PRIVACY ASSISTANT IN A NUTSHELL

How to run GDPR compliant surveys in EFS

Kamil Machura
kamil@questback.com
27. April 2018

GDPR IN EFS

INTRODUCTION

Beginning on 25th May, 2018, the General Data Protection Regulation (GDPR) redefines the legal requirements to conduct surveys. Users who seek to obtain insights from their respondents have to follow new rules when they process personal data relating to respondents. Some of the key changes are:

› The GDPR rises the bar for relying on valid consent for conducting surveys. A valid consent requires a clear, informed, explicit and affirmative statement from your respondents. Users must inform respondents about the survey in clear and plain language. Pre-ticked consent boxes are prohibited and will not serve as a valid consent.

› When they collect and assess feedback data, users must to be able to demonstrate how they comply with the new data protection regulation, e.g. users must define the purpose of data processing prior to each survey.

› Personal data shall not be kept longer than is necessary for the purpose of the processing, i.e. feedback assessment. This implies that there is a time limit how long personal data can be used after the survey. Therefore, users should define a retention period for respondent's personal data after which such data will be deleted.

› The GDPR provides respondents with several rights, including a right to object any data processing, a right to withdraw consent and to transfer their data in a commonly-used machine readable format.

› Supervisory authorities have powers to impose significant fines of up to Euro 20million or 4% of total worldwide annual turn-over for users that do not comply with the GDPR.

If activated, **Questback's Privacy Assistant**

› enables users to identify ("flag") personal data prior to the survey to ensure complete and accurate deletion of personal data which is no longer needed after the survey.

› supports users to create a "consent form" to obtain informed, explicit and valid consent from their respondents.

› offers a library of purposes statements to provide adequate information to respondents about the purpose for data processing.

› helps users to provide statutory information to their respondents as required by the GDPR, e.g. contact information, individual rights, retention period and many more.

› allows users to create an information sheet for respondents on their personal data which can be exported (data portability).

IMPACT ON FEEDBACK DATA COLLECTION

Without going into too much detail, the green boxes in the following overview show you the areas in the GDPR that are of particular importance when creating and running surveys.

1. Extra-Territorial Scope	2. Data Processors	3. Data Protection Officer	4. Accountability	5. Consent
• The GDPR expands the territorial and material scope of EU data protection law. • It applies controllers and processors established in the EU, and those outside the EU, who offer goods or services to, or monitor EU data subjects.	• GDPR imposes several statutory obligations on data pocessors • Controller may engage only processors that provide sufficent guarantees for GPDR compliant processing • Data Processing Agreement is mandatory	Controllers and processors must designate a data protection officer if core activities involve "regular and systematic monitoring of data subjects on a large scale" or, if the entity conducts large-scale processing of "special categories of personal data".	The concept of accountability requires: • Dilligent documentation • Records of processing activity • Deletion concept • Data protection impact assessment	• GDPR rises the bar for relying on valid consent • Clear, informed, explicit and affirmative action • No pre-ticked boxes (by default) • Respondents can withdraw consent any time

6. Privacy Notice	7. Individuals' Rights	8. Breach Notification	9. International Data Transfer	10. Sanctions
• The GDPR requires you to provide specific information to ensure valid consent and transparent processing. • Information must be given in an easily readable form, using clear and plain language.	Respondents are entitled to several individual rights such as • the right to object any processing • the right to rectify • the right to access • Data protability	• Data controller must notify supervisory authorities of a data breach within 72 hours, unless there is no risk for respondents. • Duty to notify respondents, if breach bears "high risk" to their rights.	• Data transfer outside the EU/EEC remains prohibited unless that country ensure adequate level of data protection. • Controller has multiple option to take appropriate safeguards, e.g. EU standard model clauses, BCR etc.	• Supervisory authorities have powers to impose significant fines of up to €20million or 4% of total worldwide annual turn-over • Respondents can sue for pecuniary or non-pecuniary damages (i.e. distress).

Below you can see the upcoming GDPR assistance package, which will assist you in the setting up GDPR compliant surveys.

PRIVACY ASSISTANT FOR YOUR SURVEY

This is where you enable GDPR assistance for your survey.

Once the GDPR assistant has been activated, you will be able to **configure your consent form** as well as to **set a retention period for the personal data** you are about to collect.

The configuration is done within the new 'respondent consent form' page in the questionnaire editor.

SETTING UP A CONSENT FORM

The consent form can be created from scratch or by adapting one of our example forms from the library (for each of your survey languages).

In addition to the purpose statement you will need to add a couple of fields that ensure that you end up with a fully compliant GDPR consent. The tooltips will assist you in adding the needed information (see on next page).

Privacy information ⓘ

Company name (controller)	
Contact details	
Controller's representative (if applicable)	
What personal data will be collected and used	
What special categories of personal data will be collected and used	
Legal basis for processing	

If you want to obtain feedback from your respondents based on their consent, you should ensure to comply with the legal requirements for valid consent.

The GDPR defines consent as a freely given, specific, informed and unambiguous indication of one's agreement.

As a controller for respondent data, you are expected to provide sufficient information to your respondents prior to their participation to enable them to make an informed decision, to understand what they are agreeing to and to exercise their legal rights (i.e. to withdraw consent).

The consequence of not informing your respondents in a proper fashion is that consent will be invalid and you may be in breach of data protection legislation.

In addition, Art. 13 GDPR requires you to provide certain information to your respondents at the time personal data is obtained from them as transparency is a fundamental principle of lawful data processing.

