documents are, in which situations they are required, and how SMEs should keep them in a practical and compliant way.

A. Data Protection Impact Assessment (DPIA)

A DPIA is a structured check that SMEs must carry out before processing any data that could pose a risk to people's rights and freedoms in the event of a data breach.[33] It helps you think ahead, spot problems early, and plan how to avoid them.

When is a DPIA required?

You should carry out a DPIA when your planned data processing activity:

- Involves a lot of personal information, for example, data about many customers or employees, or detailed profiles about individuals.
- Uses information in a new or unusual way.
- Could have a big impact on someone if there is a mistake or misuse involving their data.[34]

If the activity could seriously affect someone's privacy, you will need a DPIA. For example, you must carry out a DPIA if you check your customers against any type of risk or fraud list. A DPIA is also required if you start using a new system that stores sensitive information, such as health details. In addition, installing cameras or other tools that monitor people, including staff or customers, requires a DPIA before the activity begins If you work with a small number of people and handle their personal data in simple, low-risk ways that are part of your regular business activities, a DPIA is not usually needed. For example, if you run a small online shop and only process basic customer information such as names, email addresses, and delivery details in

[33] Regulation (EU) 2016/679, Article 35.
[34] Regulation (EU) 2016/679, Article 35(3).

order to fulfil orders, this activity is considered low-risk and small-scale; you do not need to conduct a DPIA.[35]

What should a DPIA include?

The DPIA should clearly explain:

- What you plan to do with the data you process.
- Why you need the information you plan to process in order to meet your objective.
- The risks that could occur for data subjects in the event of a data breach
- What you will do to reduce the risks and keep data subject information safe.[36]

If after carrying out the DPIA it becomes clear that the planned data processing would present a high risk to data subjects, you must consult relevant data protection authority[37] before starting the activity.[38] For example, if a business starts using a tool that tracks the location of its delivery drivers in real time, including detailed movement patterns and daily behavioural data, this could create a significant risk to individuals' privacy. If the DPIA still shows a high risk after safeguards are added, the SME must consult the **Data Protection Authority** before going ahead.

A **Data Protection Authority (DPA)** is the independent public authority in each EU country that ensures the protection of personal data and compliance with the. DPAs handle complaints, give guidance, supervise companies, and can issue fines when rules are broken.[39]

B. Privacy notice/privacy policy

A Privacy Notice is a document that explains to people what information you collect about them, why you collect it, who you share it with, and what rights they have.[40] Every business must have a Privacy Notice, and the level of detail can remain simple depending on your business, the type

[35] European Commission (n.d.) *When is a Data Protection Impact Assessment (DPIA) required?* Available at: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en (Accessed: 4 March 2026).
[36] Regulation (EU) 2016/679, Article 35(7).
[37] The relevant DPA is the supervisory authority of the EU country where your business is established or, if you process data across borders, the authority of your main establishment. You can find the full list of national authorities here: https://digital-strategy.ec.europa.eu/en/library/list-personal-data-protection-competent-authorities.
[38] Regulation (EU) 2016/679, Article 36.
[39] Regulation (EU) 2016/679, Articles 51-59.
[40] Regulation (EU) 2016/679, Article 12(1).

of data you process, and the purposes for which you use it.[41] A clear Privacy Notice helps people understand what happens to their information and shows that your business is open and trustworthy.

Where should you put your privacy notice?

Your Privacy Notice should be easy for people to find. It can be placed on your website, usually in the footer. It must also be accessible from any form where you ask people for permission to process personal data, and through any other means through which a person provides their personal data to you, such as a newsletter sign-up page or a contact form.[42]

What should a privacy notice include?

Your Privacy Notice should explain in clear language:

- Who you are and how people can contact you.
- What personal data you collect and why you collect it.
- Who you share the data with, including any providers outside the EU.
- How long you store the data.
- The rights people have over their data.
- How somebody can make a complaint if they are unhappy about how their data is being processed.[43]

C. Records of Processing Activities (ROPA)

Businesses need a ROPA because the GDPR requires controllers to document their processing activities, especially when they handle personal data on a regular basis. A ROPA is a written record that explains how your business handles personal information.[44] Different to a Privacy Notice, a ROPA is an internal accountability document and is not intended to be public or shared with data subjects.

