sermo

GDPR compliance in connection with market research services at Sermo

Table of Contents

The recent implementation of GDPR had a great impact on the market research field, so we have prepared this informational document to share our thought process around the new regulations. Please note that we analyze each project on a case by case basis to provide our clients with the best possible service.

1. Background

What is GDPR?

GDPR stands for **General Data Protection Regulation**. This is a new regulation from the European Commission that came into effect in May 2018. GDPR sets new and individual-focused standards of lawfulness, fairness and transparency for the collection, use, processing, and transfer of the personally identifiable information (PII) of European Union citizens. GDPR's goal is to control how personal data is being used by organizations and make sure organizations are kept accountable for data protection.

Is GDPR consistent across all EU countries?

There are a few exemptions that allow countries some discretion. In the context of market research, Article 9, which concerns processing of special data categories as data concerning health, allows states to exempt GDPR guidelines by local laws.

In connection with the UK Brexit, for as long as the UK is part of the EU, GDPR will apply. Once the UK leaves the EU there will be some changes made to GDPR at the UK legislator's discretion. As of today, there is a proposed bill that is making its way through both houses for approval and is very similar to the requirements of GDPR.

Does GDPR apply to anonymized data?

If the data collected and transferred to a client is anonymized, GDPR will not apply. Therefore, when Sermo as the controller provides the sample, conducts the fieldwork, and provides anonymized data – GDPR regulations will not apply.

What is personal data?

GDPR expends the definition of personal data and includes any information that is related to a person or can identify or link to a person. We advise our clients to think through the process before starting the project and tightly define what personal information is being dealt with as part of the project.

Examples of personal data:

- Name, contact information, email address
- Mailing address
- IP address
- Photo
- Audio and video recordings
- Online behavior such as cookies, posts on social networks, etc.

The data controller and the data processor

GDPR applies different obligations on the data controller and the data processor. Therefore, it is important to determine each party's role prior to the beginning of the project.

- The data controller is the entity that determines the purposes, conditions, and means of personal information obtained from data subjects. Therefore, in the context of market research the owner of the panel and the sample is the controller of the information.

- The data processor is the entity that processes the personal data on behalf of the controlling entity. In situations in which organizations are jointly determining the purposes and means of processing of the data, both parties will be joint data controllers.

2. How does Sermo ensure GDPR compliance ?

Sermo has taken the following steps to ensure we are in compliance:

- We have invested in both internal and external legal advice to ensure compliance in our business and implemented the recommendations accordingly.
- We have updated our privacy policy.
- The legal basis that allows us to use, process, and transfer data is the consent we obtain from our users. We have obtained consent from our members to continue using their personal data and explained the purpose for using it. The requested consent is provided in easy and simple language and allows our members to opt out if they no longer want us to use their personal data. We also have a legitimate interest as a legal basis to process the personal data since our members have an active relationship with Sermo and are actively provided with our services.
- We appointed our CFO as our Data Protection Officer: Gerard Smith (gerard.smith@sermo.com).
- We have prepared updated vendor contracts with standard GDPR clauses. We are also using NDAs and Data Processing Agreements with third parties who are processing information on our behalf to ensure they are only processing the information in accordance with our instructions as well as erasing the information at project closure.
- We have addressed our ability to provide users with access to their personal data and their right to be forgotten. We currently support any request to modify or delete personal data from our servers and have published an internal policy to ensure compliance by our teams.
- We have addressed data protection by design.

- We have addressed the issue of transfer data outside of the EU and we are allowing clients who request to keep the data inside the EU the technical ability to do so.
- We have employed a third-party external network security auditor to ensure our systems security (certification available upon request).
- We have secured information with a next-generation Palo Alto firewall.
- We have shredded all storage media once retired (third party certificates available upon request).
- We have published a full suite of information security policies, including: data breach policy, access control, business continuity, backup and recovery, and information security.
- We have implemented technical and organizational measures to comply with Article 32 of the GDPR.
- We have implemented processes to ensure data breaches are reported to a data controller and/or the ICO as soon as possible and in any case no later than within 72 hours.

