Advanced

A Guide to Understanding and Complying with GDPR Requirements

Implications, Tips and Checklists to process personal data

simplystakeholders.com

A Guide to Understanding and Complying with GDPR Requirements

Implications, Tips and Checklists

Allison Hendricks
Stakeholder Engagement Specialist Director, Darzin Software

Fraser Henderson
Public Consultation Specialist Darzin Software

www.darzin.com

***DISCLAIMER**: This information is not intended to be a comprehensive and definitive guide on the GDPR, or legal advice for your company to use in complying with the GDPR. Instead, it provides background information to help you better understand some of the implications this legislation has for consultation processes. This information is not the same as legal advice, where an attorney applies the law to your specific circumstances, so please consult an attorney if you'd like advice on your interpretation of this information or its accuracy. In a nutshell, you may not rely on this information as legal advice, nor as a recommendation of any particular legal understanding.*

TABLE OF CONTENTS

Overview of the GDPR

The General Data Protection Regulation sets new standards for the collection, storage and use of Personal data for all organisations doing business with EU citizens.

On 25 May 20218, the General Data Protection Regulation (GDPR) will replace the Data Protection Directive as the new global standard on data privacy for all government agencies and organizations that do business with European Union (EU) citizens. When it does, all organizations that control, maintain, or process information involving EU citizens will be required to comply with strict new rules regarding the protection of personal customer data.

The GDPR refers to the term “personal data” to discuss information about individuals. There are two types of personal data and they cover different categories of information:

Personal data can be anything that allows a natural person to be directly or indirectly identified. This may be a name, an address, or even an IP address. It includes automated personal data and can also encompass pseudonymised data if a person can be identified from it.

GDPR calls sensitive personal data as being in 'special categories' of information.

These include trade union membership, religious beliefs, political opinions, racial information, and sexual orientation.

Both personal data and sensitive personal data are covered by GDPR.

- Personal data, a complex category of information, broadly means a piece of information that can be used to identify a person. This can be a name, address, IP address... you name it.
- Sensitive personal data encompasses genetic data, information about religious and political views, sexual orientation, and more.

These definitions are largely the same as those within current data protection laws and can relate to information that is collected through automated processes.

Where GDPR differentiates from current data protection laws is that pseudonymised personal data can fall under the law – if it's possible that a person could be identified by a pseudonym.


GDPR
6 THINGS TO KNOW
1
25 MAY 2018
GDPR is a set of privacy laws coming into effect on 25 May 2018 that focus on the proper handling of the personal data of EU citizens
2
GRANULAR CONSENT
Your Stakeholders must know what they are signing up for and what will they receive.
Your data collection and privacy policy must be clear and upfront (not hidden in general terms and conditions)
3
RECORD MANAGEMENT
You have to keep records of consent from your Stakeholders.
You must enable Stakeholders to easily get a copy of all data you store on them, to manage their subscriptions and request permanent deletion.
4
EXISTING DATA
GDPR applies to existing data as well.
You need a process in place to get all your existing records centralized and categorized, a management plan to obtain and record consent (if you don't already have this).
5
DATA BREACHES
You should have a procedure in place to detect, report, and investigate breaches in personal data
6
PRIVACY POLICY
Your Privacy notice must be GDPR-compliant
www.darzin.com

Key Clauses & their Implications

A look at some of the key clauses in the GDPR and what implications they have within a Public Consultation context.

Lawful basis of processing

WHAT IT MEANS	HOW DARZIN HELPS
You need to have a legal reason to use Stakeholder personal data. That reason could be consent (they opted in) with notice (you told them what they were opting into), performance of a contract (e.g. they are your customer and you want to send them a bill), or what the GDPR calls "legitimate interest" (e.g. they are a customer, and you want to send them directly related information).	Darzin makes it clear exactly when and where each stakeholder record was created – the project that "owns" the record. If you also keep records of how/why/when you obtained consent, then this requirement would be satisfied. Keep a record against each stakeholder (in Custom Fields) to document the 'legitimate basis'.
You need the ability to track that reason (also known as "lawful basis") for a given contact.	Use the About field in Darzin to record any changes to Consent or Records (as well as editing their actual subscription as requested)
Public sector customers are likely to use "public task" as their lawful processing basis. This reduces the requirements of consent.	

Consent

WHAT IT MEANS	HOW DARZIN HELPS
One type of lawful basis of processing is consent with proper notice. **In order for Stakeholders to grant consent under the GDPR, a few things need to happen:** • **They need to be told what they're opting into. That's called "notice."** • **They need to affirmatively opt-in (pre-checked checkboxes aren't valid). Filling out a form alone cannot implicitly opt a person into everything your company sends.** • **The consent needs to be granular, meaning it needs to cover the various ways you process and use the stakeholders personal data (e.g. marketing email or sales calls). You must log auditable evidence of what the stakeholder consented to, what they were told (notice), and when they consented.**	Use Custom Fields on Stakeholders to track: - Consent obtained - Date of Consent - Granularity of consent (what exactly did they sign up for) - How consent was obtained - Date Consent was updated (if relevant) If you are unsure about an existing stakeholder's consent, mark that stakeholder as "unsubscribed" in Darzin until you get formal confirmation of consent.

