Code on Protection of Personal Data for Market, Media and Public Opinion Research Agencies

Contents

Introduction

The Code of Conduct for Market, Media and Public Opinion Research Agencies was prepared with an aim to a clearly interpret EU Regulation 2016/679 in the practice of market, media and public opinion research in the Republic of Croatia with the ultimate aim of transparent fulfilment of obligations established by the Regulation and accompanying regulation by all stakeholders.

The goals of the Code are to identify the key stakeholders and their requirements in the context of market, media and public opinion research.

- The Code establishes minimum obligations for Market, Media and Public Opinion Research Agencies operating in the Republic of Croatia in accordance with the regulatory obligations and professional rules.
- The Code confirms the rights of data subjects and obligations of Market, Media and Public Opinion Research Agencies for fulfilment of data subjects' rights in the context of market research and professional rules.
- The Code establishes a minimum level of establishing relationship between clients and the Market, Media and Public Opinion Research Agencies in the context of market research and professional rules.
- The Code establishes a minimum level of establishing relationship between subcontractors and the Market, Media and Public Opinion Research Agencies in the context of market research and professional rules.

This Code does not cover activities related to the so-called "Big Data Projects" or surveys on the Data subjects Panel. These projects are regularly established for a specific purpose and goal and a separate assessment of impact on the protection of personal data needs to prepared for each one. The Agency, Controller may use the structure of this code to prepare a separate assessment of the impact on the protection of personal data.

An agency that accepts the rules, obligations and responsibilities associated with this Code is required to confirm the acceptance of this Code in writing and publish it on its website.

An agency that accepts this Code is obliged to promote the same with all interested parties for the purpose of enhancing the protection of personal data in the practice of market, media and public opinion research.

Research context

Collection and processing of personal data is of crucial importance for the work of the Market Research Agency.

Different research techniques based on qualitative, quantitative or passive data collection methods such as surveys, focus groups, digital measurement or analytics of large data sets enable researchers to collect and process personal data to provide knowledge based on best professional practices to their clients.[1]

[1] Appropriate use of different legal bases under the GDPR June 2017 (p. 4)

In the context of market, media and public opinion research, it is important to emphasize the difference between data identifying individuals in market, media and public opinion research from data gathered from data subjects during the data collection phase, like responses, expressed opinions etc.

- The first group of data makes the category of identifying demographic data (personal data),
- Responders' responses are considered personal data only when they can be linked to demographic data of an individual (or if the responses themselves have identifying data) [2]

For this reason, researchers should take steps to anonymize data at an early stage of research.

ESOMAR - Fundamental principles[3]

1. When collecting personal data from data subjects for the purpose of research, researchers must be transparent about the information they plan to collect, the purpose for which it will be collected, with whom it might be shared and in what form.
2. Researchers must ensure that personal data used in research is thoroughly protected from unauthorised access and not disclosed without the consent of the data subject.
3. Researchers must always behave ethically and not do anything that might harm a data subject or damage the reputation of market, media and public opinion research industry.

Principles relating to processing of personal data

1. Lawfulness, fairness, and transparency - personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Purpose limitation - personal data must be collected for specified, explicit and legitimate purposes and may not be processed in a manner that is incompatible with these purposes; Further processing for the purposes of archiving in the public interest, for the purposes of scientific or historical research or for statistical purposes, in accordance with Article 89 Paragraph 1 is not considered to be incompatible with the original purpose.
3. Data minimisation- personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are being processed.
4. Accuracy - personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. Storage limitation - Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 Paragraph 1 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
6. Integrity and confidentiality - Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The rights of data subjects

1. Right of access by the data subject (Article 15 of EU Regulation 2016/679)
2. Right to rectification (Article 16 of the EU Regulation 2016/679)

[2] Appropriate use of different legal bases under the GDPR June 2017 (p. 7)

[3] ICC/Esomar international code on Market, Opinion and Social Research and Data Analytics (p. 7)

3. Right to erasure (‘right to be forgotten’) (Article 17 of EU Regulation 2016/679)
4. Right to restriction of processing (Article 18 of EU Regulation 2016/679)
5. Notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 of EU Regulation 2016/679)
6. Right to data portability (Article 20 of EU Regulation 2016/679)
7. Right to object (Article 21 of EU Regulation 2016/679)
8. Automated individual decision-making, including profiling (Article 22 of EU Regulation 2016/679)

Description of market research process, risk assessment and impact on the protection of personal data, organizational protection measures at project level

An integral part of this Code is the initial assessment of the impact on the protection of personal data for the rights and freedoms of the data subjects (hereinafter referred to as the "impact assessment") in the market research process.

Agency may use the points of this Code relating to the impact assessment in the market research process.

In this part of the Code:

- The market research process from the aspect of the Agency was established.
- For each part of the process and type of research, the roles of the Client and the Agency have been determined
- For each part of the process and type of research that affects personal data, key risks are identified by organizational roles.
- For each part of the process, the type of research and the organizational role, an assessment of the necessity and proportionality of processing procedures related to their purposes has been established.
- For each part of the process, the type of research and the organizational role, risk assessment for the rights and freedoms of the research subject has been established before implementing risk mitigation measures.
- For each part of the process, the type of research and organizational role minimum organizational measures that need to be taken to reduce risk and assess the results of the implemented measure were defined.
- For each part of the process, the type of research and the organizational role, risk assessment for the rights and freedoms of the data subject after the implementation of risk mitigation measures has been established.
- For the infrastructure used in the realization of the process, the technical measures to be taken for the purpose of risk reduction and the cumulative evaluation of the results of the implemented measures have been established.
- The minimum level of conditions for transferring the whole or part of the research project of the Agency to subcontractors has been established.
- The minimum level of prior consultation of the Agency and the Client (sale and contracting) was established.
- Further obligations of the Agency have been established in accordance with the requirements of the Regulation with application in market, media and public opinion research.

In case that it acts as the controller, the Agency must perform impact assessment for each processing involving personal data and is not included in the impact assessment within this Code.

The Agency must perform impact assessment before the processing of the data from the data subjects.

The Agency may, if necessary and mandatory in the event of a change of the key parameters on which the impact assessment is based in the Code, carry out a review and an update of the impact assessment and must seek advice from the Data Protection Officer.

If the Agency conducts a separate impact assessment for processing not covered by the impact assessment in this Code, it must seek advice from the Data Protection Officer.

If acting as a processor, the Agency should assist the controller in preparing and carrying out the impact assessment.

The research process phases

The research process phases in the Market Research Agency have been established by ISO 20252: 2012 standards (for market, media and public opinion research).

The aforementioned standard was chosen as the basis for this Code of Conduct because of the ability to clearly supervise personal data through the research process.

Table: Review of Research Projects Phases and Expected Presence of Personal Data of Data Subjects in Research

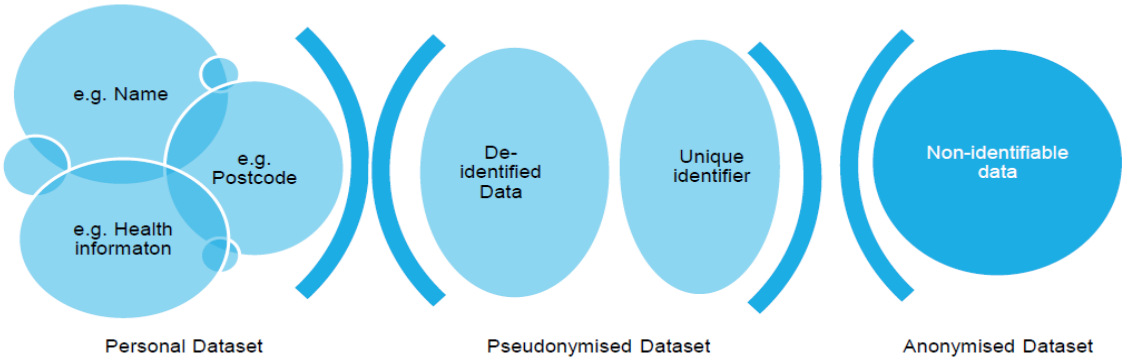
Research process phases	Research process phases (in detail)	Personal data of data subjects
Sale	Sale	None
Preparation	The questionnaire / guide	None
	Sample	Databases of data subjects
Data collection	Data collection and control	Responses from data subjects
Data processing	Creating a mask	Responses from data subjects
	Data cleaning	Responses from data subjects
	Data coding	Pseudonymised
	Data analysis	Pseudonymised
Reporting	Reporting	None

Pseudonymisation and Anonymisation

Agencies and researchers should ensure the implementation of pseudonymisation and anonymisation of data as soon as technically possible.

(Picture[4] - of personal data – from pseudonymised to anonymised data)

Figure 1: From personal to anonymised data



The data is pseudonymised when there is a possibility of linking personal data with the data subject by using a unique identifier.

- If pseudonymised data is used in the work it is necessary to restrict access to it.

[4] Appropriate use of different legal bases under the GDPR June 2017 (p. 8)

- In managing pseudonymised data is necessary to apply all the associated organisational and technical protection measures.

Data is anonymised when the following conditions are met:

1. Data cannot be associated with the data subject directly or indirectly,
2. The data is not relatable to any pre-stored data of the data subjects
3. The data is not relatable to the data subject unless disproportionate costs, time, human and computer power are used.

Anonymised data need to be protected from the aspect of business importance, but they are not covered by the Regulation.

Phase 1: Sales

In the sales phase the client determines the (operational) purpose of the research, determines the choice of methodology, which includes definition of questionnaires, sample size, data collection method, data processing level and reporting.

- Depending on the purpose of the research in the above mentioned phase, the client can determine that the research will be carried out on databases submitted by the client, which may contain personal data of the targeted data subjects.
- The mentioned decisions determine the level of impact of the research project on each data subject.

Based on the chosen purpose and methodology, a bid containing the cost and time dimension of the research project is determined.

The activities of determining the purpose and the engagement of funds for the realization of the research project define the client as the controller.

* If the Agency carries out the research for its own purposes and subsequently offers it on the market, i.e. it is not prompted by the client then the Agency is the controller.

Phase 2: Preparation

In the second phase of the research process, the client, the Agency on behalf of the client or Agency in its own name:

- Define specific questions in the Questionnaire / Guide to be given to the data subjects.
    - When the client prepares a questionnaire / guide that the Agency is required to implement, the client is required to limit the collection and subsequent processing of personal data to questions relevant to the purpose of the research in order to reduce the amount of data.
        - The agency should warn the client in case of excessive data collection.
        - The Agency is required to keep a documented client order.
    - When the Agency prepares a questionnaire / guide as a consultant on behalf of a client, it is required to limit the collection and subsequent processing of personal data to questions relevant to the purpose of research with a goal to reduce the amount of data collected.
        - The Client is responsible for approving the final version of the questionnaire / guide by which the data will be collected.
        - The Agency is required to keep a documented client order.
    - When the Agency prepares a questionnaire / guide for its own needs, it is required to limit the collection and subsequent processing of personal data to questions relevant to the purpose of research with a goal to reduce the amount of data collected.

