123FormBuilder & the General Data Protection Regulation (GDPR)

Summary

This document explains how 123FormBuilder implements the GDPR requirements, which are mandatory after May 25th, 2018, for all companies that handle data of EU citizens. It also contains the responsibilities of its customers, in terms of GDPR compliance.

Version: 1.0

Updated: March 21st, 2018

Created by: Tudor Bastea, CTO, 123FormBuilder

For the latest version of this document, please visit
https://www.123formbuilder.com/gdpr-compliance/

Glossary

GDPR	The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.
123FormBuilder or The Company or Data Processor	123FormBuilder is a company that builds and supports the Platform, allowing its Customers to create forms, surveys, quizzes, polls, using data which they collect from their own clients (named End Users, see below).
Platform	The multitude of website, source code, servers, web services, API services, and everything else that is needed for offering Customers the possibility to build and use forms, surveys, quizzes, polls.
Customers or Form Owners or Data Controllers	The companies or individuals that create 123FormBuilder accounts, both free and paid, with the purpose of creating forms, surveys, quizzes, polls, that will later be filled by the End Users.
End Users or Data Subjects	The citizens, both from EU and outside, that fill the forms, surveys, quizzes, polls, created by Data Controllers
Submissions	The data obtained by 123FormBuilder (the Data Processor) on behalf of Customers (or Data Controllers or Form Owners). It can consist of Personal Data and / or non-Personal Data.
Personal Data	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, 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.
Processing	As for GDPR, processing means any operation or set of operations

	which is performed on personal data or on sets of personal data, if by automated means, such as 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
DPA	National data protection authorities, in the EU countries
Personal Data Breach	It means 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.
Sensitive Data	Data about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (GDPR, Art 9)
Amazon Web Services (AWS)	AWS is a cloud hosting solution, offered by Amazon. It uses the latest technologies, and is the de facto leader for hosting SaaS companies, like 123FormBuilder.
EEA	The European Economic Area is the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, including the freedom to choose residence in any country within this area.

Key GDPR requirements

123FormBuilder helps its Customers understand GDPR in relation to their usage of the Platform. This document should not be used as a substitute for legal advice. The customers should seek independent legal advice regarding their obligations under GDPR and they should adopt proper transparent information towards their responders to the prepared forms with clear information regarding the Data Processor (123FormBuilder), mentioning their decision related to all required GDPR information (type of data collected within form, retention period, processor information, data location, etc).

After analyzing the full text of GDPR [1], 123FormBuilder concludes that it contains some clear pieces of information (definitions, principles), and some requirements which each company should analyze and decide how the company should behave in order to comply with GDPR.

Below is the list of the key GDPR topics we have identified, followed by a detaliation of how we understand to comply with each of the requirements.

#	Topic	GDPR references
1	Data security & confidentiality	Art. 25, 28, 29, 30, 32
2	Rights of Data Subjects	Chapter III
3	The need for informed, freely given, consent	Rec. 32, 40; Art. 6
4	Obligation to appoint a DPO	Art. 37
5	Cross-border Data Transfers	Art. 44 - 47

1. Data security & confidentiality

123FormBuilder considers Data Security a core requirement for its business and has implemented several measures to support this:

- The Company conducts its processes by following specific standards and has the following certifications:
    - ISO 9001:2015
    - ISO 27001:2013

    - ISO 27017
    - ISO 27018
- The Company builds the Platform trying to offer Data Controllers as much granularity as possible, when speaking of permission to collect, view, and modify Submissions
- The source code that is developed for the Platform is always peer-reviewed, to prevent involuntary mistakes that could affect the collected Submissions
- The infrastructure is highly redundant, and hosted entirely in AWS. Every service or hardware component grants access only from the required sources (networks, specific IPs, etc)
- The subsystems of the Platform are built with security in mind. From the design phase, they are built in such a way to offer data protection

For years, 123FormBuilder has maintained its Incident Response Plan, and it was updated to respect the requirements of GDPR. In the undesired event of having a data breach, 123FormBuilder and the Customers commit to respecting the GDPR requirements and notify the necessary parties.

By the nature of its business, 123FormBuilder does not automatically encrypt collected Submissions. This is mainly because encryption would compromise certain features of The Platform (ie: the ability to search in Submissions, the ability to reject duplicate Submissions from the same individual, etc).