3. Who is the data controller when conducting studies with Sermo?

When Sermo is recruiting from panel only	Data controller: Sermo Data processor: Client/Recipient of Data
When Sermo is recruiting from a client provided target list only	Data controller: Client/Target List Provider Data processor: Sermo
When Sermo is recruiting from both panel and client provided target list	Data controller: Sermo & Client/Target List Provider Data processor: Sermo & Client/Recipient of Data

- **When Sermo is recruiting from our panel:**

  Sermo is the data controller of such information. As such, Sermo has the consent of our data subjects to be invited to surveys by agreeing to our Terms of Use. As long as we don't provide clients or Pharma sponsors with any personal data, Sermo does not need to do anything additional and we can proceed in compliance with GDPR.

  a. When clients or Pharma sponsors are asking to re-contact a data subject in regards to an adverse event and provide them with members' personal data, Sermo would need to obtain informed consent from the respondents and explain the following:

     i. For what purposes we are providing the information

     ii. To whom they will be identified

     iii. What will happen to the information they give

     iv. What, if anything, will happen to them as a result of their waiver

  b. For qualitative pre-tests where personal data is provided to clients or Pharma sponsors, Sermo will ask you to sign a DPA to confirm you are only going to use the data for the purposes specified and will delete such information following the interview.

- **When Sermo is recruiting from a client-provided target list with non-Sermo panel members:**

  The controller of the information is the provider of the target list and Sermo will follow their lead as to how to process the information and how to recruit. Sermo will name the end client/Pharma sponsor when recruiting from the list and inform the data subjects of the purpose of collecting their data.

  Any time we are recruiting from a client-provided target list, we need to have the list provider sign a consent form that allows us to recruit from

the list and confirms they have the data subjects' consent to provide us with such information. Additionally, Sermo would sign a DPA upon request to ensure we are only using the data in accordance with their guidance and will delete such information at the end of the project.

— **When Sermo is recruiting from our panel and client-provided target lists:**
In such situations both the provider of the list and Sermo are considered joint data controllers. We will need to disclose both our name and the list provider's name and obtain the required consent from all data subjects respectively.

— **When Sermo is using a vendor/field work partner for recruitment:**
If Sermo is using a vendor to recruit for us from their own database, they are the data controller of this information. Sermo will ensure they have consent from their respondents to use their personal data and transfer it to Sermo.

General questions regarding GDPR in market research

1. What is the general practice to ensure GDPR compliance when conducting market research?
Sermo's general practice when conducting a standard market research survey is to provide our clients with anonymized project data in connection with the research results, excluding any personal data. When requested, we provide our clients with more detailed information as long as it does not contain personal data. This practice was in place before GDPR was in effect and we are continuing to conduct market research accordingly.

However, there are a few situations in which our clients are requesting that Sermo provides identifiable information. In these cases, Sermo has developed best practices to ensure compliance and will reach out to the panelists to request informed consent to transfer such personal data.

2. How has Sermo informed their panelists about GDPR requirements and gained their consent to continue using their information for these purposes?

Sermo has updated its Privacy Policy, Terms of Use, and Code of Conduct as well as sought consent from every panelist following GDPR coming into effect. In case the members do not agree to our consent form that allows us to use their personal data for market research purposes, they have the ability to opt out.

It is also important to note that each panel member can opt out at any time by reaching out to our support team or the Data Protection Officer in accordance with our data deletion policy.

We adhere to EphMRA 17.7-17.10 in regard to consent.

3. When is it required to name the sponsor when conducting a survey?

GDPR requires that a data controller is identified to the data subject when the data subject's personal data is obtained. Therefore, Sermo would need to disclose the name of the sponsor to participants at the beginning of the survey if the sponsor is receiving any personal data during the research.

When the sponsor is not receiving any personal data and the panel is entirely Sermo's, the sponsor should not be revealed and Sermo's Terms of Use and Code of Conduct (which were updated in accordance with GDPR) will apply. The concern is that if we reveal the sponsor's name, the survey would no longer be blinded and respondents may introduce bias to their responses.

If transfer of personal data is required for a specific project, we can name

the sponsor at the end to avoid bias. However, if a sponsor or a client is required to be disclosed at the end of the survey, the data subject should be made aware at the beginning, that the client/sponsor will be named at the end of the survey and that they can withdraw their consent at any time.

We adhere to EphMRA 3.31 in regard to naming sponsor practices

4. Can we ask respondents their place of work or other personal data questions such as postal code?

There is a likelihood that this information in combination with other data from the survey can become personally identifiable. As a result of GDPR, Sermo has recommended the following guidelines:

- Client should avoid requesting any kind of personal data within the survey itself. However, if it is absolutely necessary to request the information for the purposes of the research, one of the following scenarios will apply:
    a. If client is requesting this information during fieldwork, then respondents must be permitted to opt out of answering these questions in the survey. The Pharma sponsor must also be disclosed at the end of the survey.
    b. If client requests personal data of our panel members post survey completion, Sermo must gain informed consent from the panel members in order to provide this information.

5. Does the pharma sponsor need to be disclosed when conducting qualitative research and if so, when/where?

Irrespective of whether the Pharma sponsor is a data controller or not, recipients of personal data must be named before any data is transferred.

When a sponsor is listening into an interview live, they need to be disclosed at the beginning of the interview as they are directly obtaining personal data. However, we can name the sponsor at the end of the survey to avoid

bias, as long as the HCP is informed that their data is going to be transferred and that the sponsor name will be disclosed at the end of the survey. In any of the aforementioned cases, if at any time during the interview the HCP is requesting to know the name of the sponsor, the name has to be disclosed. Please note that some exclusions apply due to local laws and regulations.

When a sponsor is simply receiving a recording of the interview, the sponsor needs to be disclosed at the end of the interview to ensure a blinded interview and avoid bias. If a sponsor is not listening to theinterviews live or reviewing recordings/transcripts, the Pharma sponsor does not need to be disclosed.

In cases where the sponsor is disclosed at the end, the data subject should be informed upfront that such disclosure will be provided at the end of the survey.

We adhere to EphMRA 11.4 in regard to naming sponsor practices when conducting qualitative research.

6. How are client-provided target lists shared across countries?

- International transfers of personal data for processing may be made within the EU and EEA (Iceland, Liechtenstein, and Norway) with no restrictions.
- Transfers to the US from the EU should be avoided as much as possible. Currently Sermo is using internal, inter-company mechanisms for such transfers where necessary. Sermo would also sign model clauses with clients to ensure transfer is in compliance with GDPR.

7. What consent does Sermo need to obtain when sharing exclusion lists?

When Sermo is sharing exclusion lists with clients or vendors, we are only sharing the first 3 letters of a respondent's first name and first 3 letters of the

last name. Therefore, no personal data is being disclosed or transferred and therefore no additional action is required. However, if such information is being combined with additional information like field of practice or place of work - such information is considered personal data and informed consent is required from the panelist.

8. Does Sermo need to get additional consent when re-contacting respondents for quality purposes?

For market research quality control purposes, there is no need for Sermo to obtain additional consent to contact respondents because it is very likely to be in Sermo's legitimate interest as a data controller to do so.

If the need to re-contact is initiated by a client when the client is not the Data Controller, Sermo should let the respondents know during recruitment and obtain their informed consent in accordance with our informed consent policy (available upon request).

If re-contacting respondents is required for further research unrelated to data quality, additional informed consent would be required.

We adhere to EphMRA 3.41 in regards to informed consent practices.

Please note this document highlights Sermo's guidelines on GDPR compliance and does not supply legal or procedural advice for any company and for any purpose.

Questions? Please reach out to your Sermo representative or email us at sermoinfo@sermo.com