- In order for the Agency to lawfully process personal data, there must be at least one legal basis for processing. The controller must choose the most appropriate legal basis for data processing.
    - If the client is controller, he must choose the legal basis for processing the data.
    - The Agency is required to refer the client to any doubt about the legal basis.
    - In general, legal bases in the market research process that can be used to process personal data are:
        - Consent of data subjects for processing personal data for research purposes;
        - Legitimate interests of the Controller (or third party)
        - Carrying out the public interest / official duty of the controller

    * If the consent of data subjects is selected as the basis for the processing of personal data for the purposes of research, controller is required to authorize the use of consent for possible subsequent legal effects.

- Specifies the database for sample selection framework and the sample itself. This refers to the total number and distribution of the data subjects.
    - When the client prepares the sample, he is required to limit the sample size to the relevant one for research purposes in accordance with the rules of the profession, with the aim of reducing the amount of data.
        - The agency should warn the client in case of excessive data collection.
        - The Agency is obliged to keep a documented client order.
    - When the Agency prepares a sample as a consultant on behalf of a client, it is required to limit the size of the sample to the relevant one for the purpose of the research in accordance with the rules of the profession.
        - The client is required to approve the sample.
        - The Agency is required to keep a documented client order.
    - When the Agency prepares a sample for its own needs, it is required to limit the size of the sample to the relevant one for the purpose of research in accordance with the rules of the profession.

In case that the research is carried out on databases submitted by the client which may contain personal data of the targeted data subjects, the client is required to establish and ensure the application of the legal basis for the submission of the personal data of the data subjects to the Agency.

- Prior to the delivery of personal data, the Agency is required to formalize the relationship with the client as the controller / processor or the rule established by this code is enforced.
    - The delivery of personal data database further identifies the client as the controller.
    - The client is required to ensure the delivery of a minimum set of personal data necessary for the conduct of the research.
    - The Agency is required to refer the client to deliver the minimum set of personal data necessary for the research itself.
    - To ensure the delivery process, the client should apply technical measures related to data transfer and storage.
- In case the client submits the database of the data subjects, then the Agency is required to apply the technical protection measures as described below.

Researchers: With regard to the activities that can be carried out on the research project, and particularly when the Agency is in the role of a controller or a joint controller, or the Agency consults the client when defining questionnaires / guides and samples, researchers have a significant influence on all activities in the research process. These activities are necessary for the execution of the service, and cannot be avoided.

In the case of an incident at a researcher level, an incident could have a potentially high level of influence on individual's rights and freedoms. This level of risk is not acceptable and additional measures are needed to reduce the risks associated with the researchers.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the researchers:

- Sign a contract with the researcher regarding the protection of personal data;
- Increase further awareness of the researchers regarding personal data protection.
- Limit / minimize the retention of personal data with the researchers.
- Restrict access to personal data exclusively to projects in which they cooperate.
- Establish additional supervision over the work of the researchers regarding the protection of personal data.

Even with the use of measures to further reduce the risk at the researcher's level, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms, but it would reinforce lawful position of the Agency and further influence the researchers' awareness. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Phase 3: Data Collection

At the data collection stage, the Agency collects data using client's or their own data collection infrastructure.

When the client, in accordance with the responsibilities of Phase 1 and Phase 2, is the controller:

- The Agency is a processor: in case the Agency uses client infrastructure (servers, applications, etc.) and cannot technically access the responses of the data subjects with reasonable efforts. In the aforementioned case, it may only be responsible for the possible failure of the interviewer when collecting the data.
- The Agency is a joint controller: in case the Agency uses its own infrastructure (servers, applications, etc.) through which it is technically able to access the responses of the data subjects. In the aforementioned case, the Agency may be responsible for the omissions related to the protection of personal data, while it is particularly responsible for the delivery of the data subjects' databases.

The Agency is the Controller: in accordance with Phase 1 and Phase 2 it is already fulfilling the role of the controller and using its own infrastructure (servers, applications, etc.), through which it is technically able to access the responses of the data subjects.

It is important to emphasize the responsibility of the Project Manager identified in the sales phase and the research preparation phase, as it directly influences the level of responsibility of the Agency in the data collection phase.

Quality Control of Collected Data

An integral part of the data collection phase encompasses the activities of quality control of the collected data and the work of the interviewer network.

Data processing for the purpose of quality control is necessary from the aspect of performing the requirements of the profession, and only research without an appropriate level of quality control is not acceptable as a performance of appropriate service.

- This Code of Conduct confirms the legitimate interest of the Agency to carry out direct or subsequent activities related to quality assurance for the purposes of controlling the quality of the data collected in relation to professional requirements.
- Data subjects need to be clearly informed about the possibility of quality control activities so that they are aware and expect processing for this purpose.
- The Agency is required to establish and apply internally approved quality control procedures for all types of data collection in research projects in accordance with quality assurance standards in the field of market, media and public opinion research.
    - Internal quality control procedures established by the Agency must establish the minimum and maximum levels of quality control of the data collected and the work of the interviewer.
    - For the purpose of ensuring compliance with quality assurance standards in the area of market, media and public opinion research, the Agency is required to keep the records of the implementation of controls indicating the identity of the individual for a period that is as short as possible, maximum of one year.
        - If the client as a controller requires that personal data related to the control are kept for a period of more than one year, the Agency is required to retain the documented information of the Client's order. In this case, the Client (Controller) and the Agency as (joint) controllers are required to determine the reasons and justification for keeping data over a longer period of time.

Quantitative research conducted by face-to-face and observational research

Along with data subjects, it is possible to expect next active roles: interviewers, quality control managers, coordinators, and field managers.

Interviewers: collect data from the data subjects and thus have a direct insight into the answers of the individual data subject. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- Data collection alone represents a potentially high impact on the rights and freedoms of individuals of a particular data subject, but the impact of a single interviewer is limited to a "smaller" number of data subjects by limiting the maximum number of surveys that may be collected by an individual interviewer (max 10%) according to the rules of the profession.
- Based on the mentioned limitation of the maximum number of surveys that an individual interviewer may collect, in the case of an incident at an interviewer level the incident could have a potentially low or medium level of influence on the rights and freedoms of individuals. This level of risk is not acceptable and additional measures are needed to reduce the risk associated with the interviewers.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the interviewers:
  - Sign a contract with the interviewer regarding the protection of personal data;
  - Increase further awareness of the interviewers regarding the protection of personal data.
  - Limit / minimize the retention of personal data with interviewers.

  Even with the implementation of measures to further mitigate risk at the interviewer level, a potential incident would represent an incident with a low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Coordinators: Coordinate activities of a large number of interviewers and potentially have access to surveys, including personal data and data subjects' responses, conducted under the supervision of their own interviewers. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the coordinator level, an incident could have a potentially low, medium or high level of influence on rights and freedoms individuals. The above level of risk is not acceptable and additional measures are needed to reduce the risks associated with coordinators.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the coordinators:
  - Sign a contract with the coordinator regarding the protection of personal data;
  - Increase further awareness of coordinators regarding the protection of personal data;
  - Limit / minimize the retention of personal data at the coordinator location (maximum monthly relocation of all material containing personal data that need to be kept from the coordinator location to the Agency's Office).

  Even with the implementation of measures to further mitigate risk at the coordinator level, a potential incident would represent an incident with a maximally medium level of influence on rights and freedoms of individuals. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Quality control managers: For the purposes of carrying out control activities, they may have access to a larger number of surveys and thus a larger set of personal data. These activities are necessary for the execution of the service, and cannot be avoided.

- In case of an incident at a quality control manager level, the incident could have a potentially medium level of influence on rights and freedoms individuals. The above level of risk is not acceptable and additional measures are needed to reduce the risks associated with quality control managers.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to quality control managers:

- Sign a contract with the quality control managers regarding the protection of personal data;
- Increase further awareness of quality control managers regarding the protection of personal data;
- Ensure execution of control activities exclusively from the premises of the Agency;
- Restrict access to surveys exclusively to surveys that are being controlled
- Keep records of the performed control with the provision of written and electronic notes (logs of performed control).

With the implementation of measures to further reduce risk at the quality control manager level, a potential incident would represent an incident with low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Field Manager and Support Staff: Manage the activities of all coordinators, quality control managers and interviewers, and potentially have access to all surveys, and thus to a larger set of personal data. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the level of a field manager, an incident could have a potentially high level of influence on the rights and freedoms of individuals. Although the specified level of risk is conditioned by the performance of the service itself, additional measures must be taken to reduce the risks associated with the field managers and the support staff.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to field managers and support staff:

- Sign a contract with the field manager and the support staff regarding the protection of personal data;
- Increase further awareness of the field manager and support staff regarding the protection of personal data;
- Restrict access to materials and equipment exclusively to field managers and support staff.
- Ensure access to materials and equipment exclusively from the premises of the Agency;
- Establish additional supervision over the activities of field managers and support staff regarding the protection of personal data.

Even with the implementation of measures to further reduce risk at the level of the field manager and support staff, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Archivist: The role of the archivist is to store and restrict access to the data on the printed forms / surveys, and to execute the destruction of completed surveys immediately after the deadline for destruction. This is why Archivists need to access surveys. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the Archivist level, the incident could have a potentially high level of influence on individual's rights and freedoms. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the Archivists:

- Sign a contract with the Archivist regarding the protection of personal data;
- Increase further awareness of archivist regarding the personal data protection.
- Restrict access to the archive to a minimum number of people
- Introduce records of input / output of materials in the Archive.

Even with the implementation of measures to further reduce the risk at the Archivist level, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of Archivist. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Conclusion: In the case of cumulative application of protection measures for each identified role in the data collection phase, a potential high level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the level of the field manager and the support staff. Potential incidents with interviewers and quality control managers can be minimized and limited to a low level of influence on the rights and freedoms of the data subjects. Potential incidents with coordinators can be reduced and limited to a medium level of influence on the rights and freedoms of the data subjects.

Mystery shopping

Along with data subjects, it is possible to expect next active roles: interviewers, coordinators and field managers.

Interviewers: collect data from the data subjects and thus have a direct insight into the answers of the individual data subject. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- Data collection alone represents a potentially high impact on the rights and freedoms of individuals of a particular data subject, but the impact of a single interviewer is limited to a "smaller" number of data subjects by limiting the maximum number of surveys that may be collected by an individual interviewer (max 10%) according to the rules of the profession.
- Based on the mentioned limitation of the maximum number of surveys that an individual interviewer may collect, in the case of an incident at an interviewer level the incident could have a potentially low or medium level of influence on the rights and freedoms of individuals. This level of risk is not acceptable and additional measures are needed to reduce the risk associated with the interviewers.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the interviewers:

- Sign a contract with the interviewer regarding the protection of personal data;
- Increase further awareness of the interviewers regarding the protection of personal data.
- Limit / minimize the retention of personal data with interviewers.