The fields in this section enable you achieve both, providing necessary information to your respondents to submit a valid consent and fulfilling your notification duties under the GDPR.

Recipient or categories of recipients of the personal data	ⓘ	
Transfer of data to a non-EU/EEC country or international organisation, and safeguards	ⓘ	
Statutory or contractual requirement	ⓘ	
Automated decision making	ⓘ	
Information on data subject rights	ⓘ	
Information on right to withdraw consent	ⓘ	
Information on supervisory	ⓘ	

THE CONSENT FORM MANAGER

Creating a complete consent form from scratch can be quite challenging, that's why we've added a couple of processing purpose statements for the most common use cases into the library

You can also use the library to maintain consent forms that you want to re-use across different survey projects

SET A RETENTION PERIOD

With **retention period** you set the time until all respondent data that you have flagged as personal data should be deleted. This must be in place since personal data must be kept "no longer than is necessary for the purposes for which the personal data are processed" with GDPR.

The retention period needs to be set before publishing your survey.

FLAG PERSONAL DATA IN YOUR SURVEY

When your survey is enabled for GDPR, this setting will be available for all question types as well as participant variables.

DELETION OF PERSONAL DATA

By ticking the '**flag as personal data'** box, all answers to that question are flagged as personal data and can be deleted by Questback **upon your request**.

Also, all variables flagged a personal **will be deleted automatically after the retention period expires**.

This setting can be activated even after you've published or closed your quest – but not deactivated.

You can even delete personal data for projects that are already running (after you have activated the privacy assistant) by using a new option under 'reset survey'
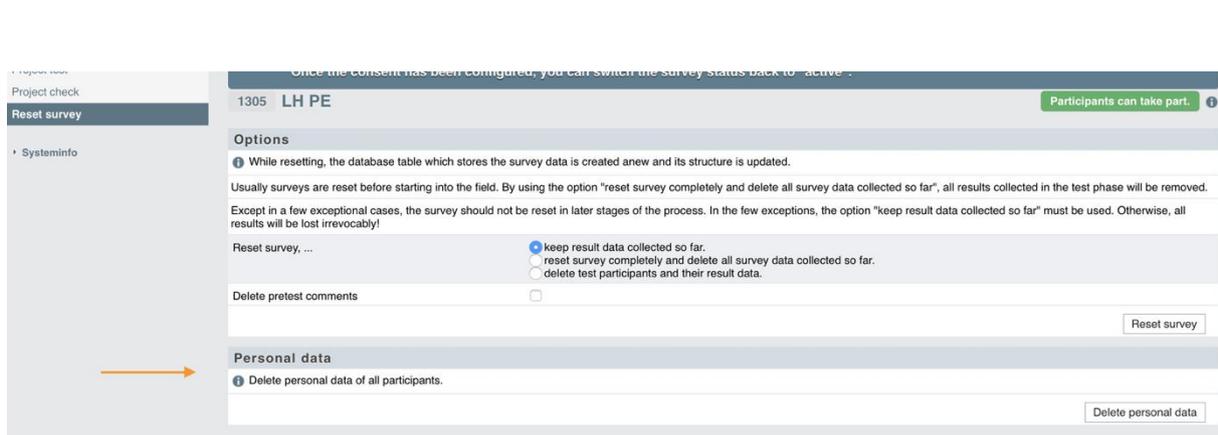
… AND THE RESPONDENTS?

You need of course tell your respondents they can feel safe with a fully GDPR compliant survey. When you have enabled your quest like described above – the selected **statement page will be displayed for the respondents to agree with the terms.**

And each individual agreement of your purpose statement is logged by Questback, together with date, time and the statement version.

Welcome!

Thank you very much for participating in our survey on **Digital Leadership.**
Digitization of the working world brings about a lot of new chances as well as challenges. The aim of this research is to gather insight into the role of leadership in the rapidly changing digitized world, in order to identify actions that can improve the workplace.

The survey should take no longer than **20 minutes**.

Participation is completely voluntary and all responses are kept anonymous.

Why do we collect and use your data

The collected data will be used for a master's thesis at the Chair of Sociological Occupational Research at the Faculty of Management, Economics and Social Sciences of the **University of Cologne**

How to contact us

University of Cologne
Albertus Magnus Platz
50923 Cologne
Phone: +49 221 470-0

If you would like to obtain more information about the processing of your personal data, please click here

☐ I agree to the processing of my personal data in accordance with the information provided herein

I don't want to participate

START THE SURVEY

IMPRESSUM

Questback GmbH
Gustav-Heinemann-Ufer 72a
50968 Köln
Deutschland

Telefon:	+49 221 27169 0
Telefax:	+49 221 27169 788
E-Mail:	info@questback.de
Homepage:	www.questback.de
Geschäftsführung:	Nils Stangnes, Ivar Blekastad
Sitz der Gesellschaft:	Amtsgericht Köln HRB 77296
UST-IDNR.:	DE203615380
Steuernummer:	224/5717/0761
Bankverbindung:	HypoVereinsbank AG Düsseldorf
	BLZ 302 201 90
	Kto. 609 839 333
IBAN:	DE92 3022 0190 0609 8393 33
Swift:	HYVEDEMM414

Questback ist europäischer Marktführer für Enterprise Feedback Management. Mit Befragungs- und Feedbacksoftware von Questback gewinnen Unternehmen gesicherte Erkenntnisse für erfolgreiche Geschäftsentscheidungen.