A ROPA must include a clear overview of:

[41] Regulation (EU) 2016/679, Articles 12-14.
[42] Regulation (EU) 2016/679, Article 13(1).
[43] Regulation (EU) 2016/679, Article 13(1).
[44] Regulation (EU) 2016/679, Article 30.

- Who you are (your business name and contact details) and why you collect personal data.
- The types of personal data you collect and whose data it is (such as customers, employees, or website visitors).
- Who you share the data with, including any external companies that help you deliver your services.
- Whether any data is sent outside the EU and how it is protected.
- How long you keep the data and the reasoning behind those retention periods.
- The basic security measures you follow to keep the data safe.[45]

If you use any external service providers such as mailing tool services or booking systems, those service providers must also keep a shorter version of this list, explaining which activities they carry out for you and whether they send any information outside the EU.[46]

Your ROPA can be kept digitally as a simple document or spreadsheet and must be shown to your national data protection authority upon request.[47]

Possible SME exemption to ROPA

Under the GDPR, businesses with fewer than 250 employees do not need to keep a full and detailed ROPA, as long as the personal data they handle is processed only occasionally, does not include special category or criminal data, and is not high risk.[48] The "occasional" exemption has been interpreted narrowly to mean processing that happens very infrequently and is not part of the business's daily, regular or predictable activities. Most SMEs process personal data every day (for example, keeping customer lists, managing bookings, or sending invoices), so this exemption rarely applies in practice.[49]

For this reason, even small businesses are encouraged to keep a simple, lightweight ROPA, which helps them stay organised and demonstrate compliance if needed.

D. Data Processing Agreement (DPA)

A DPA is a written contract between a business (the controller) and any outside company that handles any personal data (the processor) for the data controller. It explains how the processor

[45] Regulation (EU) 2016/679, Article 30(1).
[46] Regulation (EU) 2016/679, Article 30(2).
[47] Regulation (EU) 2016/679, Article 30(4).
[48] Regulation (EU) 2016/679, Article 30(5).
[49] European Data Protection Board (2025) *Targeted modifications of the GDPR: EDPB & EDPS welcome simplification of record keeping obligations and request further clarifications*. Available at: https://www.edpb.europa.eu/news/news/2025/targeted-modifications-gdpr-edpb-edps-welcome-simplification-record-keeping_en (Accessed: 3 March 2026).

must handle the controller's data. For example, if you share your customers' phone numbers with a delivery company so they can bring orders to them, you need a DPA with that delivery company.

Under the GDPR, a DPA is mandatory whenever an SME uses an external service to store, manage, or otherwise handle personal information.[50] This includes everyday tools used by small businesses such as systems for appointments, newsletters, payments, form submissions, or customer communication.[51]

A DPA must clearly describe the personal data that the external company handles, why they handle it and for how long, who the data belongs to, and what the company is allowed to do with the data.[52] The DPA must be in writing and can be kept in digital form.[53]

A DPA must also require the external company to:

- Process the data only according to your written instructions and keep all personal data confidential.
- Take appropriate steps to keep the data safe and ask for your permission before involving any other company (a sub-processor).
- Help you respond to requests from individuals who want to access, correct, or delete their personal data.
- Help you meet your GDPR duties where possible, for example during a security incident.
- Delete or return all personal data when the contract between you ends and provide any information you need to demonstrate GDPR compliance, including allowing audits if necessary.[54]

Note: If the external company uses another provider, the same protections required under the DPA must also apply to that company.

SMEs may also act as a processor for another organisation. If your business processes personal data on someone else's instructions, you must follow the same rules explained above.

[50] Regulation (EU) 2016/679, Article 28(3).
[51] GDPR.eu. (n.d.). *What is a GDPR data processing agreement?* Available at: https://gdpr.eu/what-is-data-processing-agreement/ (Accessed: 3 March 2026).
[52] Regulation (EU) 2016/679, Article 28(3).
[53] Regulation (EU) 2016/679, Article 28(9).
[54] Regulation (EU) 2016/679, Article 28(3).

2.5 Personal Data Breach and Breach Notification Obligations

Sometimes, even if your business is diligent with its data protection compliance and follows all procedures correctly, a personal data breach can still occur. Knowing how to respond in such a situation is critical, as your actions in the immediate hours can significantly reduce the impact that the breach has on your data subjects.