Even with the implementation of measures to further mitigate risk at the interviewer level, a potential incident would represent an incident with a low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Coordinators: Coordinate activities of a large number of interviewers and potentially have access to surveys, including personal data and data subjects' responses, conducted under the supervision of their own interviewers. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the coordinator level, an incident could have a potentially low, medium or high level of influence on rights and freedoms of individuals. This level of risk is not acceptable and additional measures are needed to reduce the risks associated with coordinators.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the coordinators:
  - Sign a contract with the coordinator regarding the protection of personal data;
  - Increase further awareness of coordinators regarding the protection of personal data;
  - Limit / minimize the retention of personal data at the coordinator location (maximum monthly relocation of all material containing personal data that needs to be kept from the coordinator location to the Agency's Office).

  With the implementation of measures to further mitigate risk at the coordinator level, a potential incident would represent an incident with a maximally medium level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Field Manager and Support Staff: Manage the activities of all coordinators, quality control managers and interviewers, and potentially have access to all surveys, and thus to a larger set of personal data. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the level of a field manager, an incident could have a potentially high level of influence on the rights and freedoms of individuals. Although the specified level of risk is conditioned by the performance of the service itself, additional measures must be taken to reduce the risks associated with the field managers and the support staff.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to field managers and support staff:
  - Sign a contract with the field manager and the support staff regarding the protection of personal data;
  - Increase further awareness of the field manager and support staff regarding the protection of personal data;
  - Restrict access to materials and equipment exclusively to field managers and support staff.
  - Ensure access to materials and equipment exclusively from the premises of the Agency;
  - Establish additional supervision over the activities of field managers and support staff regarding the protection of personal data.

  Even with the implementation of measures to further reduce risk at the level of the field manager and support staff, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Archivist: The role of the archivist is to store and restrict access to the data on the printed forms / surveys, and to execute the destruction of completed surveys immediately after the deadline for destruction. This is why Archivists need to access surveys. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the Archivist level, the incident could have a potentially high level of influence on rights and freedoms of individuals. This level of risk is not acceptable and additional risk mitigation measures are necessary.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the Archivists:
  - Sign a contract with the Archivist regarding the protection of personal data;

- Increase further awareness of archivist regarding the personal data protection.
- Restrict access to the archive to a minimum number of people
- Introduce records of input / output of materials in the Archive.

Even with the implementation of measures to further reduce the risk at the Archivist level, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of the field managers and the support staff. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Conclusion: In case of cumulative application of protection measures for each identified role in the data collection phase, a potential high level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the level of the field manager and the support staff. Potential incidents with interviewers and quality control managers can be minimized and limited to a low level of influence on the rights and freedoms of the data subjects. Potential incidents with coordinators can be reduced and limited to a medium level of influence on the rights and freedoms of the data subjects.

Quantitative research by telephone interview method

Along with data subjects, it is possible to expect next active roles: interviewers, quality control managers, field managers and support staff.

Interviewers: collect data from the data subjects and thus have a direct insight into the answers of the individual data subject. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- Data collection alone represents a potentially high impact on the rights and freedoms of individuals of a particular data subject, but the impact of a single interviewer is limited to a "smaller" number of data subjects by limiting the maximum number of surveys that may be collected by an individual interviewer (max 10%) according to the rules of the profession.
- Based on the mentioned limitation of the maximum number of surveys that an individual interviewer may collect, in the case of an incident at an interviewer level the incident could have a potentially low or medium level of influence on the rights and freedoms of individuals. This level of risk is not acceptable and additional measures are needed to reduce the risk associated with the interviewers.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the interviewers:

- Sign a contract with the interviewer regarding the protection of personal data;
- Increase further awareness of the interviewers regarding the protection of personal data.
- Limit / minimize the retention of personal data with interviewers.

With the implementation of measures to further mitigate risk at the interviewer level, a potential incident would represent an incident with a low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Quality control managers: For the purposes of carrying out control activities, they may have access to a larger number of surveys and thus a larger set of personal data. These activities are necessary for the execution of the service, and cannot be avoided.

- In case of an incident at a quality control manager level, the incident could have a potentially medium level of influence on rights and freedoms of individuals. The above level of risk is not acceptable and additional measures are needed to reduce the risks associated with quality control managers.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to quality control managers:

- Sign a contract with the quality control managers regarding the protection of personal data;
- Increase further awareness of quality control managers regarding the protection of personal data;
- Ensure execution of control activities exclusively from the premises of the Agency;
- Restrict access to surveys exclusively to surveys that are being controlled
- Keep records of the performed control with the provision of written and electronic notes (logs of performed control).

With the implementation of measures to further reduce risk at the quality control manager level, a potential incident would represent an incident with low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Field Manager and Support Staff: Manage the activities of all coordinators, quality control managers and interviewers, and potentially have access to all surveys, and thus to a larger set of personal data. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the level of a field manager, an incident could have a potentially high level of influence on the rights and freedoms of individuals. Although the specified level of risk is conditioned by the performance of the service itself, additional measures must be taken to reduce the risks associated with the field managers (and the support staff).

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to field managers and support staff:

- Sign a contract with the field manager and the support staff regarding the protection of personal data;
- Increase further awareness of the field manager and support staff regarding the protection of personal data;
- Restrict access to materials and equipment exclusively to field managers and support staff.
- Ensure access to materials and equipment exclusively from the premises of the Agency;
- Establish additional supervision over the activities of field managers and support staff regarding the protection of personal data.

Even with the implementation of measures to further reduce risk at the level of the field manager and support staff, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Conclusion: In case of cumulative application of protection measures for each identified role in the data collection phase, a potential high level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the level of the field manager and the support staff. Potential incidents with interviewers and quality control managers can be minimized and limited to a low level of influence on the rights and freedoms of the data subjects.

Quantitative research conducted over the internet

In addition to data subjects, it is possible to expect the following active roles: Help Desk, Field Manager and Support Staff, Coordinator, Panel Manager(s)

Support (Help Desk): Respond to the questions of the survey participants and thus have access to the specific questions of the data subjects / responses provided. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- Responding to the participant's inquiries itself is limited to the minimum set of personal data provided by data subject. Increased impact can be caused by a potentially larger number of data subjects who contact the Help Desk.
- Based on the aforementioned limitation of the personal data set provided by a data subject, a potential incident could have a low or medium level of influence on the rights and freedoms of individuals.
- This level of risk is not acceptable and additional measures are needed to reduce the risk associated with help desk.

Measures to further reduce the risk of an incident impacting on the rights and freedoms of individuals involved in supporting data subjects:

- Sign a contract with the support member regarding the protection of personal data;
- Increase further awareness of the support member regarding the protection of personal data.
- Separate support activities from coordination activities or panel activities to avoid access to personal data collected in the research.

With the implementation of additional risk mitigation measures at the level of support, a potential incident would represent an incident with a low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Field Manager and Support Staff: Manages the activities of the coordinator, support and panel manager. Due to the needs of the job, they have access to the responses in panel surveys and participants' profiles. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the level of the field manager, the incident could have a potentially medium or high level of influence on the rights and freedoms of individuals. This level of risk is not acceptable and additional measures are required to reduce the risk associated with the field manager.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to field managers:

- Sign a contract with the field manager regarding the protection of personal data;
- Increase further awareness of the field manager regarding the protection of personal data;
- Restrict access to materials and equipment exclusively to field managers and support staff.
- Establish additional supervision over the activities of field managers and support staff regarding the protection of personal data.

Even with the implementation of measures to further reduce the risk at the level of Field Manager and support staff, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of the field managers and the support staff. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Coordinator: Performs research by the order of the field manager. For the purposes of job execution, they have access to the answers to the survey. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at a coordinator level, it could have a potentially high level of influence on individual's rights and freedoms. This level of risk is not acceptable and additional measures are required to reduce the risks associated with the coordinators.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the coordinators:

  - Sign a contract with the coordinator regarding the protection of personal data;
  - Increase further awareness of the coordinator regarding the protection of personal data;
  - Separate coordination activities from panel activities or support activities to avoid access to personal data of the data subjects.
  - Restrict access to survey responses in research projects directly involved in.
  - Disable retrospective access to survey responses in the research projects they participated in.
  - Establish additional supervision over coordinator's activities regarding the protection of personal data.

  Even with the implementation of measures to further reduce risk at the coordinator level, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of coordinators. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Panel Manager(s): Controls panel activities (recruits and communicates with panel members) according to a field manager's order. For the purposes of job execution, they may have access to the personal data of the data subjects. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the level of a panel manager, an incident could have a potentially high level of influence on individual's rights and freedoms. This level of risk is not acceptable and additional measures to reduce the risks associated with panel managers are necessary.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to panel managers:

  - Sign a contract with the panel manager regarding the protection of personal data;
  - Increase further awareness of the panel manager regarding the protection of personal data;
  - Panel work activities should be separated from coordination or support activities with the aim of avoiding access to the answers collected during the research.
  - Establish additional control over panel manager activities related to the protection of personal data.

  With the implementation of measures to further reduce the level of risk at the level of the panel manager, a potential incident would represent an incident with a medium level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Conclusion: In case of cumulative application of protection measures for each identified role in the data collection phase, a potential high level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the level of the field manager and support staff and the coordinator. Potential incidents with support can be minimized and limited to a low level of influence on the rights and freedoms of the data subjects. Potential incidents with the panel manager can be reduced and limited to a medium level of influence on the rights and freedoms of the data subjects.

Qualitative research

In addition to data subjects, it is possible to expect the following active roles: recruiter, hostess, field manager (and support staff), moderator, technical staff, archivist.

Recruiters: collect a small set of data from the survey participants based on the recruitment questionnaire and thus have a direct insight into the responses of a particular data subject, but to a lesser extent. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- Recruitment of data subjects does not pose a potentially high impact on the rights and freedoms of potential data subjects. Also, the impact of recruiters due to their nature (qualitative research) is limited by a smaller sample and thus with a smaller number of potential data subjects.
- Based on the above-mentioned limitations, in case of an incident at the recruiter level, it could have a potentially low or medium level of influence on individual's rights and freedoms. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to recruiters:

- Sign a contract with the recruiter regarding the protection of personal data;
- Increase further awareness of recruiters regarding the protection of personal data.

With the implementation of measures to further reduce risk at recruiter level, a potential incident would represent an incident with a low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Hostess (who performs and controls the quality of the recruiter's work): Verifies the authenticity of the data from the recruiting questionnaire personally with the potential participant in the research and thus has a direct insight into the answers of the individual data subject, but to a lesser extent. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- Quality control activities and hostesses do not pose a potentially high impact on the rights and freedoms of potential data subjects. Also, due to the very nature (qualitative research), the impact is limited by a smaller sample and thus with a smaller number of potential data subjects.
- Based on the above-mentioned limitations, in case of a hostess / quality control incident, it would potentially have low or medium level of impact on individual's rights and freedoms. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to hostesses:

- Sign a contract with the hostess regarding the protection of personal data;
- Increase further awareness of hostesses regarding the protection of personal data.

Even with the implementation of measures to further reduce risk at the hostess level, a potential incident could still be an incident with a potentially medium level of influence on rights and freedoms of individuals, but it would lawfully strengthen the position of the Agency and further influence the awareness of hostesses. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Field Manager and Support Staff: Manage the activities of recruiters and hostesses, and potentially have access to all recruiting questionnaires, and thus a larger set of personal data. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In the event of an incident at the field managers level incident could have high impact on the rights and freedoms of potential data subjects. Although the specified level of risk is conditioned by the performance of the service itself, additional measures must be taken to reduce the risks associated with the field managers and the support staff.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to field managers and support staff:
  - Sign a contract with the field manager and the support staff regarding the protection of personal data;
  - Increase further awareness of the field manager and support staff regarding the protection of personal data;
  - Provide access to materials and equipment for conducting the work of the field manager and support staff solely from the premises of the Agency;
  - Prohibit the storage of qualitative surveys records.
  - Limit Access to Archives containing Qualitative Surveys.

  With the implementation of measures to further reduce risk at the level of field managers and support staff, a potential incident would represent an incident with the maximally medium level of impact on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Moderator: Based on the guide for qualitative research, collects the data subjects' answers in accordance with the purpose of research. Thus, is able to obtain a larger set of personal data. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the moderator level, the incident could have a potentially high level of influence on individual's rights and freedoms. The impact of the qualitative research is limited by a smaller number of data subjects and thus with a smaller number of potential data subjects. However, the impact can be significant due to the fact that qualitative surveys are recorded in a large number of cases. This level of risk is not acceptable and additional risk mitigation measures are necessary.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to moderators:
  - Sign a contract with the moderator regarding the protection of personal data;
  - Increase further awareness of moderators regarding the protection of personal data.
  - Apply measures of reduced identification of data subjects in the moderation phase (e.g. reference only by name (no surnames).
  - Limit access of moderators to qualitative research recordings (if they are preparing the report) to a period of report preparation.
  - Storage limitation of the qualitative survey recordings to the moderators (if they are preparing the report) on a personal computer to a period of report preparation.
  - Prohibition to store recordings on a personal computer if the moderator does not prepare the report
  - Establish additional monitoring of moderator activities related to personal data protection.

  Even with the implementation of measures to further reduce risk at the moderator level, a potential incident could still be an incident with a potentially high level of influence on individual's rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of moderators. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Archivist: The role of archivist is to store and restrict access to recordings, and to execute the destruction of recordings immediately after the expiration date. This is why the Archivist needs to access the recordings of qualitative research. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In the case of an incident at the Archivist incident level, an incident could have a potentially high level of influence on individuals' rights and freedoms. The impact of the qualitative research is limited by a smaller number of data subjects and thus with a smaller number of potential data subjects. However, the impact can be significant due to the fact that qualitative surveys in a large number of cases are recorded. This level of risk is not acceptable and additional risk mitigation measures are necessary.

  Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the Archivists:
  - Sign a contract with the Archivist regarding the protection of personal data;
  - Increase further awareness of archivists regarding the protection of personal data.
  - Encrypt content on recordings before saving to Archive, disable access to Archivist by passwords.
  - Apply technical measures at the level of archivists (defined subsequently);
  - Prohibit storing content on recordings before saving to Archive.

  With the implementation of measures to further reduce the risk, especially the encryption of recordings, at the Archivist level, a potential incident would represent an incident with a low level of influence on individual's rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Conclusion: In case of cumulative application of protection measures for each identified role in the data collection phase, an incident with a potentially high level of influence on the rights and freedoms of the data subjects would be possible with moderators and technical staff. Potential incidents with Archivists and Recruiters can be minimized and limited to a low level of influence on the rights and freedoms of the data subjects. Potential incidents with the Field Managers and support staff, hostesses (quality control) cannot be reduced beyond the potentially medium impact on the rights and freedoms of the data subjects.

Phase 4: Data Processing - Quantitative Researches

In data processing phase, the Agency prepares and processes data using its client or own infrastructure.

When the client in compliance with the responsibilities from Phase 1 (Sales) and Phase 2 (Preparation of Research), is the Controller, unrelated to the status of the Agency in Phase 3 (data collection):

- The Agency is a processor: in case of using client infrastructure (servers, applications, etc.) and it cannot technically access personal data with reasonable efforts. In the aforementioned case it may only be liable for any failure of employees in the process of data processing.
- The Agency is a joint controller: in case the Agency uses its own infrastructure (servers, applications, etc.) through which it is technically able to access personal data of the data subjects. In the aforementioned case, the Agency may only be liable for any failure of employees in the process of data processing

The Agency is the controller: when according to Phase 1 and Phase 2 it is already fulfilling the role of the controller and using own infrastructure (servers, applications, etc.) through which it is technically able to access the responses of the data subjects and is liable for the possible failure of employees in the data processing phase.

Data processing phase is divided into four groups of activities: preparation of the questionnaire in electronic form (Scripting), cleaning data (Editing), coding of responses (Coding), analysis of the data (Data analysis).

From the aspect of personal data protection, the key activities are preparation of questionnaire in electronic form (Scripting) and cleaning data (Editing). Activity related to coding of responses and data analysis are performed on anonymized data and are not relevant from the aspect of personal data protection.

Preparation of the questionnaire in electronic form (Scripting)

The research projects in which the responses from a larger number of survey participants are collected for appropriate subsequent statistical analysis it is necessary to transfer responses in electronic form. For this purpose, a questionnaire is created to ensure that a minimum set of questions is set up based on the data subjects' response. The questionnaire is ultimately prepared in electronic form, but depending on the approach to data collection (collection by printed questionnaire (paper questionnaire) or electronic questionnaire (using computers, tablets, laptops, mobile phones, internet), questionnaire can be prepared before the data collection process (electronic questionnaire) or after data collection (printed questionnaire).

Scripting team: In the process of preparing a questionnaire for data collection or subsequent entry of collected data, even with the use of control mechanisms, there can be weaknesses that can only be detected at the stage of data collection. The activity of correcting the questionnaires due to the dynamics of the process itself is in practice carried out on live data, thus the employees who prepare the electronic questionnaire have the business need and the ability to access the data subjects' responses, which should be recognized as an activity with potentially high impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident with an impact on the rights and freedoms of individuals related to employees preparing electronic questionnaires (scripting):

- Sign a contract with employees in scripting regarding the protection of personal data;
- Increase further awareness of employees in scripting regarding personal data protection;
- Restrict access to personal data in surveys only to employees in scripting.
- Limit access of employees in scripting solely to projects on which they collaborate.
- Limit the work of employees in scripting to equipment exclusively from the premises of the Agency (if authorisations provide access to personal data).
- Establish additional control over the work of scripting staff regarding the protection of personal data.

Even with the implementation of measures to further reduce risk at the scripting staff level, a potential incident could still be an incident with a potentially high level of influence on individuals' rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of scripting staff. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Scripting manager: The management role is necessary from the control point of view and sometimes allows direct intervention on all projects and thus all data. This role implies the business need and the ability to access the participants' responses from a larger number of researches which needs to be identified as activity with a potentially high impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident with an impact on the rights and freedoms of individuals related to employees who prepare electronic questionnaires (scripting manager):

- Sign a contract with the scripting manager regarding the protection of personal data;
- Increase further awareness of scripting manager regarding the protection of personal data;
- Limit the work of the scripting manager to the equipment exclusively from the premises of the Agency (if authorisations provide access to personal data).

- Establish additional control over the work of the scripting manager related to the personal data protection.

Even with the implementation of measures to further reduce risk at the scripting manager level, a potential incident could still be an incident with a potentially high level of influence on individuals' rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of scripting manager. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Conclusion: In case of cumulative application of protection measures for each identified role in the scripting phase, the potential high level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the level of scripting manager and scripting staff. For this reason, it is necessary to apply additional technical protection measures in the process.

Data cleaning - Editing

In the research project in which the responses of a larger number of data subjects are collected, it is necessary to review answers in terms of correctness of the entered answers for subsequent statistical processing.

The first step in data cleaning is downloading data from electronic questionnaires, and pseudonymisation of data. This is achieved by excluding any personal data of the data subject in the file that is downloaded from the electronic questionnaire.

Data is pseudonymised in a manner that retains survey identifiers (e.g., IDs). It is relatable to a specific data subject only by persons who have access to the survey and the mentioned file and linking cannot be carried out automatically in practice.

The file with pseudonymised data can and should be stored to ensure quality assurance from a professional perspective.

Exiting the data cleaning phase is the preparation of the file from which the identifiers of the survey (ID) are deleted and further activities are performed exclusively on anonymised data.
Further data processing (coding and data analysis) is performed on fully anonymised data.

Editing team: Employees who work on editing data have the business need and the ability to access the data subjects' responses, which should be recognized as an activity with a potentially high impact on the rights and freedoms of data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident with an impact on the rights and freedoms of individuals related to employees preparing electronic questionnaires (editing):

- Sign a contract with editing staff regarding the protection of personal data;
- Increase further awareness of editing staff regarding personal data protection;
- Restrict access to survey data only to editing staff.
- Restrict access to editing staff solely to projects they collaborate on.
- Limit the work of editing staff to equipment exclusively from the premises of the Agency (if the authorisations provide access to personal data).
- Establish additional supervision over the work of editing staff regarding personal data protection.

Even with the implementation of measures to further reduce risk at the editing staff level, a potential incident could still be an incident with a potentially high level of influence on individuals' rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of editing staff. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Editing Manager: A managerial role is necessary from the management aspect and sometimes it allows direct intervention on all projects, and thus all the data. This role implies the business need and the ability to access to the participants' responses from a large number of researches and can be identified as activity with a potentially high impact on the rights and freedoms of data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident with an influence on the rights and freedoms of individuals related to employees preparing electronic questionnaires (editing manager):

- Sign a contract with the editing manager regarding the protection of personal data;
- Increase further awareness of editing manager regarding the protection of personal data;
- Limit the work of the editing manager to the equipment exclusively from the premises of the Agency (if authorisations provide access to personal data).
- Establish additional control over the work of the editing manager regarding the protection of personal data.

