

8 Steps to GDPR Compliance

GDPR compliance can be tricky.

Even if you summon the willpower to slog through the pages and pages of dry legalese, it can be tough to know where to start. Start with this checklist to quickly establish a foundation for GDPR compliance.

☐ 1. Map Your Data and Conduct a RoPA

Conduct a thorough data audit to identify the types of personal data you collect, the purposes for which you process it, and the storage duration. This audit will help you understand the data flow within your organization and identify any potential compliance gaps.

Make sure you consider the various sources from which you collect personal data as well as the different categories of personal data you process. This could, for instance, include sensitive personal data.

☐ 2. Identify Lawful Basis for Data Processing

Under the GDPR, businesses must have a valid lawful basis for processing personal data. The GDPR lists out the following as acceptable lawful bases: 1) The individual's freely given, clear, and unambiguous consent; 2) the performance of a contract; 3) compliance with a legal obligation; 4) protection of vital interests; 5) performance of a task carried out in the public interest; and 6) legitimate interests pursued by the data controller or a third party, so long as the processing does not override the data subject's rights and interests.

☐ 3. Implement Data Protection Measures

The GDPR mandates that organizations implement appropriate technical and organizational measures to ensure the security of personal data. This includes measures such as pseudonymization, encryption, access controls, regular data backups, and staff training on data protection protocols.

☐ 4. Establish Notice and Consent Mechanisms

One of the key requirements of GDPR is obtaining valid consent from individuals for processing their personal data. Businesses should review their consent mechanisms to ensure that they meet the GDPR standards. Consent must be freely given, specific, informed, and unambiguous.

When obtaining consent, it is important to inform individuals about the purposes for which their data will be processed; any third parties that may receive their data; their rights regarding data access, rectification, and erasure; and more. Consent mechanisms should also provide individuals with an easy way to withdraw their consent at any time.

☐ 5. Develop a DSAR Process

Some of the privacy rights provided by the GDPR require a response from businesses controlling or processing their data. Broadly, they're referred to as data subject access requests (DSARs). Establishing a process for the timely, efficient, and accurate fulfillment of these rights is essential.

The following are examples of the sorts of requests data subjects may make under the GDPR: 1) The right to access your data; 2) the right to have inaccurate or incomplete personal data rectified and completed; 3) the right to be forgotten and request the erasure of personal data related to them on specific grounds within 30 days; 4) the right to restrict processing; 5) the right to transfer personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller; 6) the right to object to how their information is used for marketing, sales, or non-service-related purposes; and 7) the right to not be subject to solely automated decisions.

☐ 6. Evaluate International Data Transfer Needs and Frameworks

Will your organization need to transfer data outside of the EU? If so, you'll need to comply with Chapter 5 of the GDPR, which lays out the circumstances under which international data transfers are compliant. They include:

- An adequacy decision from the European Commission, in which the Commission states that the receiving country's laws or a specific international agreement between the EU and receiving country ensure that data will be protected. The U.S.'s Data Privacy Framework is an example of the latter.
- Binding corporate rules (BCRs), which enable international organizations to transfer data internally from one country's office to another's.
- Standard contractual clauses (SCCs), which are contractual agreements between the sending and receiving organizations that ensure the individual organizations adhere to a certain standard of data protection.
- Derogations in specific situations, which include a short list of alternative bases for compliant data transfers. These are things like the data subject's consent, the performance of a contract, protecting an individual's vital interests, and so on.
- And several other niche international data transfer mechanisms.

For most organizations, the international data transfer mechanism they will most likely rely on will be an adequacy decision or SCCs.

☐ 7. Secure Required Personnel

Under the GDPR, your organization will need to keep certain experts on staff depending on the nature of your organization, its business, and its location.

Notably, you may be required to hire a Data Protection Officer (DPO). If your core activities involve processing sensitive data on a large scale, or if it involves large-scale monitoring of individuals, then you'll need a DPO.

If your business is external to the EU but you process EU citizens' data, odds are you'll be required to establish a GDPR representative to serve as your organization's liaison to EU data protection authorities. Fortunately, you don't have to open up a new European branch of your business to retain a GDPR representative; there are organizations that can provide this service for you (including Osano).

8. Review and Iterate

It can be tempting to think of data privacy compliance as a one-and-done activity, but the reality is that compliance is an ongoing process. Your organization and the way your organization processes personal data will change over time. It's essential that you:

- Keep your data map and RoPA updated.
- Ensure your legal basis for processing remains valid.
- Improve upon your data protection efforts to plug any gaps, keep up with evolving security practices, and adjust as your systems and processes change over time.
- Maintain your privacy policies and notices so that they accurately reflect the reality of your organization's data processing activities.
- Iterate upon your DSAR workflow to reduce effort, risk, and cost.
- Review international data privacy developments to ensure you can adequately protect EU citizens' data abroad.
- Maintain adequate staff and plan for associated costs.

Attending to all of these requirements at once can be exhausting, especially if you rely on manual, time-consuming processes to carry out your compliance activities.

Businesses that rely on Osano for their data mapping, consent management, DSAR workflow, and other difficult but highly automatable compliance requirements regain much-needed time to maintain their GDPR compliance status. Schedule a demo to find out how Osano can support your compliance with the GDPR and beyond.

[Schedule a Demo of Osano!](#)

About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPA, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 websites to capture consent for more than 2.5 billion monthly visitors.

Copyright © 2023 Osano, Inc., a Public Benefit Corp. Osano is a registered trademark of Osano, Inc.