Last updated on: October 16, 2023

Sawtooth Software values and adheres to the protection of your personal data

We believe that everyone has the right to the protection of his/her personal data, and such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access his/her data that has been collected and the right to rectify any inaccurate or incomplete information. Hence, we would like to help our customers, end users, and survey respondents to understand more about EU's General Data Protection Regulation over the data we process.

Disclaimer: We do not offer/provide legal advice, and we are not associated to any regulatory authorities. Hence, we strongly encourage you to seek advice from a Data Protection Officer, Compliance Officer, and/or General Counsel at your company/academic institute, a Supervisory Authority in your country, or an outside counsel who specializes in cross-border data protection/transfer or privacy law. Please understand that the purpose of the Q&As is to help you become familiar with General Data Protection Regulation (GDPR) and see the importance of GDPR in relation to your research/survey project.

Frequently Asked Questions about the GDPR and Your Research/Survey

These FAQs are organized into the following sections based on these core questions:

1. What is the purpose of the GDPR?
2. How does the GDPR relate to my research/survey in general?
3. What activities are subject to the GDPR?
4. I am based in the United States. Why might the GDPR affect my research/survey?
5. When one of the above applies to my research/survey, what do I need to do before I can obtain a license to access and use Sawtooth Software's product, which comes with web hosting in the US and other locations around the world?
6. If I use your software/application, who would be the data Controller, who would be the data Processor, and who would be the data subject?
7. What are the responsibilities of a data Controller?
8. What are the responsibilities of a data Processor?
9. Do data subjects have any responsibility?
10. If the GDPR applies to my research/survey, what kinds of actions my research/survey team should complete before my research/survey proceeds?
11. How is the consent documentation and process affected by GDPR?
12. If the GDPR applies to my research/survey, what practices should be part of our research/survey?
13. Why is it important to comply with the GDPR?
14. Is it possible to apply for a waiver to the application of GDPR?
15. In what countries does the GDPR apply?
16. How is UK GDPR different from GDPR?
17. What personal information does the GDPR regulate?
18. What personal data is considered sensitive and is subject to specific processing conditions under GDPR?
19. What specific processing conditions must be satisfied before the collection of personal data considered sensitive or as a special category?

20. What are some examples of data not considered personal data?

21. To which persons does the GDPR apply? Does the GDPR only apply to EEA citizens and residents?

22. If my research/survey will only involve information that is publicly available, will the GDPR apply?

23. If my research/survey will involve de-identified data, will the GDPR apply?

24. My research/survey involves animals; none of the research/survey subjects are persons. Will the GDPR apply?

25. My research/survey team will be contracting with translators and other third-party service providers. Will the GDPR apply to those persons?

26. Does the GDPR have any requirements for research/surveys involving children?

27. Does the GDPR apply to the personal information of deceased persons?

28. My research/survey team will be working with a research/survey team from a European organization that controls the research/survey. Will the GDPR apply to our work?

29. My research/survey does not involve collecting new personal information. We will be working with an existing data set. Will the GDPR apply?

30. Are there changes I can make to my research/survey protocols that will ensure the GDPR does not apply to my study?

31. What is Anonymization?

32. What are some data anonymization challenges?

33. Are there changes I can make to my research/survey protocols that will facilitate compliance with the GDPR?

34. What is a Data Protection Impact Assessment? Why is that important to my research/survey?

35. What are some data processing scenarios that “likely to result in a high risk”?

36. Can I choose which location (country/city) I want my research/survey data stored?

Questions & Answers

1. What is the purpose of the GDPR?

In accordance with the European Data Protection Board, General Data Protection Regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law that sets the standards for the rest of the world to follow and emulate, and it also harmonizes the current fragmentation in different EU national systems and reduces unnecessary administrative burdens for countries deemed adequate.

It regulates the collection, use, transfer, storing and other processing of personal information of individuals located in the EEA.

The GDPR became effective on May 25, 2018.

2. How does the GDPR relate to research/survey in general?

- It establishes the circumstances under which it is lawful to collect, use, disclose, destroy, or otherwise process "personal data."
- It establishes certain rights of individuals in the EEA, including rights to access, amendment, and erasure (right to be forgotten).
- It requires researchers/survey design team to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk of the data.
- It requires notification to data protection authorities and affected individuals within 72 hours following the discovery of a personal data breach, which is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

3. What activities are subject to the GDPR?

- Activities involving identifiable information if personal data is being collected from one or more research participants physically located in the EEA at the time of data collection (even if the participant is NOT an EEA resident).
- Activities involving the transfer of personal data collected under the GDPR from an EEA country to a non-EEA country.

4. I am based in the United States. Why might the GDPR affect my research/survey?

The GDPR inherently has extraterritorial reach and will very likely apply to your research/survey if the research/survey activities will:

- be conducted in association with an established organization in the EEA,

- involve personal information collected from any person while they are in the EEA,
- involve monitoring the behavior of persons while they are in the EEA,
- involve transferring personal information out of the EEA, or
- involve the secondary use of data that was protected by the GDPR when initially collected.

5. When one of the above applies to my research/survey, what do I need to do before I use Sawtooth Software's product, which comes with web hosting in the US and other locations around the world?

Because the US is considered a non-adequate third country and the new EU-US Framework could be invalidated for a second time, to be in compliance with GDPR, you are required to sign a Data Processing Agreement/Addendum that includes Standard Contractual Clauses. Additionally, because data will be transferred from one or more EEA countries, you should conduct a TIA as the additional supplementary measure. If your data might include sensitive personal information, you should also conduct a DPIA.

Alternatively, in the case of Lighthouse Studio (a desktop, downloadable software), you could opt to host on your own servers located in a country within the EU or considered as adequate by GDPR.

6. If we use your software/application, who would be the data Controller, who would be the data Processor, and who would be the data subject?

You would be the Controller, because you design the survey and determine purposes and means of processing personal data.

We would be the Processor, because our software/application stores, transfers, and analyzes the data collected from your surveys. However, we work with sub-processors (you may find a complete list of sub-processors at the bottom of this Q&As) and utilize their data center(s) to store your data.

Your research/survey participants are the data subjects, because their personal information is controlled by you and processed by us.

7. What are the responsibilities of a data Controller?

- Complying with data protection principles under art. 5 GDPR.
- Upholding individuals' data protection rights.
- Keeping records of processing operations.
- Ensuring the security of processing.
- Choosing an appropriate data processor.
- Detailing in a binding contract the controller-processor relationship.
- Notifying personal data breaches to the relevant EEA data protection authority and to individuals, where applicable.
- Being accountable for the processing operations, practicing data protection by design & default, carrying out data protection impact assessments when necessary.
- Appointing a **data protection officer** when necessary.
- Complying with the data protection obligations on **international transfers** of personal data.

- Cooperating with data protection authorities.

8. What are the responsibilities of a data Processor?

- Following the controller's instructions for processing controller's data.
- Keeping records of processing operations.
- Ensuring the security of processing.
- Respecting and upholding the binding controller-processor contract.
- Obtain the authorization of the controller before engaging a new sub-processor (and give the controller a possibility to object). If applicable, a processor - sub-processor contract must be put in place and equate to the initial contractor- processor contract.
- Notifying personal data breaches to data controller.
- Notifying GDPR breaches to the controller.
- Being accountable for the processing operations (e.g., practicing data protection by design & default).
- Appointing a data protection officer when necessary.
- Ensuring that international transfers are authorized by the controller and comply with the GDPR.
- Cooperating with data protection authorities.

9. Do data subjects have any responsibility?

No, GDPR and other similar data protection and privacy laws and regulations intend to protect the fundamental rights and freedoms of data subjects.

10. If GDPR applies to my research/survey, what requirements must be satisfied before my research/survey may proceed?

a. Provide GDPR informational notices for research/survey participants and other data subjects.

You must provide GDPR informational notices to prospective research/survey subjects and to enrolled research/survey subjects before any personal information is collected.

The notices must disclose what personal information will be collected, the purposes for which it will be used, whom it will be shared with, and how long it will be retained, as well as information about an individual's rights under the GDPR and how to exercise them. These requirements may be met by supplementing other notices that will otherwise be provided to individuals.

b. Obtain a consent for transferring personal information out of the EEA to the US or to another non-EEA country.

If personal information will be transferred out of the EEA, your study will be required to have a separate justification for that transfer. The US and most non-EEA countries do not meet the GDPR's privacy requirements to be exempted from this requirement.

For example, if your research/survey team will collect personal information in the United Kingdom, and then upload the personal information into a team folder, which stores information in the US, your study will need to obtain consents to this exporting of the information out of the EEA before the transfer

occurs. Other examples are using Sawtooth software outside of the US to collect survey data or storing data on a laptop and travelling with the laptop back to the US.

It's very important to understand that any consent to transfer will be separate and distinct from the informed consent required from research/survey subjects for purposes of meeting ethical standards or research/survey procedure requirements.

The GDPR requires that consent be:

- Freely given, that is, the individual has a realistic choice;
- Specific;
- Informed;
- Clear and unambiguous; and
- Affirmatively given. Pre-ticked boxes should not be used. For "special category" information, we recommend obtaining a signature (electronic or hand-written) to meet a higher requirement of an "explicit" consent.

c. For secondary uses of data sets, have a justification for processing and for transferring the personal information.

The GDPR has introduced new challenges to the secondary use of personal information related to or incorporated in research/survey data collected in the EEA or otherwise subject to the Regulation. Secondary use of such personal data requires a justification under the GDPR, as will any transfer of the personal data out of the EEA. The provider of the data set should confirm the data was collected in compliance with the GDPR and that the anticipated use by your research/survey team will also be permitted under the GDPR. The EDPB's guidance for secondary use of personal data is limited.

d. Satisfy the requirements for valid consents, if obtaining a consent (see Q&A 7).

e. Establish a plan to handle and manage the research/survey information securely.

EEA personal data must be protected from disclosure and unauthorized use (i.e., in keeping with the initial notice). Personal information may not be shared outside of the research/survey team. Technical security protections, including encryption, should be employed. Pseudonymization is strongly recommended whenever possible.

f. Obtain written confirmation from all service providers that they will act in compliance with GDPR.

If your research/survey study will use any external service providers, then you will need to obtain a commitment from them to comply with the GDPR. Examples include organizations that provide translation or enumeration services, as well as consultants.

g. Obtain the approval of the stakeholders, such as department head, privacy counsel, compliance officer, and data protection officer.

h. Include training in the GDPR's requirements for your research/survey team in your study plan.

To facilitate your study's research/survey activities, your research/survey team should be trained on how their actions will be impacted by the GDPR's requirements.

i. If necessary (i.e., when the collection of data may likely result in a high risk to the rights and freedoms of natural persons), prepare a Data Protection Impact Assessment (DPIA).

j. If any personal information will be transferred from EEA to the US, prepare a Transfer Impact Assessment (TIA).

11. How is the consent documentation and process affected by GDPR?

- Consent records, including time and date of consent, must be maintained for each subject. In the case of verbal, online, or any other type of undocumented consent, the Principal Investigator is responsible for maintaining a consent log indicating each subject (either by name or study ID number) and the date and time that they provided consent.

- Consent must be explicit. If the consent form or consent script serves multiple purposes (e.g., a consent form that is also the recruitment email), then the request for consent must be clearly distinguishable within the document.

- Each subject has a right to withdraw consent, at any time. Each subject must be informed of this right prior to giving consent. Withdrawal of consent must be as easy as giving consent.

- Consent must be an affirmative action. This means that opt-out procedures or pre-checked boxes indicating consent are not permitted.

- Consent information must be provided in clear and plain language in an intelligible and easily accessible format. Consent forms using excessive jargon or that do not have separate sections with section headings should be revised.

- Consent must be freely-given. Individuals in a position of authority cannot obtain consent, nor can consent be coerced. This means that faculty members or teachers cannot obtain consent from their own students.

- Consent forms must contain the following information:

    - The identity of the Principal Investigator;
    - The purpose of data collection;
    - The types of data collected, including listing of special categories;
    - The right to withdraw from the research and the mechanism for withdrawal;
    - Who will have access to the data;
    - Information regarding automated processing of data for decision making about the individual, including profiling;
    - Information regarding data security, including storage and transfer of data;
    - How long data will be stored (this can be indefinite); and

- Whether and under what conditions data may be used for future research, either related or unrelated to the purpose of the current study.

12. If the GDPR applies to my research/survey, what practices should be part of our research/survey?

a. Follow your study's plans for managing the personal information securely.
Throughout the study, ensure that the EEA personal information is protected by following secure handling practices, including those in the data management plan developed for the research/survey.

b. Enable subjects' rights.
Your research/survey team will need to be prepared to enable data subjects to exercise their EEA rights. Those rights may be exercised by a verbal request or in writing.

c. Give notice if a breach may have occurred.
The GDPR defines a "personal data breach" in Article 4(12) as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

The EEA governmental authorities must be notified within 72 hours of a security breach involving the EEA personal data. Record all details of the incident and promptly contact your IT department and Data Protection Officer with your documentation. Do not contact the EEA authorities directly. Follow your company/university's security incident reporting instructions. If the breach affects your research/survey participants personal information in any way, they may need to be informed about the breach.

13. Why is it important to comply with the GDPR?

Noncompliance with the GDPR could result in your research/survey being terminated by your company/institute, Sawtooth Software (if we are your processor), or the regulatory authority. For example

Failure to comply with the GDPR will put not only your company/institute and the processors, but also your research/survey, at risk for:

- High fines
- Regulatory orders requiring discontinuation of research/survey activities
- Violations of grant or other funding covenants, resulting in loss of funding
- Reputational harm

14 Is it possible to apply for a waiver to the application of GDPR?

No. The GDPR does not provide a procedure to be exempted from its requirements.

15. In what countries does the GDPR apply?

GDPR Countries

Austria	Finland	Lithuania	Slovenia

Belgium	France	Luxembourg	Spain
Bulgaria	Germany	Malta	Sweden
Croatia	Greece	Netherlands	United Kingdom
Cyprus	Hungary	Poland	Iceland
Czech Republic	Ireland	Portugal	Liechtenstein
Denmark	Italy	Romania	Norway
Estonia	Latvia	Slovakia	Switzerland

16. How is UK GDPR different from GDPR?

The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights, and obligations.

The Information Commissioner's Office (ICO) is the UK's independent authority responsible for upholding information rights and enforcing data protection regulations. It plays a crucial role in enforcing the UK GDPR and provides guidance and support to organizations in understanding and complying with their data protection obligations. The ICO has the power to investigate data breaches, issue fines, and take enforcement action against non-compliant organizations.

In the EU, data protection authorities (DPAs) play a similar role to the ICO in the UK. Each EU member state has its own DPA responsible for overseeing and enforcing data protection laws within their jurisdiction. These DPAs work collaboratively under the umbrella of the European Data Protection Board (EDPB) to ensure consistent application and interpretation of the EU GDPR across all member states. The DPAs have the authority to investigate data breaches, impose fines, and take enforcement actions against organizations that fail to comply with the EU GDPR.