Even with the implementation of measures to further reduce risk at the editing manager level, a potential incident could still be an incident with a potentially high level of influence on individuals' rights and freedoms, but it would lawfully strengthen the position of the Agency and further influence the awareness of editing manager. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Conclusion: In case of cumulative application of protection measures for each identified role in the editing phase, the potential high level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the editing manager and editing staff level. For this reason, it is necessary to apply additional technical protection measures in the process.

Coding Open Questions - Coding

Coding Team: Answers to open questions need to be structured so that they can be used for the purpose of concluding. This role implies a business need, but the coding activities are performed on pseudonymised data. This should be recognized as an activity with a potentially medium impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident with an influence on the rights and freedoms of individuals related to coding team:

- Sign a contract with coding staff regarding the protection of personal data;
- Increase further awareness of coding staff regarding personal data protection;
- Limit access of coding staff solely to projects they collaborate on.
- Disable access to personal data in the surveys.

With the implementation of measures to further reduce the risk, especially the disabling of access to the survey, a potential incident would be an incident with low impact on individuals'

rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Coding Manager: A managerial role is necessary from the management aspect, but is still being realized over the part of the process that accesses pseudonymised data. This should be recognized as an activity with a potentially medium impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident with an impact on the rights and freedoms of individuals related to employees preparing electronic questionnaires (coding manager):

- Sign a contract with the coding manager regarding the protection of personal data;
- Increase further awareness of coding manager regarding personal data protection;
- Disable access to personal information in surveys.

With the implementation of measures to further reduce the risk, especially the disabling of access to the survey, a potential incident would be an incident with low impact on individuals' rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Conclusion: In case of cumulative application of protection measures for each identified role in the coding phase, the potential low level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the level of coding manager and coding staff. For this reason, it is necessary to apply additional technical protection measures in the process.

Analysis of data - Data Analysis

Data Analysis Team: Prepared data is analysed on various bases using statistical tools. This role is conditioned by business, but analysis activities are carried out on pseudonymised data. This should be recognized as an activity with a potentially medium impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident impacting the rights and freedoms of individuals related to staff in the Analysis Team:

- Sign a contract with analysis team regarding the protection of personal data;
- Increase further awareness of analysis team regarding the protection of personal data;
- Restrict access to analysis staff solely on projects they collaborate on.
- Disable access to personal information in surveys.

With the implementation of measures to further reduce the risk, especially disabling access to data in the survey, a potential incident would be an incident with low impact on individuals' rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Data Analysis Team Manager: A managerial role is necessary from the management aspect, but is still being realized over the part of the process that accesses pseudonymised data. This should be recognized as an activity with a potentially medium impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident with an impact on the rights and freedoms of individuals related to employees preparing electronic questionnaires (data analysis manager):

- Sign a contract with the data analysis manager regarding the protection of personal data;

- Increase further awareness of Data Analysis Manager regarding the protection of personal data;
- Disable access to personal data in surveys.

With the implementation of measures to further reduce the risk, especially the disabling of access to data in the survey, a potential incident would be an incident with low impact on individuals' rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Conclusion: In case of cumulative application of protection measures for each identified role in the data analysis phase, the potential low level of impact in the event of an incident on the rights and freedoms of the data subjects would be possible at the level of department manager and staff.

Phase 4: Data Processing - Qualitative Research

In the process of data processing, the Agency prepares and processes data using its client or own infrastructure.

When the Client in accordance with the responsibilities from Phase 1 (Sales) and Phase 2 (Preparation of Research), is Controller, unrelated to the status of the Agency in Phase 3 (data collection):

- The Agency is a processor: in case of using client infrastructure (servers, applications, etc.) and cannot with reasonable efforts technically access personal data. In the aforementioned case it may only be liable for the possible failure of employees in the process of data processing.
- The Agency is a joint manager: in case the Agency uses its own infrastructure (servers, applications, etc.) through which it is technically able to access the personal data of the data subjects. In the aforementioned case, the Agency may only be liable for the possible failure of employees in the processing of data.

The Agency is the Controller: when in accordance with Phase 1 and Phase 2 it is already fulfilling the role of the controller and using its own infrastructure (servers, applications, etc.) through which it is technically able to access the responses of the data subjects and it is liable for possible failure of employees in the data processing phase.

Processing phase for qualitative research includes the activities of transcription and subsequent data analysis.

Making transcripts

In research projects where responses are (usually) collected from a smaller number of participants for the purpose of initial or detailed review of the data subjects, it is necessary to transfer responses to the electronic form for appropriate subsequent data analysis. Mentioned activity is carried out by transferring the interview - creating transcript.

In the transcript phase, the anonymisation of the data of the data subjects is carried out in such a way that when the transcripts are made exact names of persons are encoded in the form of Person 1, Person 2 or the like.

Transcriptionists: Transcriptionists transfer conversation to text for subsequent text processing. This is why the transcriptionist needs to access the records of qualitative research. The mentioned activity is necessary for the execution of the service, and cannot be avoided.

- In case of an incident at the transcriptionist level the incident could have a potentially high level of influence on individuals' rights and freedoms. The impact of the qualitative research is limited by a smaller number of data subjects and thus with a smaller number of potential data subjects. However,

the impact can be significant due to the fact that qualitative surveys in a large number of cases are recorded. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the transcription team:

- Sign a contract with transcriptionists regarding the protection of personal data;
- Increase further awareness of transcriptionists related to the protection of personal data;
- Apply measures of reduced identification of data subjects in the moderation phase (eg, naming only by name (no surnames).
- Restrict access to personal transcripts data exclusively to projects they collaborate on
- Restrict access to transcripts recordings exclusively in audio format.
- Providing access to video format exclusively in the case of reconstruction of communication.

With the implementation of measures to further reduce the risk at the transcriptionist level, a potential incident would represent the incident with a medium level of impact on individuals' rights and freedoms. Additional technical measures for the protection of personal data should be applied to further minimize the impact of the incident.

Transcriptionist Manager A managerial role is necessary from the management aspect and sometimes allows direct intervention on all projects and thus all data. This role implies the business need and the ability to access the participants' responses from a larger number of researches and needs to be identified as activity with a potentially high impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to the transcriptionist manager

- Sign a contract with the transcriptionist manager regarding the protection of personal data;
- Increase further awareness of transcriptionist manager regarding the protection of personal data;
- Limit the work of the transcriptionist manager to the equipment exclusively from the premises of the Agency.
- Establish additional control over the work of the transcriptionist manager regarding the protection of personal data.

Even with the implementation of measures to further reduce the risk at the transcriptionist manager level, a potential incident could still be an incident with a potentially high level of influence on individuals' rights and freedoms, but lawfully reinforce the position of the Agency and further influence the awareness of transcriptionist manager. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Conclusion: In case of cumulative application of protection measures for each identified role in the process of qualitative research, an incident with a potentially high level of influence on the rights and freedoms of the data subjects would be possible with the transcriptionist manager. Potential incidents with transcriptionists need to be minimized and limited to a medium level of impact on the rights and freedoms of the data subjects. For this reason, it is necessary to apply additional technical protection measures in the process.

Analysis of collected data

The analysis of the collected data is carried out for the purpose of preparing for reporting on research findings. Data analysis is performed on anonymised data obtained through transcripts.

* In a small number of cases that are caused by a direct client request (shorter reporting period) it is possible for a researcher to have access to recordings made during data collection. This should be recognized as an activity with a potentially high impact on the rights and freedoms of the data subjects. This level of risk is not acceptable and additional risk mitigation measures are necessary.

Measures to further reduce the risk of an incident affecting the rights and freedoms of individuals related to data processing:

- Sign a contract with researchers who have access to recordings regarding the protection of personal data;
- Increase further awareness of researchers who have access to recordings regarding the protection of personal data;
- Restrict access to recordings to the researcher solely on projects they collaborate on
- Possibly restrict access to recordings in audio format.

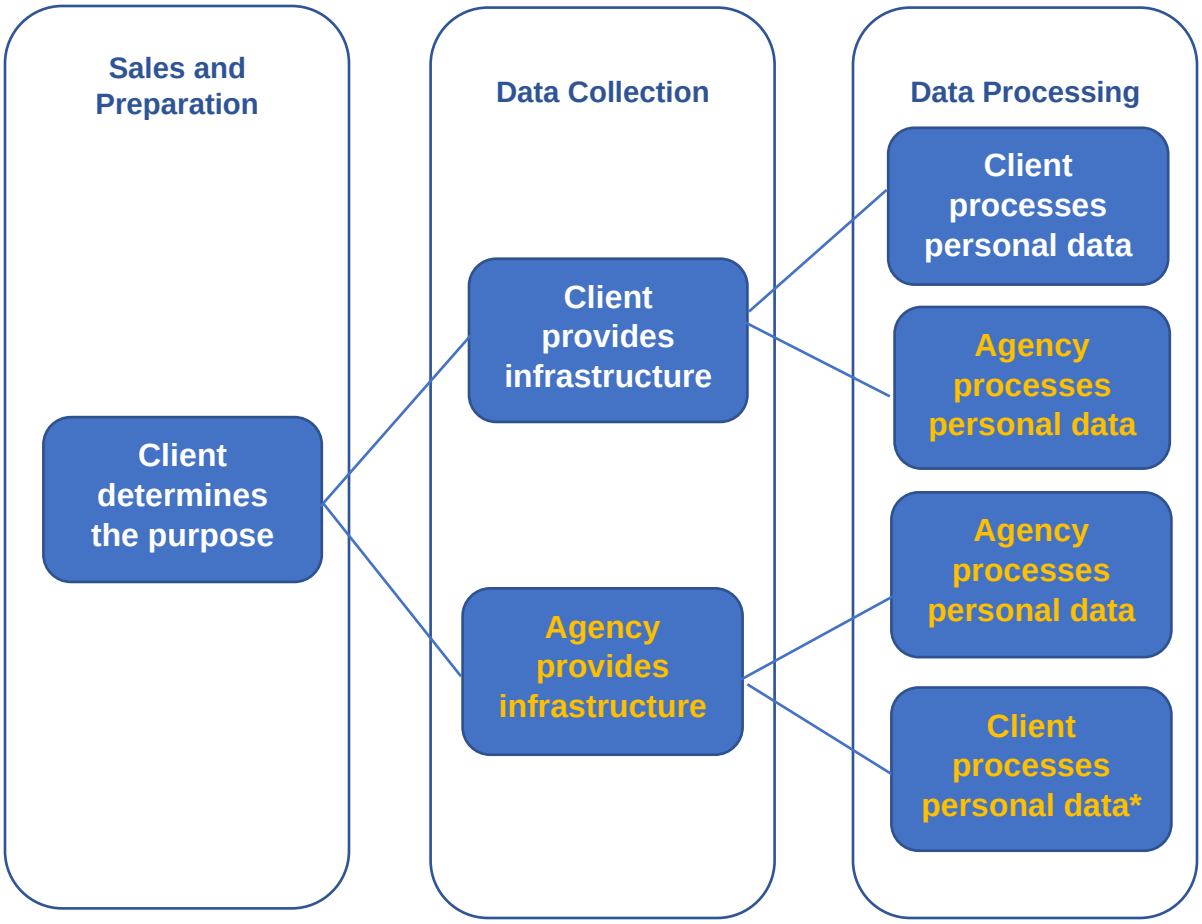
With the implementation of measures to further reduce the risk at the researcher's level, especially limiting access to audio format, a potential incident would be an incident with a low-level impact on individual's rights and freedoms. In the case of video footage, a potential incident would represent an incident with a high level of impact on individual rights and freedoms, but lawfully reinforce the position of the Agency and further influence the researcher's awareness. For this reason, it is necessary to apply additional technical measures for the protection of personal data.

