GDPR & Data-Handling
2022-01-01

Parlametric AB
Org. 559112-4556
Grönegatan 4B
222 24 LUND
SWEDEN

Summary

Parlametric's Privacy Policy reflects the company's commitment to protect the privacy and personal integrity of social media user, panelists, employees, customers, and other respondents that have, actively or inactively, provided information to Parlametric. Parlametric's business model is based on aggregate statistical data, and not individual nor personal data. Thus, we refrain from collecting individual data, will never store it for longer than necessary (see section 4.1), and we will never collect any sensitive individual data (see section 3). In this P+policy we use the term *user* to include any individual who either uses Parlametric's services or whose data Parlametric has collected.

1. Policy application. This policy applies to Parlametric's, and any of Parlametric's subsidiaries, surveys, services, applications, platforms, and softwares, including parlametric.com, parlametric.se, parlametric.io, 5urvey.com, stage.5urvey.com, parla.live (Websites), Elli (Softwares), and Speakin (Hardwares), Propel, Flare, Salmon, Needle, and ParlaMarket (Services). Should any of the above refer or link to a superior privacy policy provided by Parlametric, then that policy, and not this policy, applies for that specific project.

Parlametric's business agreements with partners and clients may contain provisions about the collection, usage, storage, and disposal about the collected information (both from digital and offline sources). If a provision of a client agreement conflicts with or is otherwise inconsistent with the provision outlined in this policy, then the provision of the client agreement prevails, but only to resolve the conflict or inconsistency.

2. Information Parlametric collects

2.1 Social media & online forums. Parlametric offer market research services to understand peoples' reaction to commercials, products, brands and other relevant information reflected in social media posts. Parlametric will always collect social media data in compliance with the privacy, personal integrity- and data handling policies of the social media companies the data is collected from. Parlametric has valid API agreements with all social media companies we collect data from.

2.2 Surveys. Parlametric provide surveys, either through panel platform companies, using Parlametric's own panels, or via clients' own registers. In some cases, Parlametric will collect data using 5urvey.com, and in other cases the data will be provided to Parlametric by the client. In terms or panel platform providers, Parlametric has valid agreements with every provider we use.

2.3 Customer or employee interactions. Parlametric provides analysis of e-mail, telephone, or chat interactions, such as customer service, technical support, onboarding, or sales activities. Depending on the use case, data transaction between Parlametric and the client can either be provided real-time or in pre-defined intervals.

2.3.1 E-mail. E-mails can either be forwarded to Parlametric, or the account can be connected via POP3 or IMAP. Individual e-mails or files containing e-mails (e.g. Excel or CSV) can be sent to Parlametric or uploaded to a mutual storage, or Parlametric can pull files from FTP or similar server.

2.3.2 Chat. Chat logs / interactions can be sent to Parlametric via API, which depends on the client's specific chat system. Files (e.g. Excel or CSV) containing chat logs can be sent to Parlametric or uploaded to a mutual storage, or Parlametric can pull files from FTP or similar server.

2.3.3 Telephone. Recordings can be pushed or pulled via FTP, or Parlametric can have access to the storage and download recordings as they come in. Parlametric's technology is compatible with all major sound files (e.g. MP3, MP4, WAV etc). Recordings can either be sent to Parlametric, uploaded to a mutual storage, or exchanged via FTP or similar.

3. GDPR and anonymization

All Parlametric Websites, Softwares, Hardwares and Services comply with current GDPR regulations. Personal names, numbers (e.g. telephone or social security), addresses (e-mail and physical) are filtered out during data pre-processing. Non-commercial sensitive information such as sexual orientation, religious beliefs and political views will not be analyzed. Upon request, stricter filters can be applied (e.g. discarding health-or union information).

3.1 Sending data to partners. To protect the users and ensure that sufficient GDPR and privacy regulations is upheld, Parlametric usually refrain from sending raw or aggregate data to partners. Should such a transaction be necessary, a data transfer agreement between Parlametric and the receiving party needs to be in place. In such an agreement, the receiving party guarantees to uphold sufficient GDPR and privacy protocols.

3.2 Sending data to third parties. Parlametric will never send data to a third party unless all parties within a project has a mutual data-handling agreement in place. In such as case, it is up to the receiving party to fulfill a privacy policy and adhere to the current GDPR regulations.

3.3 Encrypted respondent register. Respondents from Parlametric's own panels can ask to have their user deleted from the panel registry. These are stored locally in an encrypted database and can only be accessed by Parlametric's CTO. For third party panels, their policies for respondent registry applies.

4. Storage and encryption

Reliability is a core value at Parlametric, pertaining both to the quality and accuracy of the data analysis, and to ensure that our clients' data is kept safe and secure throughout the collaboration.

4.1 Storage time. In accordance with current GDPR regulations, raw data is stored for three months, and aggregate data is stored for 12 months, afterwards these are discarded.

4.2 Encryption. All data (incl. inbound and outbound traffic data, to and from cloud services) is encrypted via TLS (HTTPS). Our encryption protocols are continuously reviewed and updated to ensure the newest and safest protocols.

4.3 Data residency. All servers are located in EU countries and are maximally isolated to reduce the risk of potential undesired events. Upon special request, we can designate hosting to a specific region.

4.4 Authentication and authorization. We ensure that only authorized Parlametric staff is granted access to specific data by requesting two-factor authentication and using multiple authentication- and access control protocols. Each access is logged.

4.5 Security & monitoring. All systems are monitored 24/7 and any and all suspicious activity is reported and traced. Parlametric applies a high level of security using firewalls and TLS.

4.6 Backup. All services, storage and databases are continuously backed up using high quality, secure and robust backup and recovery solutions. This minimizes downtime and maximizes availability, even during undesired events, and ensures that our clients' data maintains safe and intact.

Thomas Strandberg, CEO