GDPRValidatorApendix

August 9, 2022

1 GDPR General guidelines

All questions of the checklist for GDPR compliance of the general GDPR compliance guidelines:

1. **Lawful basis and transparency**. According to article 6 and recital 40, personal data should only be processed with the consent of the data subject, in this case the customers, or on another legitimate basis. Recital 58 and article 12 regulate the transparency of information. Some related questions on the checklist are the following:

   (a) ***Does the company conduct an information audit to determine what information is processed and who has access to it?***

   Report suggestion: The most effective way to demonstrate GDPR compliance is to conduct a data protection impact assessment (DPIA), article 35. Among other things, the DPIA must include the purpose of the processing, the types of data you process, who has access to it in the organization, any third parties (and their location) who have access, and how you plan to protect the data (such as encryption), and when you plan to erase it (if possible). The CSP must provide your company with all this data access information. Therefore, the CSP should prepare its DPIA to keep track of all cloud accesses. This issue can be agreed upon when signing the SLA with the CSP. Your company will need to ask the CSP for their DPIA to complete their DPIA.

   The GDPRValidator, framework allows companies to assess whether they need a Data Protection Impact Assessment [**?**] (DPIA), see Section **??**, and generates a draft of it.

   (b) ***Is there a legal justification for your data processing activities?***

   Report suggestion: The possible answers to this question relate to the legal basis for the processing defined by article 6. When the legal basis is *"consent"*, that is, the data subject (in your case, your

customer) has given consent to data access, your company has additional obligations that include offering data subjects the opportunity to revoke this consent. In the case of processing for *"legitimate interests"* pursued by the others (your company, the CSP, or by a third party), article 6. f, an assessment of privacy impacts must be conducted by your company. There are other provisions in articles 7 to 11 related to children and special categories of personal data.

(c) ***Does the company provide clear information about your data processing and legal justification in your privacy policy?***

Report suggestion:
This information should be included in your privacy policy and provided to data subjects when their data are collected. Data subjects must be informed about the data collected about them and why, according to article 12. You must report how the data is processed, who has access to it, and how it is kept safe.

2. **Data security**. Whenever personal data is processed, the company needs to follow the data protection principles outlined in article 5. Some of the questions that allow us to evaluate the security of data processing are the following:

(a) ***From the moment projects begin to develop products to each time data are processed, does the company consider data protection at all times?***

Report suggestion: The company should evaluate whether the company applies the principles of *"data protection by design and default"* defined in article 25, such as implementing *"appropriate technical and organizational measures"*.

(b) ***When a data breach occurs, does your company have a procedure for contacting the authorities and your data subjects?*** It is important to consider that, according to GDPR, a data breach that exposes personal data must be reported to the supervisory authority within 72 hours.

Report suggestion: Here, we provide a list of the EU member states' supervisory authorities. And we include in the recommendation report the following: According to article 34, you must also notify the supervisory authority and your customers immediately, within 72 hours, if there is a data breach. Unless the breach is unlikely to put them at risk, for instance, if the data stolen is encrypted.

(c) ***Whenever possible, does the company protect personal information by encryption, pseudonymization, or anonymization?***.

Report suggestion: Your company must implement cryptography or pseudonymization as often as possible under the GDPR.

(d) ***Does your company create an internal security policy for your team members and build awareness about data protection?***.

Report suggestion: The GDPR requires additional training for employees with access to personal data and non-technical employees. The provision of training courses for your company's staff is recommended.

(e) ***Has your company established a process for conducting a data protection impact assessment?*** We do not need to consider this question, because it is related to question 1.a.

3. **Accountability and governance**. Accountability for data protection refers to taking responsibility for actions and decisions regarding data protection, while governance refers to controlling and directing data protection. The two concepts are interdependent, article 5.

   (a) ***Has your company signed a data processing agreement with any third parties who process personal data on your behalf?***

   Report suggestion: For GDPR compliance, almost all services require a standard data processing agreement, which includes any third-party services that handle your data subjects' personal information. A template for this agreement is available at `https://gdpr.eu/data-processing-agreement/`, and it must be visible on your website and specify the rights and obligations of each party. It is imperative to only work with third parties who can provide adequate data protection guarantees. Thus, the SLA with the CSP must specify the list of permitted third parties.