Similarities:

1. Objective: The objective of conducting DPIAs remains the same in both the EU and the UK. It is to assess the impact of data processing activities on individuals' privacy rights and identify measures to address potential risks.
2. High-Risk Processing: DPIAs are mandatory in situations where data processing is likely to result in a high risk to individuals' rights and freedoms. This includes processing of sensitive data or large-scale systematic monitoring.
3. Accountability: Both the EU GDPR and the UK GDPR emphasize the principle of accountability, requiring organizations to demonstrate compliance with the regulations. This includes maintaining detailed records of data processing activities, implementing privacy by design and default, conducting data protection impact assessments (DPIAs), and appointing a Data Protection Officer (DPO) in certain cases. Meeting these accountability requirements can be challenging, particularly for organizations with limited resources or complex data processing operations.

Differences:

1. Legal Framework: The EU GDPR is an EU regulation that applies to all EU member states. In contrast, the UK GDPR is the data protection law specific to the United Kingdom. This distinction in legal frameworks necessitates compliance with different regulations depending on the jurisdiction.

2. Supervisory Authority: In the EU, organizations consult and cooperate with the supervisory authority in the member state where they have their main establishment when conducting a DPIA. On the other hand, under the UK GDPR, organizations consult the Information Commissioner's Office (ICO), the UK's independent authority responsible for upholding information rights and enforcing data protection regulations.

3. The implementation of additional security and privacy measures. It is crucial to identify these variances and ensure compliance with the specific obligations of each framework.

17. What personal information does the GDPR regulate?

GDPR *personal data* includes any information that identifies or could identify a person.

Personal data protected by the GDPR is much broader than Personal Health Information protected by HIPAA or other types of personal information protected in the United States, such as Social Security numbers and financial account numbers.

The list below includes examples of personal data. This is not a complete list.

- Name
- Email address
- Phone number
- Social Security numbers and other identification numbers

A name alone is personal data.

It is not necessary to have a name associated with the information. If the information, taken in the aggregate, could be used to identify a person, it is personal data protected by the GDPR.

Researchers working with human subjects will often hear the phrase, "remove all identifiable data" or, "protect identifiable data with reliable security measures." **Identifiable data** is vulnerable, as it includes information or records about the research participant that allows others to identify that person. If unauthorized individuals gain access to identifiable data, there could be a breach in confidentiality and privacy agreements. Most personal identifiers include the following:

- Names
- Social security numbers
- Bank account information
- Fingerprints
- Telephone numbers
- Home or email addresses
- Medical record numbers

- Codes that link de-identified data to identifiers (not stored separately from data)

Data may also be considered identifiable if it is combined with enough information to potentially identify a participant. For example, **indirect identifiers** are instances where a researcher does not collect personal identifiers, such as names, but combines enough information that someone familiar with the participant's background could potentially identify them. Indirect identifiers include:

- Age
- Ethnicity
- Gender
- City or state of residence
- Occupation or role
- Job function or title
- Specific time, event, context, or occasion

While these identifiers alone may not be enough to deduce a participant from a study, a combination of them might make a participant identifiable. For example:

- Demographic information and immigration status of ethnic minorities in a rural county
- A study on workplace performance among individuals with depression recruited from a small organization
- Graduates' perspectives from a small high school coupled with their occupation

Some additional personally identifiable information that most people might not realize:

- Location data
- Usernames
- Online identifiers
- IP addresses
- Online cookie ID - *Note that in some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies – the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002(OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004*) *of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1)*
- Images (i.e., a photograph, video, and drawing of a research/survey participant)
- Voice (i.e., the voice recording of an interview)
- Distinctive body markings
- Content generated by the individual

18. What personal data is considered sensitive and is subject to specific processing conditions under GDPR?

- personal data revealing racial or ethnic origin, political opinions, religious, or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data; or
- data concerning a person's sex life or sexual orientation.

19. What specific processing conditions must be satisfied before the collection of personal data considered sensitive or as a special category?

You must check the processing of the special category data is necessary for the purpose you have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose.

- You have identified an appropriate lawful basis for processing the special category data.
- You have identified an appropriate Article 9 condition for processing the special category data.
- Where required, you have also identified an appropriate DPA 2018 Schedule 1 condition.
- You have documented which special categories of data you are processing.
- Where required, you have an appropriate policy document in place.
- You have considered whether you need to do a DPIA.
- You include specific information about your processing of special category data in your privacy information for individuals.
- If you use special category data for automated decision making (including profiling), you have checked you comply with Article 22.
- You have considered whether the risks associated with your use of special category data affects your other obligations around data minimization, security, and appointing Data Protection Officers (DPOs) and representatives.

20. What are some examples of data not considered personal data?

- a company registration number;
- an email address such as info@company.com; and
- anonymized data.

21. To which persons does the GDPR apply? Does the GDPR only apply to EEA citizens and residents?

The GDPR applies to all persons located in the EEA. There is no requirement that a person be an EEA citizen or an EEA resident.

On the other hand, the GDPR does not apply to EEA citizens while they are located outside of the EEA and participate in research/survey studies, provided, none of the organizations associated with the research/survey study are established in the EEA and the personal information is not transferred into the EEA.

If you process (see the Definition of Processing) the personal data of anyone who is the data subject protected under the GDPR, then GDPR becomes an applicable law that you must comply with when Processing and/or transferring this person's personal data.

