PrivacyBoard

Data Protection Audit Report

For **Plausible**

22 March 2022

Table of Contents

1. Overview

Requirement	Rating
Designated DPO or GDPR correspondent	Compliant
Privacy Policy	Compliant
Country & Type of Data storage	Compliant
Data transfers outside the EU	Compliant
Legal tools for Subcontractors	Compliant
Data Breach Notification	Compliant
Right Requests Process	Compliant
Data Privacy Impact Assessment	Compliant
Employee Trainings	Compliant
Security Policy	Not Compliant
Organizational and Technical Security Measures	Compliant
Data Encryption	Compliant
Restriction of access	Compliant
Reuse of data	Compliant
Exemption of cookie consent	Compliant
Submission to Cloud Act/FISA	Compliant

2. Finding & Recommendations

2.1. Designated DPO or GDPR correspondent

Description	According to Article 37 of the GDPR, a Data Protection Officer (DPO) must be designated to a Supervisory Authority when: - your business core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or - your business core activities consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offenses referred to in Article 10. Apart from cases of mandatory designation, the appointment of a DPO or GDPR correspondent is highly encouraged. It allows to entrust an expert with the identification and coordination of actions to be taken in the data protection field. According to Articles 13 and 14 of the GDPR, apart from being communicated to the Supervisory Authority, the DPO contact details must also be within reach of data subjects and third parties (whether controllers or subprocessors) to facilitate and centralize any demand on privacy matters.
Rating	**Partially Compliant**
Findings	Plausible doesn't mention having a DPO or GDPR correspondent but has a privacy dedicated email contact available on its website: privacy@plausible.io
Recommendation n°1	Confirm us or make public that you have a skilled privacy correspondent in your team to facilitate and centralize any demand on privacy matters coming from data subjects or third parties you're contracting with (whether they be controllers or subprocessors).

2.2. Privacy Policy

Description	A Privacy policy is an official document in which you need to sum up the goals and commitments you've settled in terms of privacy and data protection regarding your clients', employees' or customers' personal data. This document is to be published on your website and tool for everyone to see and read, your data subjects, third parties as well as supervisory authorities. Articles 13 and 14 of the GDPR oblige controllers to give transparent information to data subjects relating to the processing activity and how to exercise their rights. If this obligation relies on controllers towards data subjects, processors have to make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28. When writing a “website privacy policy”, you’re addressing data subjects about how you’re processing personal data on your website for commercial and marketing purposes. When writing a “cloud privacy policy”, you’re addressing controllers and data subjects about how you’re processing personal data through your SaaS tool. It must at least contain: your identity, contact details of the DPO, purposes and legal basis of the processing activities, the categories of recipients, intended transfers to a third country and legal safeguards on which they are based, data retention period, data subjects’ rights, and the existence of automated decision-making.
Rating	Compliant
Findings	Regarding cloud: https://plausible.io/data-policy Regarding website: https://plausible.io/privacy

2.3. Country and type of data storage

Description	Data storage can be of two types: - on a controller's premises ; - in a third party's cloud (whether it is a processor or subprocessor). Concerning storage on premises, the editor of the tool has little responsibility towards personal data, except when conducting maintenance and IT support and accessing data in clear. In such cases, employees accessing data must be submitted to NDAs. Concerning cloud storage, the editor of the tool becomes a processor and bears much more responsibility towards personal data and how it's handled, especially when choosing where and by whom personal data will be hosted. At this point, several verifications must be undertaken by the processor and communicated to the controller: - in which country data is transferred ; - what is the nationality of the servers provider ; - national legislations applicable and if they ensure sufficient data protection.
Rating	Compliant
Findings	<u>Company Headquarters:</u> Estonia (EU) <u>Storage Facilities:</u> All analytics data is processed by German cloud provider Hetzner, in Germany. Possibility to host Plausible Analytics on controller premises.