   (b) ***Has your company appointed a Data Protection Officer (if necessary)?***

   Report suggestion: There are some circumstances in which organizations are required to have a Data Protection Officer (DPO). These conditions usually arise when a company's activity involves large-scale data processing or sensitive or special categories of data are processed, according to articles 9 and 10. A DPO should be an expert in data protection. This officer should have duties that include monitoring GDPR compliance, assessing data protection risks, advising on data protection impact assessments, and cooperating with regulators. In any case, although having a DPO is not mandatory, it is recommended.

   (c) ***Has your company appointed someone to ensure GDPR compliance?***

   Report suggestion: According to the guidelines of *"data protection by design and by default"*, article 25, GDPR compliance must be assigned to someone within the organization. Data protection policies must be evaluated and implemented by this individual.

(d) ***Does your company appoint a representative within an EU member state if it is not an EU member?***

Report suggestion: If you process data relating to individuals in a particular country, you must designate a representative there who can communicate with the data protection authority on your behalf, article 27. In cases where EU citizens are affected by processing in the multiple Member States, the GDPR does not provide guidance. In this case, it may be prudent to designate a representative in a member state that speaks your language.

4. **Privacy rights**. Following article 12, the controller shall facilitate the exercise of data subjects' rights under articles 15 to 22. A controller may not deny the customers' rights unless the controller can demonstrate that it is not in a position to identify them, article 11.

   (a) ***Can your customers easily access all the information you have about them?***

   Report suggestion: First, your organization should ensure that the client requesting the data is verified. Your customers have the right to know what personal information your company has about them, how it is used, how long it is stored, and why it is stored, article 15. You must respond to these requests within one month, article 16. This information is sent for free the first time it is requested, but subsequent copies may have a cost.

   (b) ***Do your customers have the ability to update inaccurate or incomplete information easily?***

   Report suggestion: First, your company needs to check the identity of the customer asking for the information. Make sure your company has a process that allows customers to audit their data and update their personal information if necessary, article 15. Your company must respond to these requests within one month, article 16.

   (c) ***Do your customers have the option of deleting their personal information?***

   Report suggestion: It is also necessary to verify the identity of the person making the request. Customers have the right to request the deletion of all their data held by your company, article 17, also called the right to be forgotten. You can refuse the request in certain circumstances, such as exercising freedom of speech or fulfilling a legal obligation. These requests must be answered within one month, article 16.

   (d) ***Can your customers ask you to stop processing their data easily?***

   Report suggestion: Several grounds allow your customers to restrict or stop the processing of their data, see article 18. Usually, this

happens when there is a dispute over whether the processing is lawful or accurate. However, you can still store their data while processing is restricted. The customers must be notified before you resume processing their data. Your company has to send this notification within a month.

(e) ***Do your customers have the option of receiving a copy of their data in a form that can be easily transferred to a different company?***

Report suggestion: Therefore, your organization should be able to send the customer data in a commonly readable format, either directly to them or to a third party they choose, article 20. Your customer data may be given to your competitor, which may seem unfair from a business perspective. However, from a privacy perspective, the idea is that people own their data, not you.

(f) ***Do your customers have the option to object to the processing of their data?***

Report suggestion: If your organization processes customers' data for direct marketing, it must cease doing so immediately for that purpose, article 21. On the other hand, you may be able to challenge their objection if you demonstrate "compelling legitimate grounds".

(g) ***Does your organization have procedures to protect individuals whose rights are affected by automated processes?***

Reporting suggestion: Some organizations use automated processes for decisions that affect people with legal effects or "of similar importance", article 22. If you think that applies to your organization, you need to create procedures to guarantee their rights and protect their freedoms and legitimate interests. Your company must make it easy for customers to request human intervention, evaluate decisions, and question them.

5. **Third Parties**.

(a) ***Do you have third parties requesting "consent" to access your customers' data that are not included as recipients in your contracts?*** For each of these companies, please enter the following information: company category, the purpose for access, action, duration of storage, in the case the data is copied.

Report suggestion: Your company must have the identification of those companies that wish to access your customer's data before the *"consent"* is given, as well as the purpose of the access, the action to be carried out on the data and, in the case of copying this data, the duration of storage of that copy.

All questions in the checklist for GDPR compliance of the cloud-related GDPR compliance guidelines:

1. **Contracts**.

   (a) ***Has your company signed an SLA with the CSP to be responsible for the treatment of personal data on your behalf?***

   Report suggestion: Your company must sign an SLA with the CSP responsible for processing your customers' data, acting as the *joint controller*, article 26. The SLA should identify the responsibilities of the SME and the CSP, as *controller* and *joint controller*, in a transparent manner. Specifically, concerning the exercise of rights of the interested party (customers) and their respective responsibilities to provide the information referred to in articles 13 and 14, the agreement may designate a point of contact for these interested parties. It is important to keep contracts updated.