22. If my research/survey will only involve information that is publicly available, will the GDPR apply?

Generally, personal information is protected even if it has been otherwise publicly disclosed. The GDPR provides protection not only for maintaining privacy, but also for how personal information is used.

23. If my research/survey will involve de-identified data, will the GDPR apply?

Yes, so long as the EEA participants data is not anonymized, GDPR applies.

HIPAA de-identified information will be considered pseudonymized personal data under the GDPR, not anonymized. So long as a key exists to re-identify information, even if the key is sequestered from the research/survey team, the information will not qualify as anonymized.

Under the Regulation, anonymous information neither identifies an individual nor makes it possible to identify an individual.

24. My research/survey involves animals; none of the research/survey subjects are persons. Will the GDPR apply?

If your research/survey will collect or otherwise include personal information of persons, then the GDPR will very likely apply. For example, if your research/survey will collect the contact or other identifying information of the animals' owners or veterinarians, then that personal information will be protected by the GDPR. GDPR protection extends beyond the immediate subjects of the research/survey to third parties.

25. My research/survey team will be contracting with translators and other third-party service providers. Will the GDPR apply to those persons?

The contact and other limited personal information your research/survey team will need for those persons will not be in scope for the GDPR unless you can satisfy one of the scenarios listed in Q&A 4.

Additionally, if GDPR applies to your research/survey, GDPR may also apply to any processors or sub-processors that you use. A contracted translator (i.e., independent contractor) translating data that involves personal information is a sub-processor.

26. Does the GDPR have any requirements for research/surveys involving children?

Yes. There are special protections for children under the age of 16. Be sure to obtain proper guardian/parental consent before the collection of any children data and ensure you are in compliance with all local rules and regulations.

27. Does the GDPR apply to the personal information of deceased persons?

No, it does not. However, your study may still need to comply with other regulations in each country.

28. My research/survey team will be working with a research/survey team from a European organization that controls the research/survey. Will the GDPR apply to our work?

Yes. You will need a contract with the European organization that addresses the GDPR's requirements and the other obligations each party has.

29. My research/survey does not involve collecting new personal information. We will be working with an existing data set. Will the GDPR apply?

If the information will be fully anonymized *before* your team receives it, then the GDPR will not apply.

However, if the information will not be anonymized, then the GDPR will very likely apply if the data set includes information that was:

- collected by an established organization in the EEA
- collected from any person while they were in the EEA, or
- transferred out of the EEA.

30. Are there changes I can make to my research/survey protocols that will ensure the GDPR does NOT APPLY to my study?

a. Make sure that the study's objectives can be met without including personal information from the EEA.

If you expect that personal information from EEA countries could be excluded from the study without a negative impact, then consider including measures in the protocol to exclude that information and, by doing so, ensuring the GDPR does not apply to your study.

Examples:

- For studies that will collect information using an online survey, access to the survey might be blocked for persons in the EEA by blocking IP addresses from the EEA.
- For studies that will collect information by phone, do not call outside of the US assuming that your research/design team is in the US.
- If contact with research/survey subjects is to be made by mail, do not mail anything outside of the US assuming that your research/design team is in the US.

b. Make sure that all the EEA personal data the study/survey collects or otherwise processes are anonymized. However, it's not as easy as one might think!

If your study can be structured to only collect and use anonymized information in every stage of the study, then you will not be required to comply with the GDPR's restrictions.

If anonymization is accomplished later in the study, GDPR will apply until the anonymization has been effected; however, GDPR will not apply afterward to the anonymized data.

If the personal information to be processed has already been collected as part of an earlier study, or will be collected separately from your study, then you could consider requiring anonymization before you receive the data.

Only if the researcher/survey design team would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous. For example: if an organization collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the researcher/survey design team would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data.

31. What is Anonymization?

An effective anonymization solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification, once again depending on the context and purposes of the processing for which the anonymized data are intended.

32. What are some data anonymization challenges?

a. A specific pitfall is to consider pseudonymized data to be equivalent to anonymized data. The pseudonymized data cannot be equated to anonymized information as they continue to allow an individual data subject to be singled out and linkable across different data sets. Pseudonymity is likely to allow for identifiability, and therefore stays inside the scope of the legal regime of data protection. This is especially relevant in the context of scientific, statistical, or historical research.

EXAMPLE: A typical instance of the misconceptions surrounding pseudonymization is provided by the well-known "AOL (America On Line) incident". In 2006, a database containing twenty million search keywords for over 650,000 users over a 3-month period was publicly released, with the only privacy preserving measure consisting in replacing AOL user ID by a numerical attribute. This led to the public identification and location of some of them. Pseudonymized search engine query strings, especially if coupled with other attributes, such as IP addresses or other client configuration parameters, possess a very high power of identification.

b. Singling out: It is still possible to single out the records of an individual (perhaps in a non-identifiable manner) even though the records are less reliable.

c. Linkability: It is still possible to link the records of the same individual, but the records are less reliable and thus a real record can be linked to an artificially added one (i.e., to 'noise'). In some cases, a wrong attribution might expose a data subject to significant and even higher level of risk than a correct one.