A data breach occurs when personal data is lost, stolen, shared with the wrong person, or accessed by someone who should not see it.[55] According to the GDPR, there are certain actions that you must take immediately in case of a personal data breach.

These actions are as follows:

- ✓ You must quickly understand the incident and decide whether it has created a privacy risk to your data subjects.
- ✓ If the breach has created such a risk, you must report it to your national Data Protection Authority within 72 hours.[56]
- ✓ If the breach has created a high risk to your data subjects (e.g., identity theft, fraud), you must also tell the individuals directly and without delay.
- ✓ You must keep an internal record describing what happened, when it happened, how it was handled, and what measures were taken.
- ✓ You must take appropriate measures to protect personal data and improve security after a breach.[57]

[55] Regulation (EU) 2016/679, Article 4(12).
[56] Note that this information may change. See Part 4 of this Volume for more information.
[57] These actions are derived from the GDPR's breach notification rules, in particular Articles 33 and 34, together with the accountability and security principles in Articles 5(2) and 32.

2.6 Individual Rights under the GDPR and What Businesses Must Do to Protect Them

Just as GDPR places obligations on businesses to protect personal data, it equally grants rights to data subjects in relation to deciding how their data is processed.[58] These rights are as follows:

A. Right of access

Definition: The right of access means that individuals can ask a company what personal data it holds about them and how that data is being used. This information must be provided free of charge.[59]

Scope: Under right of access, a data subject can request the following information:

- The purpose of the processing and the nature of the personal data you hold.
- The recipients you share the data with, including any extra-EU transfers.
- How long you keep the data and how you decide the storage period.
- Information regarding their rights as a data subject, such as rectification, erasure, restriction or objection, and their right to complain to a supervisory authority.[60]
- The source of the data, if you did not collect it directly from the data subject themselves.[61]

SMEs must answer subject access requests within one month. [62] Before responding to an access request, you should first confirm the person's identity to avoid disclosing data to the wrong individual. Ideally, this should be done by requiring the user to use an online account with verified login credentials. Alternatively, you can ask for probative information that is part of the personal data you already keep (e.g., the amounts on the last two invoices you have sent that individual). The more sensitive the data that the user requests access to, the higher the threshold for authentication.

[58] Regulation (EU) 2016/679, Articles 15-21.
[59] Regulation (EU) 2016/679, Articles 15.
[60] More information on these rights is provided throughout this part.
[61] Regulation (EU) 2016/679, Article 15.
[62] According to the GDPR, it must be responded within one month. See Regulation (EU) 2016/679, Article 12.

In exceptional cases, you may ask the person to provide proof of ID. However, this must only be done where absolutely necessary – otherwise, you risk excessive data collection in breach of the data minimisation rule.

How SMEs should respect the right of access:

- ✓ Set up a simple internal process that explains who checks the request, who finds the data, and who sends the reply. If your company has appointed a Data Protection Officer (DPO), they may check the request.[63] The team member who manages the relevant information may locate the data. The DPO or your privacy contact usually sends the response.
- ✓ Keep a record of the data that you process or store so that the personal data you hold concerning the data subject is easily found.
- ✓ When responding to a Subject Access Request, you must provide a copy of the person's data and a clear explanation of how and why you used it, including all information required under Article 13:[64]
- ✓ Who you are, how they can contact you, and the contact details of your Data Protection Officer (if you have one).
- ✓ Why you use their personal data, the legal basis you rely on, and, if relevant, what your legitimate interests are.
- ✓ Any third parties who receives their data, including any service providers, and whether it is transferred outside the EU, together with the safeguards you use to protect their data during such transfers.
- ✓ How long you keep the data, or how you decide on your retention periods, and what rights they have (such as access, correction, deletion, restriction, portability, and objection).
- ✓ A reminder that consent can be withdrawn at any time (if you rely on it), that they may complain to the supervisory authority, and whether providing the data is required and what happens if they do not.
- ✓ Where you obtained their data (if it did not come directly from them), and whether you use automated decision-making or profiling including a simple explanation of how it works and what it means for them.

[63] Under Article 37 of the GDPR, a Data Protection Officer (DPO) is required only in specific situations, such as when an organisation carries out large-scale monitoring or processes sensitive data on a large scale. As a result, most SMEs are not required to appoint a DPO.
[64] Regulation (EU) 2016/679, Article 13.