   Furthermore, your company needs to ensure that the hired CSP must declare adherence to the EU Cloud Code of Conduct (EU Cloud COC) [**?**] about its cloud service, article 40. It provides cloud-specific approaches and recommendations, including a road map that tracks code requirements to GDPR and international standards such as ISO 27001 [**?**] and 27018 [**?**][1]. In addition, the CSP and the competent supervisory authority must certify that the cloud service fully complies with the provisions in the code.

   (b) ***Has the CSP signed an SLA for data processing with any third parties who access/process personal data?***

   Report suggestion: For GDPR compliance, almost all services require a standard data processing agreement, which includes any third party services that handle your data subjects' personal information. It is imperative to only work with third parties who can provide adequate data protection guarantees. This suggestion complements the one in the point **??** of the checklist related to *Accountability and governance* in the general GDPR compliance guidelines.

2. **Duration**.

   (a) ***Does your company establish a date for data retention?***

   Report suggestion: The storage of data should not exceed the necessary storage time. The SLA signed with the CSP must specify the processing duration. After the retention period has expired, all data, including copies, must be deleted.

3. **Information**.

[1]The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) sets out the requirements for an information security management system (ISMS) by the definition of the standard ISO/IEC 27001. To ensure the protection of "personally identifiable information" processed by cloud service providers, ISO/EIC published ISO/IEC 27018 (ISO 27018) in 2014.

(a) ***Does your company specify a procedure to notify when a breach is detected?***

Report suggestion: GDPR in the article 4 determines what is considered a breach in the collection, retention, and processing of data: *"the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"*. Then, the company must specify the procedure that it follows to notify when a breach is detected, for instance, in the event of theft or a leak. Before a breach is reported in the media, the CSP should inform your company, and your company should notify its customers and supervisory authorities. According to article 36, the *controller* must report any breach of personal data to the supervisory authority competent under article 55 within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. This suggestion complements the related one in point **??** in *Data security* in the general GDPR compliance guidelines.

(b) ***Does the CSP explicitly inform your company where each customer's data is stored?***

Report suggestion: All data of European citizens should either be stored in the EU, so that they are subject to European privacy law, or in a place where the same level of protection is guaranteed. Your company is responsible for arranging with the CSP the location for storing the customers' data. The SLA, signed between the CSP and the company, should include this information.

4. **Privacy rights**. Some of these questions are related to the ones shown in the general GDPR compliance guidelines (Privacy rights 6) but applied in the cloud context.

(a) ***Can your company access and delete the customers' data from the cloud?***

Report suggestion: Your company has the right to access its customers' data and have them deleted, the right to access (article 15), and the right to erasure ("to be forgotten", article 17). The CSP must facilitate this process by making the data available to your company and your customers in a structured format. It is also important to consider data backups when deleting customer data.

(b) ***Does your company retain ownership and control of your customers' data at all times?***

Report suggestion: As *controller*, your company must retain ownership and control of your customers' data at all times. To ensure that your company retains ownership and control of your customers' data at all times, the corresponding SLA should include this condition.

(c) ***Does your company have information about the metadata that the CSP collects?***

Reporting suggestion: Your company should ask the CSP what metadata it collects and whether your company has a right to opt out. The CSP must guarantee that it will inform your company about this metadata, so this condition should also be included in the contract.

5. **Data Protection Impact Assessment (DPIA)**.

(a) ***Does the CSP have a Protection Impact Assessment (DPIA) that determines the risks associated with cloud hosting or services?***

Report suggestion: The CSP, as a *joint data controller*, should also have a DPIA (see Section **??**) that determines the risks associated with cloud hosting or services. It is recommendable, but not mandatory. The CSP must send this DPIA to your company every time that it is updated. This suggestion complements the related one in point **??**, under *Lawful basis and transparency* in the general GDPR compliance guidelines.

6. **Third Parties**.

(a) ***Do you have third parties in the cloud requesting "consent" to access your customers' data that are not included as recipients in your contracts?*** For each of these companies, please enter the following information: company category, the purpose for access, action, and duration of storage, in the case of the data being copied.

Report suggestion: Your company must have the identification of those companies that wish to access your customer's data before the *"consent"* is given, as well as the purpose of the access, the action to be carried out on the data and in case of copying this data, the duration of storage of that copy.