

GDPR and Nfield Toolkit

Last updated: 29 November 2024



Copyright © 2024 NIPO

All rights reserved

Nfield GDPR Toolkit contains proprietary information of NIPO.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between NIPO and the customer and remains the exclusive property of NIPO. If you find any problems in the documentation, please report them to us in email. NIPO does not warrant that this document is error-free. In cases where the documentation significantly differs from the software implementation, the end user is encouraged to contact NIPO. However, the information in this document can not be used to grant the end user of the product any rights with regard to updates or fixes, demanding a match with the existing documentation.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of NIPO. You are not allowed to share the software with individuals outside your company.

Contents

About this booklet	3
Why you should care about GDPR	3
Nfield: secure and compliant	4
1: Data Minimization & Accuracy	5
2: Storage Limits	5
3: Legitimate Interest	6
4: Consent	6
5: Individual Rights	7
Right to be Informed	7
Right to Access	7
Right to Rectification	8
Right to Erasure	8
Right to Restriction of Processing	8
Right of Data Portability	8
Right to Object	8
Summary Nfield's GDPR supporting features	9

About this booklet

Trust is critical in market research, especially with regards to raw data. Your respondents trust you with all kinds of sensitive data about their lives, you need to be able to trust us to keep that data safe. That is why NIPO is committed to offering the most secure survey solutions for the professional market research industry. Our ISO 27001:2013 certification is strong and independent proof in how we are leading the area of data security.

Nfield includes features to assist you in your efforts to address GDPR controls. Such features include the ability to search cross surveys for respondents, to delete or pseudomize interviews and to anonymize data in surveys.

Our goal is simple: To provide functionality in Nfield so our customers can address GDPR controls without having them compromise on data collection efficiency.

This booklet, we call it our Nfield GDPR toolkit, highlights the Nfield features that can help you to address GDPR. A guide like this can never be a 100% complete, so please feel free to reach out to your sales representative with any questions you might have around Nfield and its functionality.

Please note that this toolkit is not a replacement for legal advice. We advise that, in case you have not done so yet, you seek legal advice on how GDPR applies specifically to your organization, and how best to ensure compliance.






Why you should care about GDPR

On 25 May 2018 the European Union will make its biggest change in privacy legislation to date. On this date the European Union General Data Protection Regulation (GDPR) will be enforced, replacing the 1995 Data Protection Directive 95/46/EC and all current national laws based on it. GDPR will impact every industry, including the Market

Research industry, and it will significantly impact the way you are to handle data collected during surveys.

Under the new legislation the privacy rights of EU citizens is bolstered, in particular, their right to the protection of personal data. The GDPR introduces new obligations on organizations that process personal data of EU citizens, new rights for EU citizens and stricter penalties for non-compliance.

GDPR harmonizes privacy legislation across all EU member states. This means all EU citizens will have the same privacy rights, independent of the EU country they live in. GDPR applies to the processing of personal data of EU citizens done by a company established in the EU, and to companies established outside the EU who offer goods or services in the EU or who monitor the behavior of individuals in the EU. So even if your business is located outside the EU, for example in the U.S. or in Singapore, when you offer your services in the EU or engage EU citizens in your surveys, then you need to make sure you comply with GDPR.

GDPR				
				
Applicable worldwide	Right to be forgotten	Substantial penalties	Prompt incident reporting	Nfield's feature
As long as the organization stores personal data of EU citizen	Enhanced right to information right to be forgotten	Up to 20 million euro or 4% annual worldwide turnover	Within 72 hours, severe penalties for failure to report	Enhanced GDPR feature to support compliance with GDPR

Nfield: secure and compliant

Data Security is essential to addressing GDPR controls. It is good to know that NIPO is committed to offering the most secure survey solutions for the professional market research industry. We have procedures for everything, encrypt your data everywhere, limit access across the board and continuously test for potential security flaws.

Our ISO 27001:2013 data security certification is strong and independent proof in how we are leading the area of data security. Not just NIPO is ISO27001:2013 certified, also all the parties (sub-processors) we engage to offer Nfield are, making sure every step in the value chain is secure and independently audited.

At NIPO we are not only serious about data security, we are also very serious about confidentiality. That is why NIPO staff have no access to your data in Nfield. Your Nfield data really is your data. You define what data is available in Nfield, you manage who has access, to what functionality they have access, the password policies applied, etcetera.

Nfield is setup with local compliance in mind. For you this means that if you are working on a EU domain, we guarantee that none of your data leaves the EU. Of course, if you download data that is collected in a EU domain from the U.S. there is not much we can do about that.

We make a log available to you where you can trace all actions that have happened with regards to anonymizing data or deleting records from your surveys. The logs state which user did what actions at what point in time. This allows you to trace back in detail why your data looks like it looks.

And finally, we actively monitor what happens on the Nfield system. In case we suspect a data breach we will immediately launch an investigation and work with our data protection officer to make sure we deliver you the information you need to engage with your local data protection authority.

