Flikarus

Flikarus GDPR Compliance and Confidentiality Procedures Explanation

V1.1, June 2018

First Published, 2018

Flikarus
Słonecznikowa 26
Dębogórze, 81-198
Poland
www.flikarus.com

AGENDA:

This document outlines the manner in which Flikarus complies with the GDPR requirements and how it protects confidentiality of project materials.

Individual projects may entail additional levels of data protection.

All of these procedures are subject to change; if you wish to be kept informed of changes, email flizik@flikarus.com.

Individual responsible

- Agnieszka Flizik is the designated Flikarus representative responsible for creation of procedures for and adherence to data protection procedures.

General data protection and confidentiality rules

- All project materials and data, including personal data from respondents, are stored in a secured location, accessible only to Flikarus. That location is the Flikarus place of business, which is locked when Flikarus staff are not present.
- The data can also be stored on laptop computers, which can be taken outside of the secured location.
  - Access to the laptop is "locked" with a password, and access to individual project folders has an additional security lock. The laptop is never left unattended when it is active and unlocked.
  - No one aside from Flikarus staff has access to, or passwords to, files on the Flikarus computer(s).
- Study materials and respondent data can be stored on a separate, secured hard drive (to counter risk of data loss). The hard drive is kept exclusively in the Flikarus place of business.
- Flikarus may occasionally print out hard copies of project materials (not personal data of respondents). Those materials are generally kept in the Flikarus place of business.
  - When travel is necessary, and the printed materials need to be carried, Flikarus keeps the printed materials with the traveling individual (e.g., not in checked luggage, or unsupervised in a public location).
- For research projects for which the final project data are the property of an entity other than Flikarus (a "client"), which generally means that Flikarus has been subcontracted to help with part or all of a project, Flikarus does not serve as a "representative" or "controller" (as defined in the GDPR) and does not have the responsibility for ensuring all other entities are compliant with GDPR rules. In such situations, Flikarus is only responsible for ensuring its own adherence to GDPR rules, as outlined here.
- Flikarus only serves as a "representative" (as the term is defined in the GDPR regulations) when this responsibility is explicitly included in its Statement of Work, Master Service Agreement, or other legally-binding document outlining its terms of work with a client.
  - Since Flikarus is not a "representative" on research projects executed by clients, it would not be the point of contact for any respondents wishing to delete, amend, or get access to their data (the client remains responsible, for example, for activities described in Section 3, Articles 16-20). Flikarus has no responsibilities for such activities other than to follow the directives of the client to remove data of respondents when requested, in which case Flikarus reserves the right to delete the entire data file for the project within three business days of the request.
- Flikarus does not share study materials or respondent data with any person or entity without explicit permission from a client, and always in accordance with data protection procedures outlined in this document.
- Flikarus is legally liable for data breaches only when it is definitely demonstrated that it was directly and solely responsible for the breach. Breaches that were due, or also due, to the procedures, behaviors, or negligence of clients or other parties; or that occurred before or after Flikarus became involved in a project; or that occurred for reasons or due to circumstances other than those directly and solely attributable to Flikarus, are the responsibility of the client or the other parties.
- When Flikarus works with clients that have their own confidentiality / data protection procedures, when those procedures are shared with Flikarus, and exceed the stringency of the Flikarus procedures, Flikarus always follows the more stringent set of procedures for the project for which it has been engaged unless explicitly requested to do otherwise by the client, in which case all legal liability for potential data breaches falls to the client.

