U.S. based callers: 1-888-376-1079
Callers from outside U.S.: +1-617-398-7067
www.verasafe.com

VeraSafe's GDPR Privacy Policy Checklist

For Compliance with Articles 13 and 14 of the General Data Protection Regulation

Introduction

This checklist is designed for companies that wish to create or update their privacy policy in accordance with the requirements of the General Data Protection Regulation of the European Union (GDPR). The checklist contains a list of items that your organization should consider including in your privacy statement to ensure compliance with Articles 13 and 14 of the GDPR.

One of the most essential obligations imposed on data controllers under the GDPR is to publish a privacy statement (also called a "privacy policy" or "privacy notice") that explains to data subjects how you will handle their personal data. This document compiles a set of specific requirements that you, as a data controller, must consider when preparing a GDPR-compliant privacy policy. In addition to the substantive items discussed below, your organization's privacy statement should be easy to read. As such, it should be written in clear and plain language. It should also be concise, transparent, and easy to access.

For specific examples, refer to the UK Information Commissioner's Office guide titled *Good and Bad Examples of Privacy Notices*:

https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf

Disclaimer

The information contained in this guide is not legal advice and any organization using this checklist may not rely upon it as such. The GDPR is a complex principle-based law which is open to interpretation, and also provides Member States an opportunity to implement higher standards than those laid down in the Regulation itself. The GDPR creates significant compliance risk for organizations regulated by the law. It is strongly recommended that organizations seek professional legal advice on how to prepare for the GDPR, including with regard to the drafting of privacy policies.

	Required Disclosure	Explanation
☐	**Your name and contact details, and, if applicable, your representative in the EU.**	The individuals whose data is processed by your organization must be able to identify and contact your organization. If you are based outside of the EU, you're likely required to appoint a representative in the EU, and disclose how to contact that representative. Contact VeraSafe if you need help appointing a representative in the EU.
☐	**Name and contact details of your data protection officer (if applicable).**	The GDPR requires some organizations to formally appoint a data protection officer (DPO). If this applies to you, include his/her name, email address, and phone number in your privacy policy. The contact details of your DPO can be used by data subjects to submit their questions or concerns about your processing of their personal data.
☐	**Categories of personal data you collect/process.**	Outline the types of personal data that your organization processes. Personal data is defined as data which relate to an identified or identifiable living individual (e.g., name, email address, street address, job title, credit card information, social security number, etc.)
☐	**The purposes for which you intend to use/process the personal data.**	You must state how the personal data you collect and otherwise process will be used. Consider identifying the purpose for each data element you process.
☐	**Your legal basis for processing.**	You must have a valid lawful basis to process personal data. For example, you may rely on the consent of the data subject, performance of a contract between you and the data subject, the legitimate interests of your business, your legal obligations, or the vital interests of the individual.
☐	**Your legitimate interests in cases where you rely on "legitimate interests" as your legal basis of processing personal data.**	If you rely on your legitimate interests or the legitimate interests of a third party as a lawful basis for processing personal data, you must identify those interests in your privacy policy.
☐	**Recipients or categories of recipients of the personal data.**	A "Recipient" is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed. This includes your vendors, contractors, business partners, etc.
☐	**Transfers of personal data to countries outside of the EEA (e.g., to your group companies or vendors) and the applicable safeguards in place to protect the data after the transfer.**	Your privacy policy must specify if the personal data will be transferred outside of the European Economic Area and what safeguards you have taken to protect the data (e.g., EU Standard Contractual Clauses, and transfers on the basis of an adequacy decision, including the Privacy Shield Framework).

☐	**Data retention policy.**	Your privacy policy must specify how long you will store the personal data, or if that is not possible, the criteria used to determine that retention period. It is important to be aware that the GDPR states that personal data must be kept "no longer than is necessary" to achieve the purposes of processing.
☐	**The existence of certain rights of the data subjects.**	Your privacy policy must inform the individuals about their rights concerning the data you process about them. This includes, among others, a right to access one's personal data, to object to the processing of one's personal data, and to rectify, erase, and export one's personal data. Some of these rights are elaborated below.
☐	**The existence of the right to refuse the data processing (if the processing is based on consent).**	If you process personal data of a data subject based on consent, the data subject must have a right to withdraw its consent. Note that it must be at least as easy to withdraw consent as to give it in the first place.
☐	**The existence of the right to object to processing (if processing is based on legitimate interests).**	If you process personal data of a data subject based on the legitimate interests of your organization or of third parties, the data subject must be able to raise an objection to such processing.
☐	**The existence of the right to object to processing of personal data for direct marketing purposes.**	If you use personal data for direct marketing, the data subjects should be allowed to object to such processing.
☐	**The existence of the right to lodge a complaint with a data protection authority.**	If a data subject cannot resolve his or her complaint with you, they have a right to bring the complaint to the relevant data protection authority, which has the power to enforce the GDPR.
☐	**The existence of automated decision-making, including profiling (if applicable), and details of such automated logic.**	If your organization carries out any processing activity which is automated and leads to decisions that produce significant impacts on individuals (mortgage applications, job applications, etc.), you must explain the logic involved in such processing operations, and the consequences of such processing. If such processing activity is wholly automated (i.e., does not involve human oversight), individuals have the right not to be subject to it.
☐	**Details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable).**	If your organization processes personal data based on a statutory or contractual requirement, you must inform your data subjects of the consequences of refusing to provide the personal data.
☐	**The source(s) of the personal data, in cases where the personal data were collected from a source other than the data subject him/herself, and whether or not the personal data came from a public source.**	You must inform individuals of the sources from which you collected their personal data if you did not collect it directly from them, as well as whether or not those sources included public sources of personal data.

☐	**Description of the security measures that are implemented to secure the personal data.**	You need to provide some general information on how the personal data will be kept secure.
☐	**Changes to the terms of the privacy policy.**	You should state how changes to your privacy policy will be communicated to the data subjects.

About VeraSafe

VeraSafe's strength lies at the intersection of law and IT. Two skillsets not traditionally found under the same roof, VeraSafe's team combines American and European data protection attorneys, privacy professionals, and IT security experts. VeraSafe is dedicated to providing industry-leading privacy and security advice that matches the budget, risk tolerance, and needs of each client we serve.

With its focus on European privacy and cybersecurity law, VeraSafe provides a complete solution for your organization's compliance with the GDPR. VeraSafe can assist you with identifying the precise extent of the GDPR's applicability to your organization and provide expert support to operationalize your complex obligations under the law.