EXAMPLE: Genetic data profiles are an example of personal data that can be at risk of identification if the sole technique used is the removal of the identity of the donor due to the unique nature of certain profiles. It has already been shown in the literature that the combination of publicly available genetic resources (e.g., genealogy registers, obituary, results of search engine queries) and the metadata about DNA donors (time of donation, age, place of residence) can reveal the identity of certain individuals even if that DNA was donated "anonymously."

d. Inference: Inference attacks may be possible but the success rate will be lower and some false positives (and false negatives) are plausible.

It's utterly important to remember that, as long as the data are identifiable, data protection rules apply - it does not matter what the intentions are of the data controller or recipient.

33. Are there changes I can make to my research/survey protocols that will satisfy some the GDPR security measures?

Consider incorporating these recommendations in your study's protocols to lessen the impact of the GDPR's administrative requirements, while continuing to meet your study's objectives.

a. Minimize the personal information collected and processed.

Data minimization is one of the core principles of the GDPR. See FAQ I(3).

Consider the range of information your study will be collecting. Are all types of information necessary to meet the study's purposes? Are the categories of personal information, and the specific data items, tailored to the study's focus? The fewer types of personal information collected, the less risk there will be to the data subjects' privacy, and the less risk there will be of noncompliance.

b. If anonymization is not possible, pseudonymize the personal information whenever feasible.

The GDPR encourages the practice of reducing the identifiability of personal information by using pseudonymization as a safeguard for data subjects. Under the GDPR, data is pseudonymized if

- The information cannot be attributed to a specific individual without the use of additional information (i.e., a "key")
- The key is kept separately from the data set
- Access to and use of the key is protected by technical and administrative measures. The key must be kept separately, but designated, authorized persons within the research/survey team may have access.

The GDPR's requirements are less restrictive if personal information is pseudonymized. For example, some of the rights data subjects otherwise have will not apply.

c. If consistent with your study's objectives, consider excluding minors as data subjects.

The GDPR permits the processing of personal information of minors. It imposes a requirement that the informational notice and any consent for minors be adapted to their level of understanding. The inclusion of minors should be factored into the weighing of the subjects' privacy rights against the research/survey study's requirements. We expect the level of scrutiny by supervisory authorities will be higher if minors were involved in the research/survey.

d. Consider not transferring the data collected in the EEA out of the EEA.

The GDPR includes restrictions not only on processing personal data, but on transferring personal data out of the EEA. If your study will be able to be completed without transferring the personal information out of the EEA, or if anonymization can be accomplished before the transfer, then the study will not be subject to the GDPR transfer restrictions.

If you must transfer personal information from EEA/UK to the US, you must perform additional security measures, such as having Standard Contractual Clauses in place and conducting a TIA.

34. What is a Data Protection Impact Assessment? Why is that important to my research/survey?

DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance.

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA, carrying out a DPIA in an incorrect way, or failing to consult the competent supervisory authority where required, can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

35. What are some data processing scenarios that "likely to result in a high risk"?

a. Evaluation or scoring.

The data processing is likely to result in a high risk to the rights and freedoms of natural persons if you involve profiling and predicting, especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability, behavior, location, or movements. The data Controller is required to carry out a DPIA under circumstances as such.

Example 1: A financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing or fraud database.

Example 2: A biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks.

Example 3: A company building behavioral or marketing profiles based on usage or navigation on its website.

b. Automated-decision making with legal or similar significant effect.

The data processing is likely to result in a high risk to the rights and freedoms of natural persons if you aim at taking decisions on data subjects producing legal effects concerning the natural person or which similarly and significantly affects the natural person. The data Controller is required to carry out a DPIA under circumstances as such.

Example: The computer programmed processing may lead to the exclusion or discrimination against the school/job/funding applications of certain individuals.

c. Systematic monitoring.

The data processing used to observe, monitor, or control data subjects, and the data subjects may not be aware of who is collecting their data and how their data will be used. Additionally, it may be impossible for individuals to avoid being subjected to such processing. The data Controller is required to carry out a DPIA under circumstances as such.

Example: A research project intends to utilize the school's security videos to analyze certain behaviors of the students.

d. Sensitive data or data of a highly personal nature.

The processing includes special categories of personal data (see Q&A #18), as well as personal data relating to criminal convictions or offences. The data Controller is required to carry out a DPIA under circumstances as such.

Example 1: A general hospital keeping patients' medical records.

Example 2: A private investigator keeping offenders' details.

Example 3: A researcher collecting and keeping research participants' political opinions.

Example 4: A survey author requiring the survey participants to identify their sexual orientation.

e. Data processed on a large scale.

The Working Party 29 Guidelines provide the following factors on what may be considered "a large scale" data processing:

- The number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
- The volume of data and/or the range of different data items being processed;
- The duration, or permanence, of the data processing activity; and/or
- The geographical extent of the processing activity.

The data Controller is required to carry out a DPIA under circumstances as such.

f. Matching or combining datasets.

The processing requires combining data originating from two or more data processing operations performed for different purposes and/or by different data Controllers in a way that would exceed the reasonable expectations of the data subject. The data Controller is required to carry out a DPIA under circumstances as such.

f. Data concerning vulnerable data subjects.