Stage 5: Reporting

In the reporting stage, personal data of the data subjects are not used, but they are used in anonymised form as a basis for the purposes of the conclusion and reporting.

Determining roles and responsibilities of the Agency and the client

Example: The client determines the purpose and method of processing data (initial controller)



Infrastructure consists of Servers / Applications / Databases; does not apply to laptops / workstations

* It should not be allowed without explicit consent of the data subject (ESOMAR RULES)

Example: The agency itself determines the purpose and method of processing the data

Legend:

White = Client is the controller/ Agency is the processor

Orange = Client is the controller/ Agency is a joint controller

Red = Agency is the controller

Technical protection measures

With the implementation of organizational measures, Agencies must establish and apply a minimum level of technical measures to protect the personal data of the data subjects and other personal data, taking into account the achieved level of technological development, the costs and the type of data to be protected.

Minimum technical measures have been set below for each protection element. At least one technical measure has to be applied from each element. Cumulative application of technical protection measures for each element ensures a sufficient level of protection for the collection and processing of any type of personal data including special categories of personal data.
It is recommended to an Agency to introduce a larger number of suggested or additional technical measures per each element of protection, especially when collecting a large number of personal data including special categories of personal data.

* For additional technical measures that the Agency may introduce for each element of protection, it is possible to consult the current revision of ISO / IEC 27001 or other standards in the field of information security.

Building / house

Access to the Agency's premises must be limited, and fire protection / workplace safety measures must be applied.

- For the purpose of limiting unauthorized access, it is possible to apply a solution or a combination of solutions, for example
    - video surveillance
    - physical protection
    - alarm
    - passage control system
    - security door
    - a limited distribution of input keys
- Unauthorized persons must not be allowed movement on agency's premises without escort.

Archive

- Room / rooms containing personal data stored in printed form for a longer period of time (completed surveys for the completed project) must be locked.
- Access to the Archive should be limited by applying a solution or combination of solutions, for example
    - video surveillance
    - alarm
    - passage control system
    - security door
    - limited distribution of input keys
- It is necessary to establish and apply records of input / output of the material into the Archive.

Server room / server closet / communication cabinet

- A room with server / communication equipment (or a server / communication cabinet itself, if there is no separate room), must be locked.
- Access to the server room has to be limited by applying a solution or combination of solutions, for example
    - video surveillance
    - alarm
    - passage control system
    - security door
    - limited distribution of input keys
- Access to server / communication facilities to persons who are not employed by the Agency is allowed only with the escort of an authorized person.

Other rooms (e.g. work rooms)

- Personal data of data subjects who may be located in other premises in the Agency must be stored in a way that they are not directly accessible to unauthorized persons.
- At the end of working time, personal data must be stored in a way that they are not directly present at the desks.
- Workstations are not allowed to keep personal data of the data subjects for completed projects

Network

- The Agency should establish a limited access to its own network isolated from the public network.
    - Each user should have their own profile for access to the network.
        - The same must apply to all users with a higher access level
    - An advanced password management policy at the network level needs to be established and implemented.
    - Access to the local network from a separate location must be limited by a secured VPN.
- The Agency must manage the process of changing the access rights to the network or its part.
    - The assignment / revocation / change of the right of access to the employees must be confirmed by the authorized person (mail / ticket / document) prior to the change / implementation of the right.
- Vulnerability scanning at the network level needs to be established and implemented regularly.
- Anti- virus protection at the network level must be established and the same must be updated daily
    - All e- mails must be checked for malicious programs.

Applications and Databases

If in the application / database (hereinafter "Applications") it is possible to link the personal data of the data subjects and / or the answers of the data subjects, the answers are considered personal data.

- Applications must enable the fulfilment of participants' rights (independently or with an administrator intervention).
- Applications that contain personal data need to be protected by applying one or more protection measures.
    - The application must contain minimally administrator and specific user roles that have restricted access to personal information.
    - The minimum level of protection should allow minimally individualized access by using user / password authentication with the use of complex passwords.
    - Personal data in the application must be encrypted with a minimally 128-bit encryption.
    - For applications that are exposed to external networks, it is necessary to have regular scans and enhancements in order to reduce their vulnerability.

- The application must ensure the implementation and supervision of at least one or more protection measures
    - In order to prove the fulfilment of the rights of the data subject in the Application, the log management system should be enabled and supervised.
    - Application access logs must be collected
    - Logs for downloading personal data must be collected
    - Intervention logs on the Application or Database must be collected.
        - Each intervention must be approved by the authorized person and recorded with the keeping of records / logs for at least 24 months.
- Personal data from the application must be deleted after the survey has been conducted no more than 12 months after the completion of the research project.
    - If this is not in contravention of quality requirements or contractual obligations, it is suggested to delete personal data from the Application immediately upon download and verification at the editing stage.
- When internally developing applications, it is necessary to apply the principles of technical data protection and integrated data protection.

Data transfer

- The use of unauthorized (personal) e-mails by employees is not permitted.
- Files that contain personal data in the transfer should be protected during the transfer.
- It is recommended to use SFTP data transfer protocol or other security measures (HTTPS or so).
- If personal information is sent via public service (WWW) then the file must be encrypted with minimally 128 bit encryption.
- For the delivery of the key allowing access to the file, it is necessary to submit it via another channel (e.g. by SMS).

* The Agency should refer its clients to apply minimal security measures related to the transfer of personal data.

Data storage and archiving systems

- Personal data collected during the research projects should be kept as short as possible, i.e. for the time needed to carry out the project's purpose.
    - Personal data that can be used for the purpose of proving the levels of quality control applied should be stored for a minimum of 12 months and maximum 24 months in accordance with the quality assurance requirements
    - By contract, a client may require to archive the information for a longer period of time.
    - If the backup system is not technically advanced at the level to ensure that the data is extracted or deleted from the archive based on the request of the data subject, then internal rules should be established to ensure restriction / deletion of personal data immediately after restoring the data from the storage system.

Computers

- Access to the personal computer under the supervision of the Agency must be limited by the use of advanced password management policy.
- All computers in the Agency must have an automatic locking procedure implemented in case of longer inactivity or departure from the workplace.
- Notebooks or their part where personal data may be stored must be encrypted.
- Stationary computers or their part where larger amounts of personal data may be stored must be encrypted.
    - It is recommended that computers used in data processing, especially for scripting and editing activities, are stationary computers.

- It is not recommended to use the BYOD policy (bring your own device). If the BYOD policy is applied, the Agency is obliged to ensure the same level of protection on the given computer as it is on its own computers.
- USB and similar media that are not supervised by the Agency must be reviewed for protection against malicious software before use.
- It is recommended to avoid using or controlling the use of USB or similar portable devices and methods for transferring files with personal data.
    - It is especially recommended to restrict the use of USB or similar portable devices and methods for scripting and editing activities.

Computers for data collection

- Stationary devices located in the Agency that are used for data collection and where personal data may be located for technological processes must be protected minimally by a password.
- The laptop / tablet devices used to collect data that may contain personal data must be completely encrypted or limited encryption may be implemented where personal data may be present.
    - The access to the portable device must be limited minimally by a password.

Subcontracted associates

For the purpose of carrying out a contractual obligation towards the client - the implementation of the research project or the operational implementation of the research project involving the participation of the Agency as a controller and / or joint controller and / or processor, the Agency may cooperate with a large number of natural and legal persons - processors.

The Agency is required to ensure that external associates who have access to personal data have signed a confidentiality agreement regarding personal data collected during the research process prior to access to personal data.

If this subcontracted processor fails to comply with the data protection obligations, the Agency remains fully responsible to the controller for the performance of the obligation of the said processor.

Subcontracted Agencies

In case of subcontracting, the Agency is required to engage joint controllers or processors who adequately safeguard the implementation of appropriate technical and organizational measures in such a way that processing is in accordance with the requirements of this Regulation and that it protects the rights of the data subject.

The Agency may subcontract the execution of part or all stages of processing in the research process with other Agencies that:

1. accept (in writing) to conduct all stages of the research project research in accordance with this Code.
2. are certified (Article 42 according to the accredited procedure) for activities that are covered by subcontracting.
3. in other way, sufficiently guarantee the implementation of appropriate technical and organizational measures in such a way that the processing is in accordance with the requirements of this Regulation and that it protects the rights of data subjects.

The Agency is required to carry out an analysis / audit of the business processes of the Subcontracted Agency prior to the transferring work of personal data processing.

- The Agency can accept positive findings from paragraph 1 and 2 as a positive result of business process analysis.
- The Agency is required to carry out additional monitoring of Subcontracted Agency in the event that findings from paragraphs 1 and 2 are not positive.

If the business process analysis indicates that the processing would not comply with the requirements of this Regulation and does not ensure the protection of the rights of data subjects, the Agency may then request the execution of additional technical and organizational measures for the purposes of the research project or withdraw from the cooperation with the said Agency.

The Agency is required to inform the controller of the engagement of another agency with an access to personal data and it is required to get approval for the said engagement.

Subcontracted (external) researchers

The agency may contract external researchers for capacity or specific expertise.

The Agency is required to limit or disable, when possible, access to personal data of data subjects to subcontracted researchers.

Exceptions are research projects "in the scope of qualitative research" where, for a project type, the researcher as a moderator or project manager directly approaches the data subjects.

The Agency is required to inform the controller of the engagement of external researcher / specialist with an access to personal data and it is required to get approval for the said engagement.

Subcontracted interviewers, recruiters, quality control managers

The agency can engage a larger number of external associates - interviewers, recruiters, quality control managers and coordinators for data collection that are involved in the process of collecting responses from data subjects.

The mentioned practice is market-driven and clients give general consent for the use of interviewers, quality control managers, coordinators for the needs of the project by contracting the activities with the Agency in accordance with this Code.

The Agency is required to provide technical and organizational prerequisites for the work of the interviewer at minimum of:

- A confidentiality agreement has been signed regarding the personal data collected during the research process.
- Assigned / used portable devices must be equipped to the minimum technical requirements (See Computers for data collection, Computers).