But 123FormBuilder has an encryption feature, that is clearly offered to the Data Controllers. It is the Data Controllers' own responsibility to evaluate the type of data they collect, and to enable the encryption feature, for their entire account. 123FormBuilder invests resources into detecting which Data Controllers collect Sensitive Data, and to suggest them to use encryption for their Submissions.

Data Processor's obligation of confidentiality

123FormBuilder employees are required to sign confidentiality agreements and to conduct periodical confidentiality trainings.

Data Processor's records of processing activities

123FormBuilder has powerful logging systems, that record the processing activities. The systems can be consulted easily, in case a DPA requires it. Only specific 123FormBuilder employees have access to the Submissions collected using The Platform, and access is logged and monitored.

2. Rights of data subjects

GDPR strengthens some of the rights of the Data Subjects, and also creates some new rights for them. The Customers must grant these rights to the Data Subjects. To help Customers, we have created this list of essential rights, and the articles where they are defined, in GDPR.

Right of access by the data subject	Art. 15
Right to rectification	Art. 16
Right to erasure ('right to be forgotten')	Art. 17
Right to restrict processing	Art. 18
Right of data portability	Art. 20
Right to object to processing	Art. 21
Right to object to processing for the purposes of direct marketing	Art. 21(2)-(3)
Right to object to processing for scientific, historical or statistical purposes	Art.21(6)

In the relationship with 123FormBuilder, the Customers act as Data Subjects themselves. 123FormBuilder grants all the rights specified by GDPR.

Customers can export data from 123FormBuilder, using the functionalities of The Platform. They can also use the 123FormBuilder API, for this purpose.

When 123FormBuilder receives a complete deletion request from a Customer, 123FormBuilder will delete the Customer data from all its systems within a maximum period of 60 days unless retention obligations apply.

3. The need for informed, freely given, consent

GDPR establishes clear guidelines regarding consent: it should be freely given, specific, informed and unambiguous. When signing up for a 123FormBuilder account, Customers are clearly informed about how their data will be used, and how they will be contacted. The Customers will have the option to remove their consent, after logging on the platform.

Depending on the type of data collected, the Data Controllers might be required to ask for consent, on the forms / surveys they create using the platform. They have the responsibility of evaluating the need for consent and implementing it, if needed.

4. Obligation to appoint a DPO

As Data Processor, 123FormBuilder understands that, by the nature of its business, it is expected to designate a Data Protection Officer (DPO), and has designated Mr Cristian Zlavog for this role. His previous experience regarding data security recommends him for this role. The designated DPO is aware of the requirements of GDPR and their implementation within 123FormBuilder.

Data Controllers having accounts on The Platform have the responsibility to evaluate their own need to assign a DPO, according to DGPR recommendations.

5. Cross-border Data Transfers

123FormBuilder has identified that The Platform processes two types of Personal Data:

Personal Data collected using Submissions
They are holding Personal Data of Data Subjects and can transferred to third parties as follows:

- Applications that The Platform integrates with (examples: Salesforce, Mailchimp, Zoho, AWeber, Wix, Marketo, and many others). 123FormBuilder conducts a review of all these Applications, in order to make sure all of them comply with GDPR
- Customers can set Webhooks, which receive the Submissions at the URL they specify. 123FormBuilder does reasonable efforts to accept only safe URLs, but the

responsibility of making sure the Webhooks are GDPR compliant comes to the Data Customers.

Personal Data collected from Customers

They are collected with the purposes of:

- offering them the best possible experience on the Platform
- understanding their needs and trying to sell them paid plans of the Platform

For this purpose, 123FormBuilder sends this data to other platforms that are used internally (ticketing systems, emailing systems, newsletter systems, etc). All such platforms comply with the GDPR requirements and are periodically reviewed.

Got questions?

For the purpose of solving its Customers' GDPR compliance issues, 123FormBuilder has:

- created a special email: gdpr [at] 123formbuilder [dot] com .
- created special page was created for GDPR compliance: https://www.123formbuilder.com/gdpr-compliance/

Resources

For understanding and implementing the GDPR requirements, we have used the following resources, which we recommend all our Customers to read.

[1] GDPR, full text: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] https://www.eugdpr.org/

[3] https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation