PrivacyCheq

Technical Requirements of the GDPR

Purpose

The purpose of this white paper is to list in detail all the technological requirements mandated by the new General Data Protection Regulation (GDPR) laws with regard to providing notice and managing consent.

Providing Notice and Collecting Consent

Before collecting personal data, data collectors must provide a privacy notice that provides specific information to the data subject. It should provide information about who will process that personal data, why and for how long the data is processed, and share all options the data subject has for managing the processing of their data.

Create a Privacy Notice

Article 12 of the GDPR law says that this privacy notice should be "explicit", "specific", "informed", and "intelligible". It should be "easily accessible" and use "clear and plain language" to convey all the information required by the law in a form that holds the data subject's interest and allows them to digest the notice. According to **Articles 13 & 14** of the GDPR, some items that are required by the GDPR law in a privacy notice include:

- The legal basis on which the data was collected
- A description of what the personal data requested is used for
- Who is collecting the data
- Information on how to reach a data privacy officer of the data collector
- Any data processors the data controller hopes to use
- How long the data controller will keep the personal data, or how that period is calculated
- The request for consent should be clearly distinguishable from other matters
- If automated processing is used the notice should reveal where data subjects may lodge complains
- The source of data that is not collected directly from the data subject
- The existence of the right to be forgotten
- The right to lodge a complaint with a supervisory authority
- Whether collecting personal data is required or not
- Whether the controller intends to further process the data

There could be a case where a data controller might want to capture consent for several purposes at once. For example, they might want to get consent to collect personal data from a data subject and simultaneously get consent to transfer data outside of the European Union. **Recital 32** states "When the processing has multiple purposes, consent should be granted for all of the processing purposes." That means that data controllers are free to build several purposes of consent into a single privacy statement for the data subject to consent to.

Consent to "special category" data of an EU subject

If the data collector requires a category of personal data that is defined as being in a "special category", the privacy notice should contain language requesting the data subject's consent. According to **Article 9** of the GDPR, "The processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation shall be prohibited" except in the case where "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes".

Consent to any automated decision making

The GDPR protects data subjects from unseen data processing that could result in an automated decision making. **Article 22** reads "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

However, automated data processing is allowed in the case that the processing "is necessary for entering into, or performance of, a contract between the data subject and a data controller" or that permission is "based on the data subject's explicit consent" according to **Article 22**. If the data controller or processor relies on one of these cases, they should take extra precautions to ensure that there are appropriate controls and procedures in place to protect data subjects from unintended consequences. **Article 22** limits this data processing by saying "the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

Collect the data subject's consent

Consent must be given in an "explicit" manner that is "freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed" according to **Article 6** and the definitions section of the document. In other words, consent must be an affirmative action indicating that they are comfortable with their personal data being processed or not such as a digital

signature or checkbox. Data collectors may not rely on statements like “by using this software you agree to this policy”.

Store records of the data subject’s consent and processing activities

Data controllers must be able to prove that they have successfully collected the data subjects’ consent to process their data according to **Article 7** and **Article 30**. That requires that when data subjects give their consent to collect their personal data database records recording when the consent was given and any associated identifying information should be created. These records must contain:

- The name and contact details of the controller and any joint controller, the controller's representative and the data protection officer
- The purposes of the processing as provided to data subjects for their notice and consent
- A description of categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries
- Transfer of data to a third country or an international organization, including the identification of that third country or international organization
- The envisaged time limits for erasure of the different categories of data if available
- A general description of the technical and organizational security measures
- A record of all categories of personal data processing activities carried out on behalf of the data controller:
    - The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's or the processor’s representative, and the data protection officer, if any.
    - The categories of processing carried out on behalf of each controller
    - Transfers of data to a third country or an international organization, including the identification of that third country or international organization, where applicable
    - A general description of the technical and organizational security measures of the data processor

Since consent may be given anonymously as outlined in **Article 11**, that associated identifier might just be an anonymized identifier.

Getting consent again

If a data controller should change elements of their privacy notice or alter the purpose given for collecting personal data from data subjects, the data controller needs to get consent from data subjects who may have already given consent to a previous privacy notice. Data controllers should have an automated way to “recollect” consent for the new privacy notice while still preserving the consent to the previous privacy notice and have a way to differentiate between those two or more sets of personal data.

Data Security

Considerable thought to technical and organizational security measures are required for GDPR. **Article 32** mandates that data controllers and processors should implement appropriate technical and organizational measures, to ensure a level of security appropriate to the risk. That risk should take into account the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. These security measures should demonstrate compliance with an applicable code of conduct created in compliance with **Article 40**. Data controllers should ensure that anyone acting under the authority of the data controller will use the data for any other purpose except those mandated by the data controller.

Communication of a personal data breach

Data controllers must notify the appropriate supervisory authorities within 72 hours after becoming aware of it where feasible. That notice must contain information about the nature of the data breach, describe likely consequences of the breach, and measures taken or proposed to address the breach and limit possible adverse effects.

These breaches in personal data must be documented and remedial actions must be taken. This documentation must enable the supervisory authority to verify compliance with **Article 33**.

Article 34 stipulates that data subjects whose personal data were taken in a breach must only be notified only if the "breach is likely to result in a high risk" to the "rights and freedoms" of those people. That means that if the data controller can take steps after the fact to limit the impact on these data subjects they are freed from this requirement. **Article 34** describes ways that a data controller could prevent having to send an embarrassing message to their customers:

- If the data controller implements "appropriate technical and organizational protection measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorized to access it"
- If the data controller takes "subsequent measures which ensure that the high risk for the rights and freedoms of data subjects" is no longer likely to materialize.
- If it would involve disproportionate effort, in which case there should be a public communication instead of a private one.

Managing Consent

Data subjects "shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where such personal data are being processed, access to the data" according to **Article 15**. Data subjects should also be able to:

- Learn the purposes of the data processing
- Learn the categories of personal data concerned,
- Learn who may have received the personal data and where they are located
- Get an idea of how long that data will be stored or the method to determine how long it will be stored.
- Learn more about the existence of the right to request from the controller rectification or erasure of personal data or restriction of the processing of personal data.
- Learn more about the right to object to the processing of personal data.
- Learn more about the right to lodge a complaint with a supervisory authority.
- Learn where personal data about a data subject comes from in the case that it doesn't come directly from the data subject.
- Learn whether the data processing includes automated decision making including profiling and get meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Allow data subjects to view and update the personal data collected

Data subjects should be given the opportunity to view the personal data collected on them by a data controller. **Article 15** of the GDPR gives data subjects the right know whether their personal data is being processed. If so, those data subjects may ask where and why that data is processed as well as what categories of personal data have been captured. Furthermore, this article mandates that the "controller shall provide a copy of the personal data undergoing processing" to any data subject requesting it as well as the right to rectify any data as outlined in **Article 16**.

Accept objections to any direct marketing

Consent from a data subject may be given and withdrawn at will. **Article 18** of the GDPR gives data subjects the right to ask for processing to be restricted in the following cases:

- The personal data being processed is inaccurate.
- The processing is unlawful and the data subject prefers restriction to erasure of the personal data.
- The controller no longer needs the personal data, but they are required by the data subject for the establishment, exercise, or defense of legal claims.

The law is not specific about how a data subject's objections should be raised, so data controllers and processors should consider in their technologies and procedures how they might handle any sort of customer requests to restrict data processing.

Data portability

Data subjects should have a method of obtaining "a structured and commonly used and machine-readable" versions of their personal data in case they want to share that information with another data controller or processor. Furthermore, **Article 20** says that data subjects "have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided". The law is not specific about what constitutes a "machine-readable" format, but that could be specified in the future through a "code of conduct".

The data controller or provider should consider processes to port data while considering advocacy for industrial standards in their field. Following these trends could be a challenge for data controllers.

Right to be forgotten

Article 17 of the GDPR states "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay". This response is specifically a reaction to the data subject withdraws their consent and there is no other legal ground for processing personal data. **Article 7** points out specifically that "It shall be as easy to withdraw Consent as to give it."

Collecting Parental Consent

Data controllers need to make reasonable efforts to verify that they are not collecting any personal information from a child who is below an age where parental co-consent is required according to **Article 8** of the GDPR. A child is defined as being under a certain age as defined by specific member states, with a default age of 16 years in the main GDPR language. Furthermore, data controllers need to make reasonable efforts to verify that if they do collect consent from a parent that the individual giving the consent is in fact an adult and a "holder of parental responsibility over the child".

Article 8 is not specific about what constitutes "reasonable efforts" to achieve both of these efforts. Data controllers will have to wait for a "code of conduct" as outlined in **Article 40** to be approved by the European Data Protection Board before they have any concept of exactly how to comply with this part of the law. Even then, data controllers will need to make sure that there is a "code of conduct" created that has competency over their operations before proceeding with any technological solutions.

Compliance

Supervisory authorities as defined in **Article 51** have broad and sweeping powers over the activities of data collectors. These tasks set for the authorities are outlined in **Article 57**. Complying with the GDPR regulations will take a fair amount of technology, even if just for the bookkeeping. Not only must data controllers make data subjects' personal data transparent and editable, they must make records of the data subjects' wishes available to regulators or else face sanction.

Generating reports

The GDPR regulatory bodies require that you record the users who have given their consent. **Article 58** gives supervisory authorities broad powers to investigate how data controllers and data processors are handling personal information. Any of these failures is punishable by a significant fine.

- Failure by a Controller or Processor, or their representative, to provide information on request to a supervisory authority required for the performance of their tasks.
- Failure by a Controller or Processor to provide access to all personal data or information necessary for performance of supervisory authority tasks.
- Failure to allow access to premises, including any data processing equipment.
- Failure to comply with an order to comply with a data subject's requests re: rights under the Regulation.
- Failure to comply with an order to bring processing in to compliance in a specified manner and in a specified period.
- Failure to comply with an order to communicate a personal data breach to Data Subjects.
- Failure to comply with a prohibition on processing.
- Failure to comply with an order to rectify, restrict, or erase data and to notify 3rd parties of such actions.
- Failure of a Certifying Body to comply with an order to cease issuing certifications.
- Failure to comply with an order to cease transfers of data to 3rd countries or an international organization.

Conclusion

The GDPR requires that data controllers provide data subjects with information and options. Many if not of these mandates may be fulfilled using technology like the systems and procedures being developed by PrivacyCheq. Before deciding whether to build this infrastructure yourself, consider that ConsentCheq could both be the answer to these problems as well as a valuable resource in future compliance related technology opportunities.

Appendix: Definitions

- Data Subject -- An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- Consent – Consent is any freely given, specific, informed and unambiguous indication of a data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;
- Data Controller -- The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law.
- Data Processor – A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
- Processing Data -- Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Personal Data – Any information relating to an individual data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. This data could be anything from a name, an email address, geolocation data, or even a username or IP address.