- ✓ A final note guaranteeing that you will inform the data subject before using their data for any new purpose. [65]

B. Right to rectification

Definition: The right to rectification means that if a person's information is wrong or incomplete, SMEs must correct it in a timely manner and make sure the updated information is accurate everywhere it is used.[66] SMEs are not required to run regular accuracy checks, but they must correct or update data as soon as they become aware that it is inaccurate, including when the data subject notifies them.

How SMEs should respect the right to rectification:

- ✓ Set up an easy way for people to tell you their information is incorrect (email, form, or phone contact).
- ✓ Where you have been informed of inaccurate data, update the data promptly in all relevant systems (HR tools, mailing lists, etc.).
- ✓ If you have shared this data with any other companies, you must also tell them to update it, so the mistake does not continue.
- ✓ Keep a short internal note that the correction was made.[67]

C. Right to erasure

Definition: The right to erasure means that if a person requests that a company deletes their personal data, the company must respect this request and make sure it is removed from all the places where the company uses it.[68]

Scope: The right to erasure is not an absolute right. In most cases, you must delete personal data when a person asks, but there are situations where you are allowed to keep it for a good reason.

When must you delete the data?

- Where you do not need the data anymore for the reason you originally collected it.

[65] Automated decision-making refers to when a computer makes a decision without human review. Profiling means using someone's personal data to predict things about them, such as showing targeted adverts. If you use these systems, you must ensure that a human can review important decisions, explain to individuals how the decision was made, and allow them to challenge it.
[66] Regulation (EU) 2016/679, Article 16.
[67] These actions follow the requirements set out in Articles 16 and 19 of the GDPR, together with the accuracy and accountability principles in Articles 5(1)(d) and 5(2).
[68] Regulation (EU) 2016/679, Article 17.

- Where the person withdraws their consent, and you have no other legal reason to keep using the data.
- Where the person objects to your use of their data, and you do not have a stronger reason to continue using it.
- Where you used or collected the data in the wrong way (unlawfully).
- Where EU or national law requires you to delete it.
- Where the data was collected from a child when providing online services to children.
- If the data was made public.
- If your company has publicly shared the data (e.g., posted online), and you must delete it, you should take reasonable steps to let other organisations know that the person asked for their data to be removed too. You only need to do what is realistically possible and affordable.[69]

When can you retain the data?

There are some situations where you are allowed to retain personal data even where the data subject asks for deletion:

- Freedom of expression or information: You may keep the data if deleting it would interfere with legitimate reporting or public information.
  Example: A local news blog publishes a photo from a public event. If someone in the photo asks for deletion, removing it could affect the news record.

- Legal obligation or public interest: you may keep the data if it is necessary to comply with a legal obligation or to perform a task in the public interest.
  Example: A small accounting firm must keep invoices for a certain number of years by law. Even if a customer asks you to delete their data, you cannot delete those invoices.

- Public health: you may keep the data if it is needed for public health reasons.
  Example: A small clinic or pharmacy must keep vaccination or infection-related records for health authorities. A patient cannot ask you to delete that data immediately.

- Defence of legal claims: you may keep the data if it is necessary for your defence in a legal claim.

[69] Regulation (EU) 2016/679, Article 17(1).

Example: A customer threatens a complaint or lawsuit about a service. You may need to keep emails, contracts, or messages as evidence, even if they ask you to delete their data.[70]

How SMEs should respect the right to erasure:

- ✓ Double-check whether you must delete the data or whether an exception applies (for example: a legal obligation or the need to retain data for a legal claim).
- ✓ Find all places where you store the person's data and remove it from each system or tool.
- ✓ Inform any third parties you shared the data with so they can delete it too.
- ✓ If immediate deletion is not possible, make sure the data is not used anymore and will be removed automatically in the next backup cycle.
- ✓ If you shared the data publicly, contact the platforms or organisations where you posted it and request removal.
- ✓ Keep a short internal note showing that you deleted the data or explaining why you could not delete it.[71]

D. Right to data portability

The right to data portability means that upon request, SMEs must give data subjects their personal data in a structured, commonly used, and machine-readable format (i.e., a format that a computer can open and use without any problems). This right applies only when the person gave their data voluntarily (consent) or signed a contract, and if the data is processed by automated means.[72]

How SMEs should respect the right to data portability:

- ✓ Prepare a clear digital file that contains the person's information in an organised way so it can easily be saved or shared, for example in a commonly used format such as PDF or Word.
- ✓ Include only the personal data the individual gave you, or the data that was created directly through that individual's use of your service.
- ✓ Make sure the file is easy to understand, without requiring special software or technical knowledge.
- ✓ Send the file securely to the individual or, should they request it, directly to another organisation or service they choose.