Clients

In the sales phase that includes the contracting process, the Agency is required to point out to the client the existence of the Code of Conduct and that the Code will be applied in the work of the research project.

The client and the Agency must establish the relationship between the parties involved in accordance with the Regulation and the accompanying legal regulations.

If, in an agreement between the Agency and a client, a specific item is not specified in the offer / contract / supplement, then the rules set forth in this Code apply. Binding Offer, Contract or Supplement must include the following items:

Obligatory elements

- Determining research purposes.
- Responsibilities of each side for key research phases.
- Determine the ownership of the infrastructure that will be used during the project (servers, applications, etc.).
- Determining the position of each party in the contract (controller, joint controller, processor)
- Determining the category of personal data that will be processed for the purpose of the contract
- Period of retention of personal data (if it has not been established then it can be kept up to 24 months from the survey).
- List of external associates (if they are known before the start of the survey) and approval for use.
- Agency’s requirement to bind its employees to respect confidentiality and protection of personal data.
- Agency's requirement to bind its sub-contractors to respect confidentiality and protection of personal data.
- Rules of Procedure in the case of personal data breach with significant impact on data subjects;
- Definitions / Dictionary applied in the Contract
- Identification of applicable legislation

In case the Agency is processor

- The Agency's requirement to process personal data only according to the instructions of the controller.
- Requirement to delete or return all personal data upon completion of the processing by the Controller and deletion of the existing copy unless, in accordance with the law of the Union or the law of the Member State, there is an obligation to store the personal data or a limitation established by this Code.
- The Agency's requirement to, taking into account the nature of the processing, help the controller, through appropriate technical and organizational measures, the controller fulfils as far as possible the requirement for exercise of the rights of the data subjects.
- The Agency's requirement to assist the controller in ensuring compliance with obligations under Articles 32 to 36, taking into account the nature of the processing and the information available to the processor;
- The Agency's requirement to provide the Controller with all the information necessary to demonstrate compliance with the obligations laid down in this Article and which provides for audits, including inspections, carried out by the Controller or by another auditor authorized by the controller and contribute to them.
- Requirement of the controller (client), taking into account the nature of the processing, to assist the Agency as much as possible, to fulfil its own obligations in answering requests to exercise the rights of the data subjects.

If required, the client can determine / request

- Additional requirements for personal data processing
- List of implemented organizational and technical measures and the obligation to use them.
- Identification of possible transfer of personal data from the Agency to the Republic of Croatia, in the EU or outside the EU. The agency must clearly refer the client if the personal data will be transferred outside the EU.

Data Protection Officer

The Agency acting in accordance with this Code has to designate the Data Protection Officer.

The Data Protection Officer must sign a confidentiality contract with the Agency.

A Data Protection Officer may be employed by the Agency or perform tasks under a work contract.

A number of Agencies may appoint one Data Protection Officer, and the Officer must be easily accessible from every business establishment and must not be in conflict of interest.

The Data Protection Officer must have at least five (5) years of experience in the area of market, media and public opinion research or have relevant experience in the field of personal data protection.

The Agency communicates the contact details of the Data Protection Officer to the Supervisory Authority and publishes it on its website and other media as appropriate.

The contact details of the Data Protection Officer contain the minimum of the following items

- Name
- Surname
- E-mail
- Telephone (and / or mobile)
- Address

Responsibilities and Authorizations of Data Protection Officers

The Agency is required to include Data Protection Officer in all cases with potential impact on personal data that are not processed by this code.

In carrying out activities in the Agency, the Data Protection Officer works on orders and for the needs of the Management Board

- The Data Protection Officer must have access (upon request) to all processing procedures.
- The Data Protection Officer must plan and implement education with the purpose of maintaining knowledge of the regulations and special knowledge relating to the protection of personal data in the area of market, media and public opinion research.
- The Data Protection Officer may also perform other duties and duties that do not lead to conflicts of interest

Data Protection Officer of the Agency performs at least following tasks

- Plans, implements and / or supervises the execution of education and awareness raising activities of the employees and associates of the Agency. It also conducts and / or oversees the assessment of the success of the training.
- Establishes and supervises the fulfilment of the records required by the Regulation, the Law, the Code, the internal rules and procedures of the organization and / or the interested parties.
- Participates in each additional assessment of the effect on data protection that is not foreseen and processed by this Code.
- Coordinates, plans, implements and / or supervises the implementation of internal and external audits of personal data protection, including auditing by the supervisory authority.
- Coordinates communication activities with all interested parties.
- Monitors compliance and enforcement of the requirements of the Regulation, the Law, the Code, the interested parties and internal policies and procedures of the organization associated with the processing of personal data.
- Monitors in cooperation with other employees of the organization the compliance of the Agency's requirements by external associates.
- Participates in the process of reporting personal data breaches.
- At least once a year, reports to the Management Board on the status of all the above activities and suggests activities to improve the existing situation.

The Data Protection Officer may conduct this activity alone, with the assistance of other staff members or external associates.

Records of processing activity

The Data Protection Officer establishes a record of all data processing that is carried out for the purpose of research projects and supervises the proper filling the record by the Agency staff.

The record must be in writing, including electronic form, and must be easily accessible.

Records must include processing in which the Agency acts as a Controller, a Joint Controller, or a Processor.

The Agency may, if necessary, provide access to part or all of the Record to the supervisory authority (it must be done for official request), the Controller or the Joint Controller, the processor, and other interested parties, including certification authorities.

Minimal processing records' elements for the controller

(a) the name and contact details of the controller and, where applicable, the joint controller, controller representative and data protection officer;
(b) processing purposes;
(c) a description of the category of participants and categories of personal data;
(d) recipient categories to which personal data are disclosed or will be disclosed, including recipients in third countries or international organizations;

(e) where applicable, the transfer of personal data to a third country or an international organization, including the identification of that third country or international organization, and, in the case of transfers referred to in Article 49 Section 1, second subparagraph (EU Regulation 2016/679) documentation of adequate protective measures;
(f) where possible, the time limits for deleting different categories of data;
(g) where possible, a general description of technical and organizational safety measures

Minimal processing records' elements for the processor

(a) the name and contact details of one or more processors and any controller on whose behalf the processor acts and, where applicable, the controller's representative or processor and the data protection officer;
(b) processing categories performed on behalf of each controller;
(c) where applicable, the transfer of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of a transfer referred to in Article 49 Section 1 paragraph (h), documentation of adequate protective measures;
(d) where possible, a general description of the technical and organizational safety measures

Records and reporting of personal data breaches

The Data Protection Officer establishes a Record of Personal Data Breaches and supervises the proper filling of record by the Agency's employees.

The record of personal data breaches must contain

1. Name and contact information of the data protection officer
2. Project number and title (or other identifier of the case where personal data breach occurred)
3. The name of the data processor
4. The names of the data processors involved
5. The type of research project in which the breach was established
6. Phase of a research project where a breach has been established
7. List of Employees / Associates in the Agency involved in the breach of personal data
8. Description and context of personal data breach
    a. Categories and approximate number of data subjects concerned
    b. Categories and approximate number of personal data records in question
9. Description of likely consequences of personal data breaches
10. Assessment of the impact on individuals' rights and freedoms
    a. It does not represent a high risk for an individual's rights and freedoms
    b. It represents a high risk for individuals' rights and freedoms
11. Description of planned and undertaken measures to address the problem of personal data breaches, including, where appropriate, measures to mitigate its harmful consequences

Records on personal data breaches are kept for at least five years.

The Data Protection Officer prepares a report on personal data breaches if there is a high risk of individuals' rights and freedoms.

The Data Protection Officer reports to the Director / Management Board at least once a year on the record of personal data breaches and planned and undertaken measures.

The Data Protection Officer reports to the Director / Management Board about entry in Record of Personal Data Breaches if there is a high risk to the individuals' rights and freedoms.

The Data Protection Officer coordinates communication channels of the Agency, the supervisory authority, data subjects and the controller

Reporting to the supervisory authority

If a breach of personal data is likely to cause a risk to the rights and freedoms of individuals, the data protection officer without unnecessary delay and, if feasible, no later than 72 hours after knowledge of the breach, reports to the supervisory authority competent pursuant to Article 55 of personal data breach. If the reporting is not done within 72 hours, it must be accompanied by the reasons for the delay.

The personal data breach report must contain

- the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, and the approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer or other contact point from which further information can be obtained;
- probable consequences of personal data breach;
- measures taken or proposed by the controller to address the problem of personal data breach, including, where appropriate, measures to mitigate its possible harmful consequences.

The report before the reporting of the supervisory authority must be approved by an authorized person in the Agency.

Notification of data subjects - in case the Agency is Controller

Data Protection Officer prepares (The personal data breach report) for informing data subjects in case of personal data breach related to the research process that is likely to cause a high risk to individuals' rights and freedoms and if no technical and organizational measures have been applied which make personal data incomprehensible to any person who is not authorized to access them.

The personal data breach report contains the minimum of the following items

- Name and contact information of the personal data protection officer
- Description of likely consequences of personal data breaches
- Description of planned and undertaken measures to address the problem of personal data breaches, including, where appropriate, measures to mitigate its harmful consequences

The report before the notification of data subject must be approved by an authorized person in the Agency.

Informing data subjects about the nature of personal data breaches, which is likely to cause a high risk to individuals' rights and freedoms, the Agency may communicate by using clear and simple language with one or a combination of the following communication channels:

- Directly involved data subjects,
- Public notification to data subjects through their own web site,
- Public notification via other means of public disclosure
- Other method, if the supervisory authority decides so.

The implementation of the notification about the breach of participants’ personal data is monitored by Data Protection Officer.

Reporting to (Joint) Controller

If the breach of personal data is likely to cause a risk to individuals' rights and freedoms, the data protection officer reports to the (joint) controller without unnecessary delay.

The personal data breach report must contain

- the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, and the approximate number of personal data records concerned;

- the name and contact details of the Data Protection Officer or other contact point from which further information can be obtained;
- probable consequences of personal data breach;
- measures taken or proposed by the controller to address the problem of personal data breach, including, where appropriate, measures to mitigate its possible harmful consequences.

The report before the reporting of the controller must be approved by the Authorized Person of the Agency.

Processing records for which a separate impact assessment was performed on the protection of personal data

The Agency must establish and maintain records of all research projects in which an impact assessment is carried out on the protection of personal data of the data subjects, which is not covered by this Code.

The record must be in writing, including electronic form, and must be easily accessible.

Records must include the processing in which the Agency acts as a Controller or Joint Controller.

The Agency may, if necessary, provide access to part or all of the records to the supervisory authority (it must be done for official request), the Controller or the Joint Controller, the processor, and other interested parties including certification authorities. Depending on the type of supervision, the Agency should ensure the identification of persons and organizations who have access to Processing Record or the process itself.