In addition to keeping your data secure, NIPO have updated Nfield to help our clients address GDPR requirements for the following controls:

1. Data Minimization and Accuracy
2. Storage Limits
3. Legitimate Interest
4. Consent
5. Rights of Individuals

You can reference the following link to attain additional information regarding GDPR: <https://gdpr.eu/>.

1: Data Minimization & Accuracy

Data minimization means that you shall only process EU Personal Data that you need for realizing your business purposes. Nfield stores data in two separate storages: sample data and interview data. Using these two different storages wisely will help assist with data minimization efforts.

We suggest you always store all personal identifiers in the sample table. Nfield already does this automatically for all information you add to the system (like email addresses, physical addresses, captured GPS coordinates, etcetera) and with the *SAMPLEDATA command you can also write info you collect during the interview into the sample data storage.

If you set this up correctly, your interview data will not contain any personal identifiable data, even though you may have collected such information as part of the interview.

This makes it very easy for you to delete the personal identifiable data from the survey when no longer needed, and by doing so pseudonymize or anonymize the interview data in Nfield. You can do this for all the sample data, only specific sample data fields, for all interviews or for a selection of interviews, allowing you to manage in detail which data you keep in Nfield.

In Nfield you can correct the data is stored in the sample table of a survey. This means that, if your records state the respondent is a male, but you find out she is actually female, Nfield allows you to correct this for that specific respondents to make sure any data you have stored in Nfield is accurate. Such changes can be done both through the API as well as through the Nfield Manager.

2: Storage Limits

With Nfield you can choose which data to keep in Nfield. Nfield stores data in two separate storages: sample data and interview data. Because of this you can delete data very specifically:

- a. Do you need to keep the sample data for re-contact purposes, and have you already exported the interview data to another system? Then you can delete only the interview data while keeping the sample data.
- b. Do you send out weekly batches on the same survey and do you need to delete data for previous batches? Then you can delete data for a specific range of interviews. Additionally, you can set a data retention period to automatically delete sample data and interview data in online surveys. This feature helps streamline compliance and optimize storage through automatic clean-up, as detailed in our blog post on [customized survey-level data retention policies](#).

It is good to consider having the least number of copies needed of your data. Has your survey finished and there is no need to keep any of the data in Nfield? Then you can delete the survey, and all data contained in it. Additionally, Nfield offers an automatic clean-up feature that can automatically delete old, unused surveys, ensuring your domain remains secure, compliant, and efficient. Learn more about this feature in our blog post on [keeping your Nfield domain clean](#).

Nfield makes sure it also automatically deletes all data from the backups we keep for disaster recovery purposes. This will not be instant, but within 4 days all deleted data is removed also from all our backups.

You can easily customize how you manage the deletion of survey and interview data using our robust APIs. These APIs provide all the necessary functionality to support full survey automation, giving you complete control over your data management workflows. For more details, explore our blog post on the [Developer's Guide to Nfield Integration via the API](#).




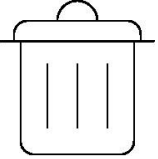
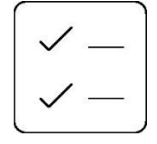
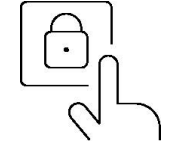
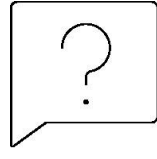
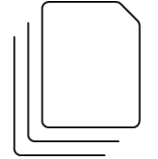
3: Legitimate Interest

Legitimate interest might only be used in market research for quality control. In many of these cases the respondent may be contacted again to validate the interview took place and to validate some of the answers given. For this it is required to store some personal identifiers longer than others. Nfield allows you to delete each identifier separately, giving you full control over which data is kept and which not.

Some personal identifiers may only be collected during the interview; for example, telephone numbers for re-contacting. During the interview, you can decide where you want to store this data. It might be best to consider storing personal identifiers collected during the interview as part of the sample and only as part of the sample. By doing so you can easily delete the personal identifiers from the survey after fieldwork has finished.

4: Consent

When consent is the pathway for data collection and processing, the data subject should be aware of the uses that you shall intend to make of their personal data.

MUST BE				
	Given by a statement of clear affirmative action	Collected data must be freely given	Proven by the data controller	Withdrawn as easily as it is given
MUST NOT				
	Be inferred from silence, pre-ticked boxes or inactivity	Make consent a condition for receiving a service unnecessarily	Use confusing unclear language	Bundle with other terms and conditions

Asking consent is nothing other than asking a question. The simplest way to do so is to make the consent request part of the interview, that way the response is also stored with the collected data.

You can use a custom interview end reason (*ENDST ###) if a respondent does not give consent. That way you can properly track your response and incidence rates.

When asking consent for processing the data collected during an interview, you can store the consent with the data in Nfield. Nfield allows you to capture consent as a recorded sound fragment (CAPI) or user approved input (Online) which is stored with

your data. To do so, just capture the response as audio feedback to an open-ended question in CAPI or as a closed question in Online.

In case you are conducting surveys on sensitive subjects consider asking different consents for different parts of the survey. This will prevent you from not being able to use a contact in case a respondent has a problem with consenting to the full interview but is willing to consent to part of it. Nfield allows you to route the interview based on multiple consents obtained, so you can make the most of each interview.