[70] Regulation (EU) 2016/679, Article 17(3).
[71] Regulation (EU) 2016/679, Article 17.
[72] Regulation (EU) 2016/679, Article 20.

- ✓ Keep a short internal note that you completed the portability request.

E. *Right to object*

The right to object means that if a person does not want their personal data to be used for a certain purpose, they can ask SMEs to stop processing their data for that purpose. This right is especially important for direct marketing, where SMEs must stop using the person's data immediately once they object (unsubscribe).[73]

How SMEs should respect the right to object:

- ✓ Make sure people can easily say they no longer want their data to be used for a specific purpose (for example through an unsubscribe link or a simple message).
- ✓ Stop using their data for that purpose as soon as they object, especially for marketing.
- ✓ Check whether there is any legal reason that requires you to continue using the data, and if not, stop the processing completely.
- ✓ Make sure all your systems and tools reflect the objection so the person does not receive unwanted messages again.
- ✓ Keep a short internal note that the objection was received and that the processing was stopped.[74]

F. *Right to restrict processing*

The right to restrict processing means that where a person asks, SMEs must temporarily pause using their personal data. This happens in situations where the person says the data may be incorrect, believes you used it in the wrong way but prefers it not to be deleted, needs it kept for legal reasons, or has asked you to stop using it while you review their concerns. During this pause, the data can be stored, but it cannot be used unless the person agrees or there is a clear legal need.[75]

How SMEs Should respect the right to restrict processing:

- ✓ Mark the person's data as restricted in all your systems so it cannot be used while the issue is being reviewed.

[73] Regulation (EU) 2016/679, Article 21.
[74] Regulation (EU) 2016/679, Article 5(2).
[75] Regulation (EU) 2016/679, Article 18.

- ✓ Do not use the data for any activity (for example marketing, profiling, or analysis) until the restriction ends.
- ✓ If the person needs the data for legal reasons, keep it safely but do not use it for anything else.
- ✓ Once the reason for the restriction is solved (for example the data is corrected or your review is finished), inform the person before you start using the data again.
- ✓ Keep a short internal note showing when the restriction was imposed and when it was lifted.

Summary of Part 2

- The GDPR sets the core rules for how SMEs must collect, use, store, and protect personal data in the EU.
- SMEs must always have a lawful basis for processing and clearly explain to their data subjects how and why they process their data.
- Key GDPR principles, lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, and security, apply to all processing.
- Individuals have strong rights (access, deletion, correction, objection, portability), and SMEs must respond to data subject requests within one month.
- SMEs must keep simple records of their processing activities, maintain a clear Privacy Notice, and ensure that processors meet GDPR standards.
- SMEs must have procedures for detecting and reporting personal data breaches. Failing to comply can lead to reputational damage and significant fines.

3. e-Privacy Directive

3.1 Introduction to the e-Privacy Directive

Directive 2002/58/EC (The e-Privacy Directive) came into force on 31 July 2002 and complements GDPR but focuses specifically on electronic communications, cookies, email marketing, and confidentiality of online communications[76] Unlike the GDPR, which is a regulation and therefore directly applicable in all EU Member States, the e-Privacy Directive is transposed by each Member State through national law and regulation. SMEs should ensure full compliance with such national rules.

Key definitions

Just like the GDPR, the e-Privacy Directive contains several key definitions that SMEs should understand before applying the rules. The most important key definitions are as follows:

User: A user is the person who uses publicly available electronic communications services for private or corporate purposes without having any subscription.[77]

Cookies: Cookies are small files that websites place on a visitor's phone or computer to remember information about their visit.[78]

Cookies are divided into two groups under the e-Privacy Directive, depending on whether they require explicit consent or not:

a) Strictly necessary cookies: Cookies that are essential for the website to function, and do not require consent.[79]

   Example: Security cookies that detect the fraudulent activities to protect users.

b) All other cookies: Cookies that are not essential and require explicit consent before being used.[80]

   Example: Cookies that follow users' habits on the website and display targeted ads.

