Vanta

Your GDPR Compliance Checklist

What is the GDPR?

Enacted in May 2018, the General Data Protection Regulation (GDPR) is the European Union's latest data privacy and security law. The GDPR establishes data protection as a fundamental right to UK & EU based users and includes numerous protections covering the use, storage, confidentiality, and transfer of personal data. The fines for violating the GDPR are severe, maxing out at €20 million or 4% of global revenue (whichever is higher).

Vanta makes it easy to prove your GDPR compliance.

To help clarify your path towards compliance, we created this GDPR checklist. If you'd like to avoid this long and tedious process, visit **www.vanta.com** to learn more about our GDPR compliance solution.

LEARN MORE

STEP 1 Determine whether the GDPR applies to you and if so, if you are a processor or controller (or both)

- [ ] Do you sell goods or service in the EU or UK?
- [ ] Do you sell goods or services to EU businesses, consumers, or both?
- [ ] Do you have employees in the EU or UK?
- [ ] Do persons from the EU or UK visit your website?
- [ ] Do you monitor the behavior of persons within the EU?

If any of the above apply to your business, you'll need to get GDPR compliant.

STEP 2 Create a Data Map by taking the following actions

- [ ] Identify and document every system (i.e. database, application, or vendor) which stores or processes EU or UK based personally identifiable information (PII)
- [ ] Document the retention periods for PII in each system
- [ ] Determine whether you collect, store, or process "special categories" of data
  - racial or ethnic origins
  - political opinions
  - religious or philosophical beliefs
  - trade union membership
  - genetic data
  - biometric data that can uniquely identifying someone
  - health, sex life or sexual orientation data

Step 2 continued...

- [ ] Determine whether your Data Map meets the requirements for Records of Processing Activities (Art. 30).
    - the name and contact details of the controller
    - the purpose behind the processing of data
    - a description of the categories of data that will be processed
    - who will receive the data including data
    - documentation of suitable safeguards for data transfers to a third country or an international organization
    - the retention period of the different categories of data a general description of the technical and organizational security measures
- [ ] Determine whether your Data Map includes the following information about processing activities carried out by vendors on your behalf.
    - the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
    - the categories of processing carried out on behalf of each controller
    - documentation of suitable safeguards for data transfers to a third country or an international organization
    - a general description of the technical and organizational security measures

STEP 3 Determine your grounds for processing data

- [ ] For each category of data and system/application have you determined the lawful basis for processing based on one of the following conditions?
    - consent of the data subject
    - contract with the data subject
    - necessary for compliance with a legal obligation
    - necessary in order to protect the vital interests of the data subject or a third party
    - necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller
    - necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the rights of data subject

STEP 4 Take inventory of current customer and vendor contracts to confirm new GDPR-required flow-down provisions are included.

- [ ] Review all customer contracts to determine that they have appropriate contract language (i.e. Data Protection Addendums with Standard Contractual Clauses)

- [ ] Review all in-scope vendor contracts to determine that they have appropriate contract language (i.e. Data Protection Addendums with Standard Contractual Clauses)

Do your agreements cover the following items?

  - ○ vendor shall process the personal data only on documented instructions (including when making an international transfer of personal data) unless it is required to do otherwise by EU or member state law
  - ○ vendor ensures that persons authorized to process the personal data are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.
  - ○ vendor have adequate information security in place, technical and organizational measures to be met to support data subject requests or breaches
  - ○ vendor shall not appoint or disclose any personal data to any sub-processor unless required or authorized
  - ○ vendor shall delete or return all the personal data after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
  - ○ vendor makes available all information necessary to demonstrate compliance and allow for and contribute to audits, including inspections

- [ ] Have you performed a risk assessment on vendors who are processing your PII?

STEP 5 Determine if you need to do a Data Protection Impact Assessment

- [ ] Is your data processing taking into account the nature, scope, context, and purposes of the processing, likely to result in a high risk to the rights and freedoms of natural persons?

Does your processing involve any of the following?

  - ○ automated processing, including profiling, and on which decisions are based that produce legal effects
  - ○ special categories of data or data related to criminal convictions and offenses
  - ○ monitor publicly accessible area on a large scale.

If any of the above are true, you may need to conduct a Data Protection Impact Assessment for existing and new data projects.