The processing of data subjects' data may cause an increased power imbalance between the data subjects and the data controller, because the data subjects may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. The data Controller is required to carry out a DPIA under circumstances as such.

Examples of vulnerable data subjects:

- Children
- Employees
- Mentally ill persons
- Asylum seekers
- Elderly
- Patients

g. Innovative use or applying new technology or organizational solutions

If the processing of data subjects' data involves the use of a new technology, such as a new Human Resources application to store employee files, then carrying out a DPIA prior to the usage is required.

Example: If you are introducing Sawtooth Software's products to your company/academic institute and you intend to deploy surveys outside of the US with our software/application, you are required to carry out a DPIA prior to using our products.

h. The processing prevents data subjects from exercising a right or using a service or a contract.

This type of processing operations aims at allowing, modifying, or refusing data subjects' access to a service or entry into a contract. The data Controller is required to carry out a DPIA under circumstances as such.

Example: A bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

36. Can I choose which location (country/city) I want my research/survey data stored?

Absolutely! Please see the list of our sub-processors and their data center locations below and chat with one of our sales executives about it at sales@sawtoothsoftware.com.

General Resources

- The European Data Protection Board website: https://edpb.europa.eu/
- The full text of the GDPR: https://gdpr-info.eu/
- The EU GDPR Portal: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- A "Compilation of Guidances on the EU GDPR" posted by the United States Office for Human Research Protections (OHRP) listing, by country, the data protection authorities of all EEA countries that fall under the GDPR.

Abbreviations and Definitions

Biometric data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Controller: A data controller determines the purposes and means of processing personal data. In other words, the data controller decides the how and why of a data processing operation. A data controller can be a legal person, for example a business, an SME, a public authority, an agency or other body.

Data concerning health: Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

EU: The European Union is an economic and political union among 28 European countries.

EEA: The European Economic Area unites the 28 EU member states and the three EEA European Free Trade Association states (Iceland, Liechtenstein, and Norway) into an internal market governed by the same basic rules.

EDPB: The European Data Protection Board is an independent European body which ensures the consistent application of data protection rules throughout the European Union. In other words, EDPB may overrule any EEA country's action or decision over data protection related matters if EDPB finds that action or decision to be inconsistent from the standards it upholds. The EDPB has been established by the General Data Protection Regulation (GDPR).

GDPR: The European General Data Protection Regulation.

Genetic data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

HIPAA: The US Health Insurance Portability and Accountability Act.

DPIA: A Data Protection Impact Assessment under the GDPR.

Processing: Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data.

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing if it is part of a structured filing system.

Processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Sub-processor: A sub-processor acts under the instructions of the processor, meaning that they may process individuals' personal data on behalf of the processor. A sub-processor can be a legal person, for example a business, an SME, a public authority, an agency, or other body.

TIA: A Transfer Impact Assessment under the GDPR. The term refers to a written analysis, conducted by a controller or a processor, of the impact that a transfer of personal data to a country outside of the EEA may have on the protections afforded to the transferred data. TIAs focus specifically, although often not exclusively, on whether the laws of the country to which the data is being imported would permit government agencies to access the personal data.

Sawtooth Software Authorized Sub-Processors

Sawtooth Software, as your survey data processor, may engage any of the following sub-processors for web hosting and data processing.

Name	**Services**	**Locations**	**DPA in place?**
Rackspace	Providing Sawtooth with hosting server tools and cloud space	Wherever data center is needed (see addendum 1)	Yes
Amazon AWS	Providing Sawtooth with hosting server tools and cloud space	Wherever data center is needed (see addendum 2)	Yes
Microsoft Azure	Providing Sawtooth with hosting server tools and cloud space	Wherever data center is needed (see addendum 3)	Yes
Oracle (only if a Saudi Arabia data center is needed)	Providing Sawtooth with hosting server tools and cloud space	Wherever data center is needed (see addendum 4)	Yes

ADDENDUM 1

Rackspace Data Centers	Locations
SYD2	Sydney, **Australia**
South American Data Center	Sao Paulo, **Brazil**
HKG5	Hong Kong, **China**
SHA3	Pudong, Shanghai, **China**
FRA1, FRA2	Frankfurt, **Germany**
AMS2	Amsterdam, **Netherlands**
MOW80	Moscow, **Russia**
SIN2	Queenstown, **Singapore**
LON3	Slough, Berkshire, England **(UK)**
LON8	London, England **(UK)**
LON5	Crawley, West Sussex, England **(UK)**
SJC2	San Jose, California, **USA**
ORD1	Elk Grove Village (near Chicago), Illinois, **USA**
MCI1	Kansas City, Missouri, **USA**
NYC1, NYC2	Somerset (near New York City), New Jersey, **USA**

DFW3	Richardson (near Dallas/Fort Worth), Texas, **USA**
IAD3	Ashburn (near Washington DC), Virginia, **USA**