The lawfulness of processing

In order for the Agency to lawfully process personal data, a minimum legal basis must be met for processing.

The controller must choose the most appropriate legal basis for data processing.

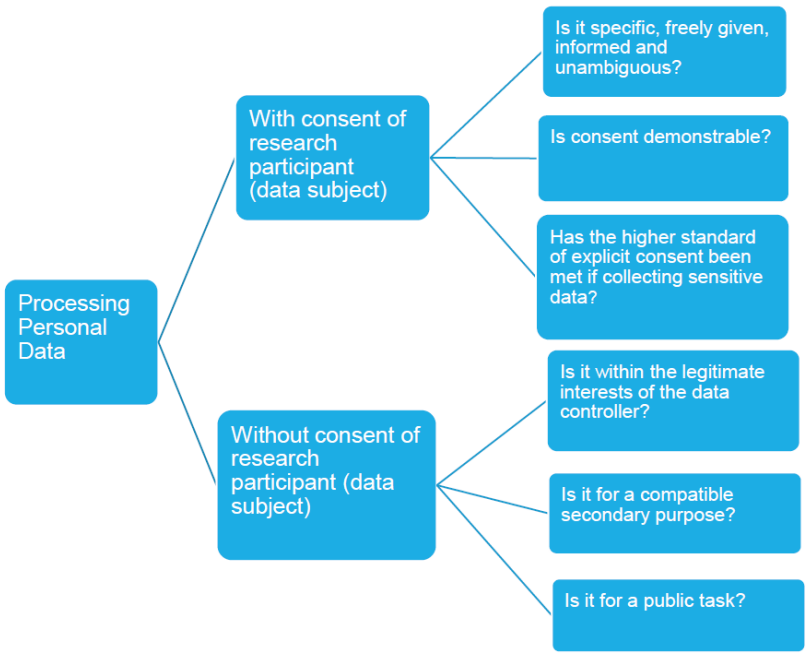
- If the client is controller, he must choose the legal basis for processing the data.
- The Agency is required to refer the client to any doubt on the legal basis.

In general, legal bases in the market research process that can be used to process personal data are:

1. Consent of data subjects for processing their personal data for research purposes;
2. Legitimate interests of the Controller (or third party)
3. Performing a public interest task or performing the official authority of the controller

Picture[5]

Figure 6 Decision Making Tree



Consent

If consent for the processing of personal data has been selected as the legal basis for the processing of personal data, the controller must ensure that the consent is given by a clear acknowledgment of the freely given, specific, informed and unambiguous consent of the data subject for processing of personal data relating to him or her.

- The statement of the data subject must be presented in a comprehensible and easily accessible form, using clear and simple language.
- Before giving consent, the data subject must be informed of the possibility to withdraw the consent at any time.

[5] Appropriate use of different legal bases under the GDPR June 2017

- In order for the data subject to be able to give the consent informed, the identity of the controller and the processing purpose for which personal data will be used should be presented to him or her.

The controller must be able to prove that data subject has given consent for processing his or her personal data for the purpose of research, by a written statement, including an electronic or oral statement.

- Silence, pre-ticked mark (or similar), marked field or inactivity is not considered a consent.
- If the data subject gives a consent in a written statement regarding other issues, the request for the consent must be presented in such a way that it can be clearly distinguished from other questions.

If the controller does not obtain consent of data subjects for processing their personal data for research, then the (potential) participant must not participate in the research.

- Consent should cover all processing activities carried out for the same purpose or purposes.
- When processing has multiple purposes, the consent should be given for all of them (e.g., a consent to participate in the survey, and an additional consent for the purpose of participating in another research).

The child's consent

Processing child's personal data is lawful if the child is at least 16 years old.

If a child is below the age of 16, processing is considered lawful only if the person with parental rights has given consent or approved it.

The Agency must make reasonable efforts to ascertain whether or not the consent has been approved by the parent responsible for the child, taking into account the available technology.

Consent in the processing of special categories of personal data

The Agency may process special categories of personal data for one or more specific purposes only if the data subject explicitly gives a consent for processing such personal data.

The Agency may process special categories of personal data for one or more specific purposes if it is apparent that the data subject has disclosed them.

Consent when interviewing by telephone

Due to the nature of telephone interviews, it is not feasible for the data subject to read the full text of consent before the interview. After presenting the basic information of the research, and the key rights of data subjects including the right to withdraw consent. In addition to the mentioned, participant should refer to the website of the Agency's Privacy Policy, with a detailed description of the rights of data subjects, as well as contacts for the purposes of communication, objection or other requests.

In the event that a conversation with the participant is recorded, for the purpose of subsequent quality control, and in order to prove the existence of consent by the participants of the research, it is necessary to make it clear at the beginning of the interview.

For the purpose of proving the consent, the record is kept to a minimum time while there is a need for personal data storage and a maximum of 2 years from the interview.

Consent when interviewing by web

Due to the nature of web surveys and limited interfaces, it is not feasible to present the full text of consent to data subject before the survey itself. Prior to conducting the survey, is required to present the participant of the research his / her minimal rights and right to withdraw consent. In addition to the mentioned, participant should refer to the website of the Agency's Privacy Policy, a detailed description of the rights of data subjects, as well as contacts for the purposes of communication, objection or other requests.

The Agency is required to note the acceptance of the consent and to keep them for need of proving their existence for the minimum time there is a need to store the personal data and a maximum of 2 years from the interview.

Withdrawing consent

The data subject has the right to withdraw its consent at any time.

The withdrawal of consent of data subject must be just as easy as giving it.

When withdrawing a consent, the data subject is required to confirm his/her identity to the Agency.

The withdrawal of the consent does not affect the lawfulness of processing based on consent prior to its withdrawal.

The Agency is required to exclude and delete the data of the data subjects if they are available.

If a data subject requests deletion of personal data once they are already anonymised (e.g., statistically processed for reporting purposes), the data cannot be excluded from the report.

The Agency must keep evidence of the withdrawal of the consent of data subjects for at least two years and a maximum of five years from the research project to which they relate.

Possible examples of using consent in research projects

- Quantitative or qualitative research based on random selection of subjects
- Surveys on data subjects panel
- Online research
- Research by media audiences
- Customer satisfaction research (not based on existing client databases)
- Demographic segmentation based on research projects
- Research based on tracking data collected in the digital environment

Legitimate interest

The Agency may conduct research projects based on the legitimate interests of the Controller (or third party) unless such interests are overridden by the fundamental rights and freedoms of the holders of data subjects

In determining legitimate interests, it is necessary to ensure the balancing of the controller's interest with any breach of rights and freedoms or interests of the data subjects. Procedure for determining legitimate interest and balancing decisions:

1. *Determine whose has legitimate interest (example)*
   - Legitimate client interest when research projects are conducted on the data subjects from the internal client database. It is important to emphasize that the client is required to decide whether it is possible to choose a legal basis, in this case a legitimate interest, as the criterion for conducting the research.
   - Legitimate interest of the Agency that contacts data subjects for the purpose of the quality control of the collected data in accordance with the requirements for quality assurance.
2. *Determine whether processing is necessary to achieve interest*
   - It is important to consider the proportionality of the processing. Can goals be achieved by collecting less data?
   - Are there more resources to increase privacy for that purpose (additional consents, encryptions?)
3. *Balancing the interests of the controller with the interests of the data subjects*
   - Evaluate whether the interest of the controller is overridden by the fundamental rights and interests of the data subject.

- It is important to consider the impact on data subjects; the way data is processed and the reasonable expectations of the data subjects.

4. *Documentation of Balancing Decision*
    a. it is necessary to document the reasons on which the conclusions of the balancing process are made (GDPR accountability principle)

Legitimate interest of the Agency for the purpose of quality control

This Code of Conduct confirms the legitimate interest of the Agency to be able to (subsequently) contact the data subjects in accordance with quality assurance standards in the area of market, media and public opinion research.

- Data subjects need to be informed about the possibility of quality control activities so that they can expect processing for this purpose.
- The Agency is required to establish and apply internally approved work control procedures for all types of research projects in accordance with quality assurance standards in the field of market research.
    - Agency control procedures must establish minimum and maximum levels of quality control.
- For the purpose of ensuring compliance with quality assurance norms in the area of market, media and public opinion research, the Agency is required to keep records of the implementation of quality control for a minimum of one year and a maximum of two years.

Possible examples of using legitimate interest in research projects

- Customer satisfaction survey (on existing customer databases).
- Quantitative or qualitative research with the use of client databases.
- Analysis of data from loyalty card.
- Research using existing data sets or third-party data (i.e. data that is not directly obtained by an individual or where there are no contractual relationships) such as social media analysis.

Performing a public interest task or executing the official authority of the controller

An agency conducting research for the purposes of performing a public interest task or carrying out the official authority of a controller works exclusively by an order and is not responsible for determining the legitimate interest of the controller.

Definitions

Client means any individual or organization that requires, conducts or subscribes to all or any part of the research project.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

A recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**;**

Biometric data means personal data obtained by special technical processing relating to physical characteristics, physiological characteristics, or characteristics of an individual's behaviour that allow or confirm the unique identification of that individual, such as face or dactyloscopic data

Data concerning health means personal data related to an individual's physical or mental health, including providing health services that provide information on his or her health status;

Enterprise means a natural or legal person engaged in economic activity, regardless of the legal form of such activity, including partnerships or associations that regularly engage in economic activity

Agency means an enterprise whose primary activity is market, media and public opinion research.

A group of undertakings means a controlling undertaking and its controlled undertakings

Binding corporate rules means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

A relevant and reasoned objection means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft

decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Primary data implies data collected by a researcher from an individual or about an individual for research purposes. Primary data may contain personal data.

Secondary data implies data collected by a researcher from other sources. Secondary data may contain personal data.

Data Analysis means the process of examining data sets that reveal hidden patterns, unknown correlations, trends, settings, and other useful information for research purposes.

The data subject is an individual whose personal information is used or will be used in the research. For the purposes of the Code, the data subject designates an identified or recognizable natural person whose personal data will be used in the research.

Passive data collection means collecting personal data by observing, measuring or recording certain actions or behaviours.

Reporting includes any form of presentation or display of research results; which may include the preparation of reports, presentations or data sets submitted to the client as a result of the research project.

The research / research project is a systematic gathering and interpretation of information about individuals and organizations. The research uses statistical and analytical methods and techniques of applied social, behavioural and data sciences to create insights and support the decision-making process by providers of goods and services, public and state administration, non-profit organizations and the general public. The research includes all forms of market, media and public opinion research and analysis.

Investigations for statistical purposes - statistical purposes are all activities of collecting and processing personal data required for statistical surveys or for producing statistical results. Outcomes of statistical surveys result in aggregate data that is not used to support measures or decisions related to individuals. The results of statistical surveys can be used for other purposes, including scientific research.