STEP 6 Review product and service design (including your website or app) to ensure privacy notice links, marketing consents, and other requirements are integrated

- [ ] Do you have a public-facing Privacy Policy which covers the use of all your products, services and websites?
- [ ] Does the notice to the data subject include the following items?
  - the identity and the contact details of the organization and it's representative;
  - the contact details of the data protection officer, if applicable;
  - the purposes to process personal data and it's legal basis for the processing;
  - the recipients or categories of recipients of the personal data, if any;
  - the details regarding any transfer of personal data to a third country and the safeguards taken applicable
- [ ] Does the notice also include the following items?
  - the retention period, or if that is not possible, the criteria used to determine that period;
  - the existence of the data subject rights (i.e. requests for information, modification or deletion of PII)
  - the right to withdraw consent at any time;
  - the right to lodge a complaint with a supervisory authority;
  - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
  - the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the consequences
- [ ] Do you have a mechanism for persons to change or withdraw consent?

STEP 7 Update external privacy policies to comply with notification obligations (redundant?)

- [ ] Update internal privacy notices for EU employees
- [ ] Do you have an Employee Privacy Policy governing the collection and use of EU and UK employee data?
- [ ] Determine if you need to appoint a Data Protection Officer, and appoint one if needed.
- [ ] Have you determined whether or not you must designate a Data Protection Officer (DPO) based on one of the following conditions (Art. 37)?
  - the data processing is carried out by a public authority
  - the core activities of the controller or processor require regular and systematic monitoring of data subjects on a large scale

STEP 8 If you export data from the EU, consider if you need a compliance mechanism to cover the data transfer, such as model clauses.

- [ ] If you transfer, store, or process data outside the EU or UK, have you identified your legal basis for the data transfer (note: most likely covered by the Standard Contractual Clauses) 3
- [ ] Have you performed and documented a Transfer Impact Assessment (TIA)?

STEP 9 Confirm you are complying with other data subject rights (i.e. aside from notification)

- [ ] Do you have a defined process for timely response to Data Subject Access Requests (DSAR) (i.e. requests for information, modification or deletion of PII)?
- [ ] Are you able to provide the subject information in a concise, transparent, intelligible and easily accessible form, using clear and plain language?
- [ ] Do you have a process for correcting or deleting data when requested?
- [ ] Do you have an internal policy regarding a Compelled Disclosure from Law Enforcement?

STEP 10 Determine if you need to appoint an EU-based representative, and appoint one if needed

- [ ] Have you appointed an EU Representative or determined that an EU Representative is not needed based on one of the following conditions?
  - ○ data processing is occasional
  - ○ data processing is not on a large scale
  - ○ data processing doesn't include special categories or data related to criminal convictions and offenses
  - ○ doesn't risk to the rights and freedoms of data subjects
  - ○ a public authority or body

STEP 11 If operating in more than one EU state, identify a lead Data Protection Authority (DPA)

- [ ] Do you operate in more than one EU state?
- [ ] If so, have you designated the Supervisory Authority of the main establishment to act as your Lead Supervisory Authority?

STEP 12 Implement Employee Trainings to Demonstrate Compliance with GDPR Principles and Data Subject Rights

- [ ] Have you provided appropriate Security Awareness and Privacy training to your staff?

STEP 13 Update internal procedures and policies to ensure you can comply with data breach response requirements

- [ ] Have you created and implemented an Incident Response Plan which included procedures for reporting a breach to EU and UK Data Subjects as well as appropriate Data Authorities?
- [ ] Do breach reporting policies comply with all prescribed timelines and include all recipients i.e. authorities, controllers, and data subjects?

STEP 14 Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk

This includes pseudonymization/ encryption, maintaining confidentiality, restoration of access following physical/technical incidents and regular testing of measures.

- [ ] Have you implemented encryption of PII at rest and in transit?
- [ ] Have you implemented pseudonymization?
- [ ] Have you implemented appropriate physical security controls?
- [ ] Have you implemented information security policies and procedures?
- [ ] Can you access EU or UK PII data in the clear?
- [ ] Do your technical and organizational measure ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed?

STEP 15 Consider streamlining GDPR certification with automation

- [ ] Explore tools for automating security and compliance
- [ ] Transform manual data collection and observation processes into automated and continuous systyem monitoring