2.4. Data transfers outside the European Union

Description	Location where data is stored is a paramount criteria for controllers. If servers hosting data are located in the European Union or in an adequate country, data transfers can be operated without additional safeguards as these countries' legislations are protective enough of personal data and individuals' rights. If servers hosting data are not located in the European Union, nor in an adequate country, appropriate legal safeguards compliant with Article 46 of the GDPR must be put in place. Most used legal safeguards regarding SaaS tools are Standard Contractual Clauses for data transfers. SCCs are templates considered adequate by the European Commission which can be incorporated into any transfer contract. However, following the decision of the EU Court of Justice known as "Schrems II", data transfers towards certain countries like the US now require complementary measures. For instance: - Technical complementary measures: encryption, pseudonymisation, anonymization, etc. - Contractual complementary measures: additional clauses, revision of existing contract, etc. - Organizational complementary measures: team awareness, internal documentation, etc.
Rating	Compliant
Findings	Plausible doesn't transfer analytics data outside the EU.

2.5. Legal tools for subcontractors

Description	According to Article 28 of the GDPR, as a processor, you may only hire another subcontractor after obtaining written authorization from your client. This authorization may be: - specific, which means granted for a particular subcontractor, or - general, which means you will have to inform controllers for every subcontractor you would like to add or change, and allow controllers to object. The subcontractor you hire needs to be subject to the same obligations as those present in the Data Protection Agreement or any other contract you have with controllers. In particular, contracts with subcontractors must present sufficient guarantees as to the implementation of appropriate technical and organizational measures to ensure the processing activity complies with the European Regulation. You can also make your subcontractors list public for more transparency.
Rating	Compliant
Findings	For every subcontractor, Plausible assesses its commitment to privacy and signs a DPA including controller-processor Standard Contractual Clauses. Plausible has made public its list of subprocessors: https://plausible.io/privacy

2.6. Data breach notification

Description	A personal data breach is a breach of security resulting in the destruction, loss, alteration or unauthorized disclosure of personal data. According to Article 33 of the GDPR, as a processor, you must notify controllers of any personal data breach as soon as possible after becoming aware of it and offer your assistance to assess the impacts on data subjects' lives. On the basis of this notification, controllers will have to notify the data breach to the competent supervisory authority under the conditions of Article 33 of the GDPR and communicate to data subjects such a breach under the conditions of Article 34 of the GDPR.
Rating	Compliant
Findings	In case of data breach, Plausible will notify the controller without undue delay by email (not later than 48 hours after having become aware of it) and provide a description of the incident as well as periodic updates about the incident, including its impact.

2.7. Rights requests process

Description	Data subjects have rights upon their personal data: right of access (Article 15), of rectification (Article 16), of erasure (Article 17) and objection (Article 21), right to the restriction of processing (Article 18), right to data portability (Article 20), right not to be subject to an automated individual decision (Article 22). According to Article 28 of the GDPR, to the extent possible, the processor must assist the controller in fulfilling its obligation to answer within one month requests of data

	subjects exercising their rights.
Rating	Compliant
Findings	Data requests will be forwarded to the controller without delay.

2.8. Data privacy impact assessment

Description	A Data Privacy Impact Assessment must be carried out by a controller when certain conditions are met and in compliance with Article 35 of the GDPR. It provides the assurance that privacy is adequately addressed, that risky processings are acknowledged and that the controller knows how to mitigate those risks for data subjects. According to Article 28 of the GDPR, as a processor, you must assist controllers in conducting this assessment and provide them all necessary information. This assistance must be included in your contract with controllers.
Rating	Compliant
Findings	Plausible will provide assistance to the controller for DPIAs.

2.9. Employee trainings on GDPR

Description	According to Article 28 of the GDPR, the processor must ensure that persons authorized to process personal data under the contract with controllers: - have signed NDAs or are subject to an appropriate statutory obligation of confidentiality ; - receive the necessary training on data protection

Rating	Compliant
Findings	Employees required to access analytics data are informed of the confidential nature of the data and comply with the GDPR obligations set out in the DPA.