Respondent data protection: Primary data

- "Primary data" consist of information provided directly by respondents after those respondents have provided informed consent for participation in research.
- For the primary data Flikarus collects directly (meaning it recruits the respondents and collects their informed consent and then collects their responses), Flikarus ensures that:
  - Respondents provide affirmative consent to participate in the research after being given information outlined in Section 2, Article 13 of GDPR.
  - The terms of participation in the research leading to the informed consent are explained in easy-to-understand language.
  - The data are either anonymous upon collection or become pseudoanonymised as soon as practicable after collection.
  - Data are shared back with the client in the pseudoanonymised format. The de-anonymization key is then deleted, making attributing answers to individual respondents difficult or impossible per GDPR rules.
  - If Flikarus has no client on a primary data collection project, then it follows the anonymisation procedure above; since the process ensures that the data become difficult or impossible to match to individual respondents, data stop being "personal data" OR making them personally identifiable again becomes excessively difficult, as defined by GDPR.
- For primary data Flikarus does not collect directly, Flikarus ensures that:
  - The data it receives are in an anonymous or pseudoanonymised format, and Flikarus does not have access to the de-anonymization key.
- Flikarus reserves the right to delete primary data files from its servers immediately after completion of research upon obtaining written agreement from the client OR six months after completion of the work. "Completion" is defined as the delivery of the first version of the final report to the client OR the day on which the final invoice for the work has been delivered to the client, whichever comes earlier.

Respondent data protection: Secondary data

- "Secondary data" consist of information collected from existing data sources; in the context of Flikarus secondary research those data have generally been shared by individuals on public platforms (E.g., drugs.com).
- For the secondary data Flikarus collects directly (meaning it is the Flikarus staff that collect the data from the public platforms), Flikarus ensures that:
  - The platform from which the data are collected is a public one, meaning that the data are meant for public consumption or are understood to be accessible by the public for consumption, making them no longer "private" data.
  - The data are stored without usernames, emails, or other such personally-identifying information.
  - All direct quotes are slightly reworded or amended in any reports or data summaries, making it difficult or impossible (as defined in GDPR regulation) to attribute single responses to specific individuals.

In addition to any client rules, or in case the client does not specify such rules, Flikarus ensures that in its consulting work:

- It minimizes the amount of respondent data it collects, receives, or retains.
- Any and all data obtained from study respondents are stored in an anonymized fashion (as outlined previously).
- Transfer of any non-anonymized data is done using a secured transfer service.
- In live, in-person interview situations in which Flikarus has a backroom presence, Flikarus ensures that the backroom attendees are authorized to be present and are aware of GDPR procedures for data protection.

Email protection

- Flikarus domain emails (directed to addresses ending in "@flikarus.com") are hosted on secured servers that do not scan email content, e.g., for marketing purposes.
- Emails relating to specific projects can be deleted from the servers, if requested by the client.
- On its discretion, and unless otherwise specified by a Master Service Agreement, Flikarus reserves the right to delete all emails relating to a project after the project has been completed for six months ("completion" defined previously).
- Flikarus does use vendor email account(s) or other electronic communication system(s) when required by clients for individual projects; email protection in those cases may be different from the above.

In case Flikarus suspects that the security of confidential project materials or private data from respondents have been breached…

- Flikarus will notify the client regarding the possible breach within 24 hours of suspecting it had occurred.
- Flikarus will immediately investigate to confirm the presence of and the extent of the breach; the duration of the investigation may depend on the nature and extent of the breach.
- At the conclusion of the investigation into the breach, Flikarus will specify to the client, to the extent uncovered through the investigation, which materials or which private data have been breached.
- Since Flikarus generally does not serve as a "representative" (as the term is defined in the GDPR regulations), it does not have any direct responsibility for notifying natural persons of any data breaches for projects on which it is not a "representative".

Data about clients

- In the normal course of business, Flikarus may need to store and process personal data about individual clients (e.g., names, physical addresses, email addresses) for purposes such as business communications, to issue invoices, for professional record-keeping, and other reasons.
- The data are stored and processed on the Flikarus-accessible laptop and on a separate secured hard-drive, as covered previously.
- The data are stored and processed for an indefinite period of time.
- Clients may request to have their personal data removed, but that may significantly impair the ability by Flikarus to conduct business with the client or the client company. To request to have personal data removed by Flikarus, please contact flizik@flikarus.com .

Policy changes

- Flikarus may from time to time alter the terms of this policy. If you wish to be kept informed about any changed, please let Flikarus know by emailing flizik@flikarus.com .