[76] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), Official Journal L 337/11., Article 1.
[77] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 2(a).
[78] European Commission (n.d.), *Cookies policy*, Available at: https://commission.europa.eu/cookies-policy_en (Accessed: 3 March 2026).
[79] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 5(3).
[80] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 5(3).

3.2 Key Obligations under the e-Privacy Directive

A. *Cookie policy*

Under Article 5(3) of the e-Privacy Directive, websites must give users clear and comprehensive information before placing any cookies that are not strictly necessary. This information is usually provided in a Cookie Policy.[81]

A Cookie Policy must clearly explain:

- Which cookies are used (strictly necessary or consent-required cookies).
- Why each cookie is used.
- How long each cookie stays on the device.
- Whether any cookies come from third parties (e.g. advertising or analytics tools).
- Whether cookie data leaves the EU, if applicable.
- How users can change or withdraw their cookie choices at any time.[82]

B. *Marketing emails/SMS*

If a business wants to send marketing emails or SMS messages to a user, it must get their clear opt-in consent first.[83] Consent in this context means that the user chooses to receive marketing by taking a clear action, such as ticking a box. If the user does nothing, you cannot contact them – silence or continued browsing does not count as valid consent. Moreover, every marketing message must include a clear and straightforward option to unsubscribe.[84]

[81] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 5(3).
[82] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 5(3).
[83] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 13.
[84] Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH, Judgment of 1 October 2019. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0673 (Accessed: 3 March 2026).

C. Confidentiality of communications

Businesses must keep electronic communications confidential.[85] This means that online communications such as email content, phone calls, chats and messages are private- they cannot be listened to, scanned, stored, or monitored by a third party. Exceptions to this rule apply where the user has consented to their communications being monitored, where it is strictly required to provide the service (e.g., spam filtering, security checks), or it is required by law.[86]

D. Third-party tools

Third-party tools are features on your website that come from another company, such as embedded videos, maps or statistics, or simple website traffic monitoring tools. Third-party tools often place their own cookies, so users must be able to accept cookies" before these parts of your website load. Third-part tools must also be clearly explained in your Cookie Policy.[87]

Practical Tips for SMEs

SMEs must follow the e-Privacy Directive when using cookies or sending marketing messages. Below are the practical actions SMEs should take to comply:

- ✓ Ask for explicit consent before using any cookies that are not essential for the website to function, including cookies used for measuring website use or showing personalised ads.
- ✓ Offer a clear "Reject all" option in the cookie banner, alongside "Accept all", and never use pre-ticked boxes. Consent must be an active choice (tick boxes must be off by default).[88]
- ✓ Allow users to change their cookie choices at any time, for example through a "Cookie settings" link.
- ✓ Provide a simple Cookie Policy, separate from the Privacy Policy, explaining which cookies your website uses, why you use them, how long they stay on the device, and how users can change their choices.

[85] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 5(1).
[86] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 5(2).
[87] Directive 2002/58/EC, as amended by Directive 2009/136/EC, Article 5(3).
[88] Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH, Judgment of 1 October 2019. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0673 (Accessed: 3 March 2026).

- ✓ Keep a basic record of cookie consents (for example, which version of the banner was shown and when consent was given).
- ✓ Review and remove tools from other companies that place their own cookies, such as tools used to display videos, maps, or website statistics, if you do not genuinely need them.
- ✓ Send marketing emails or SMS messages only if the person has actively chosen to receive them (opt-in consent) and include an easy unsubscribe link in every message.[89]

Summary of Part 3

- The e-Privacy Directive complements the GDPR by regulating cookies, electronic communications, and marketing.
- SMEs must obtain explicit consent for analytics and advertising cookies and provide a clear "reject all" option.
- A Cookie Policy is required separate to the Privacy Policy, and users must be able to change their preferences at any time.
- Marketing emails and SMS generally require opt-in consent and must include an easy unsubscribe option.

[89] These actions reflect the requirements of Article 5(3) and Article 13 of the e-Privacy Directive, together with the accountability principle in Article 5(2) of the GDPR.