2.10. Security policy

Description	A security policy is a formalized set of strategic elements, guidelines procedures, codes of conduct, organizational and technical rules, with the objective of protecting the business' information system(s). As a security policy often contains sensitive information about the business, it can therefore not be made publicly available (on your website for example). However, when contracting with a processor, a controller must ask for its Information security policy.
Rating	Not Compliant
Findings	Plausible doesn't mention having a security policy.
Recommendation n°2	Based on ISO 27001 standards, your Security policy should contain at least the following chapters on how you handle: - employee awareness raising on security - user authentication - authorization management - access tracking and incident management - workstation securing - mobile computing securing - protection of internal computer network - server securing - website securing - business continuity planning - archive securing - maintenance and data destruction

	- subcontractor management - secured exchanges with third parties - physical security - IT development supervision - data encryption

2.11. Organizational and technical security measures

Description	According to the Article 32 of the GDPR, the processor has to implement and document appropriate technical and organizational measures to ensure a level of security appropriate to the risk entailed by the processing activity, in particular: - pseudonymisation and encryption of personal data; - ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; - ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; - a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
Rating	Compliant
Findings	Server security: Cloud security relying on Hetzner. Other measures: Data anonymization, data pseudonymisation (hash), DDoS protection, back ups in a redundant site.

2.12. Data encryption

Description	Encrypting an asset ensures that only the sender and the legitimate recipients (those in possession of the key of encryption) can access its content. It guarantees data confidentiality. Data can be encrypted at rest and in transit with the utmost modern technologies: TLS, SFTP, HTTPS, etc.
Rating	Compliant
Findings	Data is encrypted in transit (HTTPS) and at rest.

2.13. Restriction of access to data

Description	Data must be accessed on a need to know principle. The processor has to write down processes and cases in which its employees might access personal data when necessary and to the extent the contract with controllers allows. Ideally, the processor should gather agreement of the controller before accessing any personal data, or at least inform the controller before accessing it. For e.g.: maintenance, IT support, etc.
Rating	Compliant
Findings	Plausible allows external access or processing of personal data to employees submitted to confidentiality clauses for IT support and maintenance.

2.14. Reuse of data

Description	A processor must always act under instructions of the controller. Contract with the controller should also contain the engagement by the processor that it will not reuse personal data generated by the use of the SaaS, whether they be to process it for its own benefit or to sell it to third parties.
Rating	Compliant
Findings	Plausible doesn't reuse analytics data or share it with third-parties.

2.15. Exemption of cookie

Description	A cookie is a small text file that may be deposited and saved on the hard drive of a device when visiting a website. It allows the controller to identify the device on which it has been saved and to keep record of certain information relating to the visitor's journey.. SaaS like analytics tools can function upon cookie technology or not. When they do, the visitor's consent must be collected and documented, pursuant to Article 7 of the GDPR. Under French law (Article 82 of "loi Informatique et Libertés"), when using an analytics tool on its website, a controller is exempted from collecting its visitors' consent if: - cookies only serve to the sole measurement of the website's audience - cookies only produce anonymized statistics
Rating	Compliant
Findings	Plausible doesn't collect cookies.

2.16. Submission to Cloud Act/FISA

Description	Foreign Intelligence Surveillance Act (FISA) and Cloud Act are U.S legislations obliging American cloud providers to provide upon request to U.S intelligence agencies and courts individuals' data that they store, control and manage in the United States or even remotely. These transfers, that are conducted without individuals' consent and controllers being informed, are considered an invasion of data subjects' privacy as they can't oppose them. When dealing with cloud providers situated in the US, the European Court of Justice has ruled necessary for business owners to put in place complementary security measures to protect personal data (like anonymization or encryption). To counteract these legislations personal data can also be stored in the European Union (or in an adequate country) by a cloud provider which is not American.
Rating	Compliant
Findings	NO, data is stored in the EU by an European cloud provider.

3. Audit Resolution

3.1. Recommendation n°1

Recommendation	Confirm us or make public on your website that you have a skilled privacy correspondent in your team to facilitate and centralize any demand on privacy matters coming from data subjects or third parties you're contracting with (whether they be controllers or subprocessors).
Resolution	Privacy questions and matters are addressed by Plausible co-founder Marko Saric in collaboration with its legal team.
Rating update	Compliant

3.2. Recommendation n°2

Recommendation	Based on ISO 27001 standards, your Security policy should contain at least the following chapters on how you handle: - employee awareness raising on security - user authentication - authorization management - access tracking and incident management - workstation securing - mobile computing securing - protection of internal computer network - server securing - website securing - business continuity planning - archive securing - maintenance and data destruction - subcontractor management - secured exchanges with third parties - physical security

	- IT development supervision - data encryption
Resolution	
Rating update	

PrivacyBoard