5: Individual Rights

The GDPR introduces new rights of individuals. Individual data subjects of EU Personal Data have the following rights under the GDPR:

1. The Right to be Informed
2. The Right of Access
3. The Right to Rectification
4. The Right to Erasure
5. The Right to Restriction of Processing
6. The Right to Data Portability
7. The Right to Object
8. Rights related to Automated Decision-Making, including Profiling

Right to be Informed

Nfield allows you to create pages in the interview where you can just show information to the respondent. This is ideal for informing respondents about processing the data you are about to collect. The advantage of informing respondents as part of the interview is that you are sure respondents have been presented with the correct information. Also, you can immediately register their consent as Nfield already has all the tools to register a respondent's response.

Right to Access

Nfield allows you to search across surveys for personal identifiers. To make optimal use of this feature you should store all personal identifiers as part of the sample. System data like captured GPS coordinates, addresses or email addresses, are automatically stored in the sample. During the interview, you can choose to store personal identifiers only as part of the sample. By doing so you make this information searchable but also easy to delete, allowing you to quickly anonymize the interview.

That is why we suggest to always store personal identifiers as part of the sample and only as part of the sample. Likewise, store the data you need for analysis always as part of the interview data. By doing so you can easily split information you need for fieldwork execution or quality control (sample data) and data you need to generate insights for you customer (interview data).

Please note that GPS coordinates are stored by Nfield as part of the sample (even though in the downloadable data files they are part of the para data), as GPS coordinates may be considered personal identifiers, especially in rural areas.

Right to Rectification

Data that is stored as sample in Nfield can be edited at any time. Before the interview, during the interview and even after fieldwork completed. Nfield will then make sure that data is changed everywhere throughout the Nfield system. Nfield does not allow you to change the data that is stored as interview data. The reason for this is that you should always be able to go back to the raw unedited interview data. If you ever need to rectify interview data, you will have to do this in a downstream system. In this case we strongly suggest you delete the interview in Nfield or delete the whole survey.

Right to Erasure

Nfield allows you to select a sample record and either delete all data or just the personal identifiable information from it, and by doing so anonymizing the data. It is up to you to decide on the best method to do so, based on your preference and/or your agreement with the data subject. You can delete the data at any time in the survey life cycle: In setup, during fieldwork or after fieldwork has completed. To properly anonymize the survey, we suggest you follow the practice of saving personal identifiable information as sample data and never as the interview data. That way you can anonymize the data while still stored in Nfield.

Nfield allows you to search for personal identifiers in sample data across surveys, allowing you to quickly identify in which surveys a specific email address is contained, and subsequently take the proper action, as requested by the data subject.

Right to Restriction of Processing

Individuals have a right to block or suppress the processing of their personal data. When the processing is restricted, you can store the personal data but not further change or process it. In the field of market research, this basically means that you cannot use the collected data anymore. Hence, when a respondent exercises this right, you can best treat it as a request to be forgotten (see Right to Erasure).

Right of Data Portability

Nfield allows you to select a sample record and then download a data file just for that record. The data file is in a GDPR compliant format and can be easily shared with the data subject, or with another data controller, if required to do so.

Right to Object

Generally, respondents object to the use of their contact details for re-contacting them as part of a quality control process. It is up to you to decide how you would like to deal with that. If you have already successfully completed the interview, you can mark the interview as rejected in CAPI or delete all data from it in both CAPI and Online. Rights related to Automated Decision-Making, including Profiling Nfield does not do profiling. Nfield is a data collection system. There is no profiling or automated decision making baked into the software.

Summary Nfield's GDPR supporting features

Principles	Supporting features
Data Minimization	Remove all data or sample data and interview data separately, per interview, set of interviews or for all interviews.
Data Accuracy	Edit individual sample data records.
Storage Limitation	Delete data for subsets of the records in the survey to support running waves in a survey with data retention policy setup. You may also delete the whole survey with automatic clean-up setup. Automatic removal from back-ups.
Consent	Ask for consent as question in the script and store the answer as part of interview.
Legitimate interests	Only storing personal identifiers collected during the interview in the sample data and partially deleting personal identifiers from the survey.
Right to be Informed	Inform respondents as part of the interview, before asking questions.
Right of Access	Cross-survey search on occurrence of personal identifiers in sample data to identify respondents and then download the data for the individual records.
Right to Rectification	Edit individual sample data records.

Right to Erasure	Delete the sample data for the interview to anonymize or delete the entire interview to remove fully.
------------------	---

Principles	Supporting features
Right to Restriction of Processing	Delete the sample data for the interview to anonymize or delete the entire interview to remove fully.
Right to Data Portability	Cross-survey search on occurrence of personal identifiers in sample data to identify respondents and then download the data for the individual records.
Right to Object	Delete the interview or mark the interview as not passed quality control (CAPI only).
Rights related to automated decision-making, including Profiling	There are no profiling functions in Nfield.

As mentioned before, a guide like this can never be a 100% complete, so please feel free to reach out to your sales representative with any questions you might have around Nfield and it's functionality.