4. Upcoming Legislative Changes

Digital Omnibus (2025-2027) and AI Rules

Data protection rules continue to evolve, and SMEs must stay alert to upcoming changes that may affect how they collect, use, and protect personal data. After understanding the GDPR and the e-Privacy Directive, it is important for small businesses to be aware of new or future regulations that could require updates to their policies, tools, and everyday practices.

In this section, we outline some important upcoming changes that may impact SMEs.

Digital Omnibus (2025–2027)

The Digital Omnibus is a large package of technical amendments the EU is introducing to streamline and modernise many existing digital laws. It is expected to start applying in 2026. Rather than creating a brand-new regulation, the Omnibus updates several pre-existing frameworks at once to make compliance simpler, clearer and more consistent for businesses.[90] For SMEs, the goal is to reduce unnecessary administrative burdens, remove overlaps between laws, and provide more harmonised obligations across the EU.

The most important upcoming changes are as follows:

- The Digital Omnibus will streamline several EU digital laws by merging cookie rules into the GDPR, When the new EU rules enter into force, websites will have to respect the cookie preference a user sets in their browser. If the user's browser is set to reject tracking cookies, the website must follow that choice automatically and cannot ask again. Once the user has said "no," the website is not allowed to show the same cookie banner for at least six months, which means users will stop seeing repeated pop-ups and SMEs will not need to keep asking for the same permissions.[91]
- Small businesses that process very limited, non-sensitive data such as a small local clothing boutique that only collects a customer's name and email when they sign up for a discount list, may no longer need to provide full privacy notices every time.[92] This change does not mean removing the Privacy Notice. It simply allows very small

[90] European Commission (2025) Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, p. 1. Available at: https://eur-lex.europa.eu (Accessed: 26 February 2026).
[91] European Commission (2025), COM(2025) 837 final, p.60.
[92] European Commission (2025), COM(2025) 837 final, p.56.

businesses, in low-risk and simple situations, to provide a shorter information message together with a link to the full Privacy Notice instead of repeating the entire Article 13 information each time. For example: "We use your name and email to send you your discount code. See our full Privacy Notice here."

- The deadline to report personal data breaches will be extended from 72 to 96 hours,[93] and organisations will be allowed to reject abusive or excessive access requests.[94]
- The EU will replace national DPIA lists with one single EU-wide DPIA list,[95] so SMEs will no longer need to check different national rules. This simplifies compliance for companies operating in more than one Member State.

AI Rules

The EU's new AI rules are being introduced gradually and are not fully in force yet.[96] Most everyday uses of AI for businesses, such as chatbots, writing assistants or basic analytics, are subject only to transparency duties.[97] However, SMEs that build AI into their own products or services will need to meet stricter, more complex compliance obligations as AI rules continue to roll out.[98]

If you are unsure how the AI Act may apply to your business, or if you plan to integrate AI into your services, get in touch at solutions@sparklegalpolicy.eu to see how we can help you ensure AI compliance. Stay tuned for our upcoming insight on how SMEs can use tools like ChatGPT in a compliant way.

[93] European Commission (2025), COM(2025) 837 final, p.20.
[94] European Commission (2025), COM(2025) 837 final, p.56.
[95] European Commission (2025), COM(2025) 837 final, p.56.
[96] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L , 12.7.2024. Article 113. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (Accessed: 6 March 2026).
[97] Regulation (EU) 2024/1689, Article 50.
[98] Regulation (EU) 2024/1689, Article 113.

Summary of Part 4

- The Digital Omnibus will streamline several EU digital laws by merging cookie rules into the GDPR, introducing browser-level consent signals, and simplifying certain information duties for small and low-risk SMEs.
- GDPR breach notifications will shift from 72 to 96 hours, and SMEs will gain clearer grounds to reject abusive or excessive access requests.
- A single EU-wide DPIA list will replace national lists, making it easier for SMEs to understand when a DPIA is required.
- Most SMEs will not see big changes from the new EU AI rules. The stricter requirements will apply mainly to high-risk AI systems, while everyday tools like chatbots, writing assistants or simple analytics will continue to work as usual.

Get In Touch

Rue des Comédiens 22,
1000 Brussels, Belgium
www.sparklegalpolicy.eu/spark-solutions/
solutions@sparklegalpolicy.eu

+32 (0) 234 50 749

Spark
Legal and Policy Solutions Ltd

Brussels, Belgium
Publication date: 12.03.2026

Spark
Legal and Policy Solutions Ltd