ADDENDUM 2

AWS Data Center Regions (Availability Zones)	**Locations / Countries**
Sydney (3)	Australia
Bahrain (3)	Bahrain
São Paulo (3)	Brazil
Central Canada (3)	Canada
Beijing (3); Ningxia (3); Hong Kong (3)	China
Paris (3)	France
Frankfurt (3)	Germany
Mumbai (3)	India
Ireland (3)	Ireland
Milan (3)	Italy
Osaka (1); Tokyo (3)	Japan
Singapore (3)	Singapore

Cape Town (3)	South Africa
Seoul (4)	South Korea
Stockholm (3)	Sweden
London (3)	UK
GovCloud US-East (3); GovCloud US-West (3); North California (3); Ohio (3); Oregon (4)	USA

ADDENDUM 3

Africa

Azure Data Center Region	**Location**
South Africa North	Johannesburg
South Africa West	Cape Town

Asia Pacific

Azure Data Center Region	**Location**
East Asia	Hong Kong
Southeast Asia	Singapore

Australia

Azure Data Center Region	**Location**
Australia Central	Canberra

Azure Data Center Region	Location
Australia Central 2	Canberra
Australia East	New South Wales
Australia Southeast	Victoria

Azure Government

Azure Data Center Region	Location
US DoD Central	Iowa
US DoD East	Virginia
US Gov Arizona	Arizona
US Gov Texas	Texas
US Gov Virginia	Virginia
US Sec Central	Undisclosed
US Sec East	Undisclosed
US Sec West	Undisclosed

Brazil

Azure Data Center Region	Location
Brazil South	São Paulo State

Canada

Azure Data Center Region	Location
Canada Central	Toronto
Canada East	Quebec City

China

Azure Data Center Region	Location
China East	Shanghai
China East 2	Shanghai
China North	Beijing
China North 2	Beijing

Europe

Azure Data Center Region	Location
North Europe	Ireland
West Europe	Netherlands

France

Azure Data Center Region	Location
France Central	Paris
France South	Marseille

Germany

Azure Data Center Region	Location
Germany Central (Sovereign)	Frankfurt
Germany North (Public)	Berlin
Germany Northeast (Sovereign)	Magdeburg
Germany West Central (Public)	Frankfurt

India

Azure Data Center Region	Location
Central India	Pune
South India	Chennai
West India	Mumbai

Israel

Azure Data Center Region	Location
Israel Central	Israel

Italy

Azure Data Center Region	Location
Italy North	Milan

Japan

Azure Data Center Region	Location
Japan East	Tokyo, Saitama
Japan West	Osaka

Korea

Azure Data Center Region	Location
Korea Central	Seoul
Korea South	Busan

Mexico

Azure Data Center Region	Location
Mexico Central	Querétaro State

New Zealand

Azure Data Center Region	Location
New Zealand North	Auckland

Norway

Azure Data Center Region	Location
Norway East	Oslo
Norway West	Stavanger

Poland

Azure Data Center Region	Location
Poland Central	Warsaw

Qatar

Azure Data Center Region	Location
Qatar Central	Doha

Spain

Azure Data Center Region	Location
Spain Central	Madrid

Switzerland

Azure Data Center Region	Location
Switzerland North	Zürich
Switzerland West	Geneva

United Arab Emirates

Azure Data Center Region	Location
UAE Central	Abu Dhabi
UAE North	Dubai

United Kingdom

Azure Data Center Region	Location
UK South	London
UK West	Cardiff

United States

Azure Data Center Region	Location
Central US	Iowa
East US	Virginia
East US 2	Virginia
North Central US	Illinois
South Central US	Texas
West US	California
West US 2	Washington
West Central US	Wyoming

ADDENDUM 4

Oracle Data Center regions	Locations
Australia East	Sydney, New South Wales, **Australia**
Australia Southeast	Melbourne, Victoria, **Australia**

Brazil East	Sao Paulo, **Brazil**
Canada Southeast (Montreal)	Montreal, Québec, **Canada**
Canada Southeast (Toronto)	Toronto, Ontario, **Canada**
Germany Central	Frankfurt, Hesse, **Germany**
India South	Hyderabad, Telangana, **India**
India West	Mumbai, Maharashtra, **India**
Japan Central	Osaka, Kansai, **Japan**
Japan East	Tokyo, Kanto, **Japan**
Netherlands Northwest	Amsterdam, North Holland, **Netherlands**
Saudi Arabia West	Jeddah, Emirate Of Makkah, **Saudi Arabia**
South Korea Central	Seoul, **South Korea**
South Korea North	Chuncheon, Gangwon, **South Korea**
Switzerland North	Zurich, **Switzerland**
London Gov Classic	London, **United Kingdom**
UK Gov South	London, **United Kingdom**
UK Gov West	Newport, **United Kingdom**

UK South	London, **United Kingdom**
Ashburn Gov Classic	Ashburn, Virigina, **USA**
Chicago Gov Classic	Chicago, Illinois, **USA**
US DoD East	Ashburn, Virigina, **USA**
US DoD North	Chicago, Illinois, **USA**
US DoD West	Phoenix, Arizona, **USA**
US East	Ashburn, Virigina, **USA**
US Gov East	Ashburn, Virigina, **USA**
US Gov West	Phoenix, Arizona, **USA**
US West (Phoenix)	Phoenix, Arizona, **USA**
US West (San Jose)	San Jose, California, **USA**