DRATA

GDPR Compliance Checklist

Meeting compliance standards can pose a challenge for businesses that process user data internationally. Of all the frameworks, 90% of compliance workers agree that GDPR standards are the hardest to meet. Whether you're new to GDPR or are trying to keep up with it, meeting its requirements is non-negotiable if your business activities involve processing personal data of data subjects in the European Union (EU).

To help you achieve and maintain compliance, we put together a GDPR compliance checklist covering the requirements to process user data.

STEP 1

Review Where and How You Store Data

GDPR requires secure data storage when handling sensitive or personal data.

Action items:

□ Perform a security check on devices and other resources where you store data, including:

  □ Physical data storage centers

  □ Cloud storage solutions

  □ Company-owned computers, laptops, smartphones, tablets, and removable media

STEP 2

Account For Data Processing Risks

Data processing workflows and systems call for risk-prevention measures.

Action items:

□ Make sure all processing activities account for risk factors and include:

  □ Data protection safeguards from development to processing user data

  □ Encryption, pseudonymization, and/or anonymization mechanisms

  □ Policy requirements that build awareness about data protection

  □ Regular data protection impact assessments

  □ Instructions on how to notify authorities and data subjects after a breach

STEP 3

Examine Your Legal Function

Because GDPR consists of legal guidelines, see how its requirements square with your legal team.

Action items:

□ Make sure your legal team understands GDPR guidelines

□ Have management include your legal team during GDPR discussions and implementations

STEP 4

Consider Appointing a Data Protection Officer

DPOs work as GDPR experts for your organization and help meet compliance standards. You may also need an EU representative if your business offers service to customers in member states.

Action items:

□ Appoint a data protection officer (DPO) or delegate its tasks to a third party, member of your legal team, or IT security expert, especially if necessary

STEP 5

Appoint an EU Representative, If Applicable

If your company processes EU citizens' data, you may need an EU representative.

Action items:

□ Appoint an EU representative if you do either of the following:

- □ Process large amounts of personal data from EU citizens or residents
- □ Process special categories of data from EU citizens or residents (e.g., criminal records, political opinions, racial or ethnic origin, etc.)

STEP 6

Review or Create Your Public-Facing Privacy Policy

The GDPR requires that companies provide customers with their full privacy policy.

Action items:

- □ Publish a privacy policy on your organization's website that:
  - □ Explains how you collect, share, store, and use personal data
  - □ Breaks down the types of data collected and/or processed
  - □ Includes provisions on data subjects' rights
  - □ Communicates changes, if any
- □ Have your legal team confirm this policy meets GDPR requirements
- □ Include a link to the policy throughout your website, especially on pages where data collection occurs

STEP 7

Refine Your Terms of Service

Write or update your terms of service and to meet GDPR standards.

Action items:

- □ Evaluate your product's terms of service and be sure to:
  - □ List all the rules users must follow when using your platform/services
  - □ Communicate your obligations and set customer expectations
  - □ Note copyrighted materials, IPs, and what customers can do with them
  - □ Explain your dispute resolution process
  - □ Include payment disclaimers and liability statements
  - □ Refer to governing laws shaping your user policies

STEP 8

Develop a Customer-Facing Data Processing Agreement

Your Data Processing Agreement (DPA) outlines how controllers and processors will exchange and use personal data.

Action items:

- □ Create a customer-facing data processing agreement and:
  - □ Outline your responsibilities as either a data controller, data processor, or both, over the customer's data
  - □ Explain how your organization use these data for business purposes
  - □ Make the agreement publicly available
  - □ Involve your Legal Counsel in the creation of this document

STEP 9

Develop a Vendor-Facing Data Processing Agreement

Data controllers need to maintain a record of data processing activities.

Action items:

- □ If a third-party vendor collects and processes user data on your behalf, consider a vendor-facing DPA that:
  - □ Addresses how user data are to be protected during the engagement
  - □ Have provisions including expected cybersecurity measures to reduce the likelihood of data breaches
  - □ Received endorsement from your legal team, ensuring it covers GDPR's standards

STEP 10

Maintain Records of Processing Activities (ROPA)

GDPR guidelines require that companies give customers ways to exercise their privacy rights. Additionally, businesses need to fulfill these requests within 30 days.

Action items:

□ Keep a ROPA that includes:

- □ An overview of your data processing practices
- □ Name and contact details of your Data Protection Officer (DPO)
- □ The reason you process this data
- □ The types of data you control or process
- □ Other countries and organizations you transfer data to
- □ Time limits before you erase various types of data
- □ An overview of your security measures protecting data

STEP 11

Create Ways for Customers to Exercise Their Privacy Rights

Use automation for continuous GDPR monitoring to ensure you stay in line with regulations.

Action items:

□ Set up mechanisms for direct communication:

- □ Provide a publicly-available email address that customers can reach out to

    - □ Establish your processes for quickly responding to customers
    - □ Create a means to adjust or delete user data at any time

- □ Make your approach to user privacy clear:
    - □ Outline how automation and marketing tools leverage user data
    - □ Write web forms explaining how user data flows through your organization
    - □ Provide cookie collection notices

STEP 12

Maintain Continuous Compliance

Action items:

- □ Select an automated compliance platform that lets you:
    - □ Proactively create response plans for incidents involving data breaches
    - □ Continuously test and monitor the effectiveness of your security processes and procedures
    - □ Store documentation on data subject requests, data processing activities, privacy impact assessments, and consent records

↗ How Drata Can Help You Achieve and Maintain GDPR Compliance

While GDPR sets a high bar for data protection, meeting its standards doesn't have to be difficult.

If you have trouble staying GDPR compliant, Drata can help. Our tool automates compliance processes and keeps you audit-ready. By continuously monitoring your cybersecurity, we can help protect your users' data and reduce your business's risk. Additionally, our team of GDPR experts can reduce the time and complexity involved with achieving compliance.

Schedule a demo to see how we can help.

DRATA