Withdrawal of consent

	WHAT IT MEANS	HOW DARZIN HELPS
Withdrawal of consent (or opt out)	Stakeholders need the ability (as data subject) to see what they've signed up for, and withdraw their consent (or object to how you're processing their data) at any time. In other words, withdrawing consent needs to be just as easy as giving it.	Use the Unsubscribe function on the stakeholder page to unsubscribe a stakeholder from your future correspondence. Use the Stakeholder report (R21) to provide a stakeholder with the detail you are currently storing on them.
Deletion	Stakeholders have the right to request that you delete all the personal data you have about them. The GDPR requires the permanent removal of a stakeholder from your database, including email history, interactions, survey responses and more.	You will be able to perform a GDPR-compliant permanent delete via a support ticket. In the near future we will make this function available to Administrators on your account as well. Currently you need to submit a request to Darzin via the support desk for a Hard Delete of a stakeholder's records. Darzin will respond to the request within 48 hours. You can make a stakeholder inactive when you flag them for deletion, or delete their record yourself (soft delete) until the Hard delete is completed.

Data handling

	WHAT IT MEANS	HOW DARZIN HELPS
Access and portability	Stakeholders can request access to the personal data you have about them. Personal data is anything identifiable, like name and email address. If a stakeholder requests access, you (as the controller) need to provide a copy of the data, in some cases in machine-readable format (e.g. CSV or XLS). Stakeholders can also request to see and verify the lawfulness of processing (see above).	Use Report 21 for full details of the data you are storing on a stakeholder – including custom fields where you will have stored details of their consent. Or you can run an export to excel for a full history of a stakeholder and their details in a machine-readable format
Data processing	The GDPR regulates the exportation of personal data outside the EU.	Darzin uses multiple data centres, one of these is located in the European Union.
Modification	A stakeholder can ask your company to modify their personal data if it's inaccurate or incomplete. You need to be able to accommodate that modification request.	You can edit a stakeholder's detail at any time in Darzin (and edits to a record are tracked and auditable). Keep a note in the "About" field in Darzin to make it clear to your team members that a modification has been made at the Stakeholder's request

Security Measures

WHAT IT MEANS	HOW DARZIN HELPS
The GDPR requires a number of data protection safeguards related to encryption at rest and in transit, access controls, etc.	As part of Darzin's approach to the GDPR, we're strengthening our security controls across the board. We're migrating our servers to Microsoft Azure UK which provides enhanced security and supports GDPR compliance. In addition to industry standard practices around encryption, we are also improving our systems for authentication, authorization, and auditing to better protect our customer's data. We will provide additional details on these security measures as they are implemented.

Tips for Consultors –to ensure your processes are compliant

What measures can you as a Consultor take to ensure that your processes and systems are compliant with each of the requirements of the GDPR?

Who is responsible?

The GDPR also specifies different responsibilities for the different types of entities that handle personal data – the controllers and processors. Here's what they mean:

CONTROLLER (THAT'S YOU, THE CLIENT)

A controller is an entity that decides the purpose and manner that personal data is used, or will be used

PROCESSOR (THAT'S US – DARZIN SOFTWARE)

The person or group that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data

RIGHT	The Right to be informed
REQUIREMENT	To provide processing information to Consultees.
SUGGESTED APPROACH	The use of a privacy note. The note should provide transparency over how personal data will be used (e.g. who controls and processes it).
DESIGN CONSIDERATIONS	Information in the privacy note should include:- • your purposes for processing personal data; • your retention periods for that personal data, and who it will be shared with. There are strict requirements about the *legibility* of these statements, particularly in terms of ensuring that children understand them. The privacy note should contain the *lawful basis* for processing.
IMPLICATIONS FOR CONSULTATION	Consultors will need to disclose more information. Consultors must provide privacy information to Consultees at the time their personal data is collected. For example:- • As a web page / linked in the header or footer of other web pages; • At the start of consultation exercises /the narrative before Consultees have responded; • At the end after the Consultee has responded.

RIGHT	The Right to consent
REQUIREMENT	The GDPR sets a high standard for consent. For public tasks, the processing must be necessary (if you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply).
SUGGESTED APPROACH	Most of the time, we anticipate that the lawful basis for data processing for the purposes of formal consultation is "public task" -which excludes some of the requirements around processing consent. This lawful basis can also be used by the private sector if working on behalf of a public-sector organisation that is consulting - but it will not apply to views gathered during observations or issues papers which are solicited during pre-consultation. This is because the legal basis is directly related to the law which is being exercised.
DESIGN CONSIDERATIONS	• Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent. • Explicit consent requires a very clear and specific statement of consent. • Keep your consent requests separate from other Terms and Conditions. • Make it easy for people to withdraw consent and tell them how. • Keep evidence of consent – who, when, how, and what you told people. Children under 16 cannot give consent. Special consent is required for equalities data.
IMPLICATIONS FOR CONSULTATION	You must keep clear records to demonstrate consent if it is the lawful basis on which data is processed (consent management). Formal consultation is likely to be considered a "public task" which means the burden on consent is diminished but this is not the case for pre-consultation engagement.

RIGHT	The Right of Access
REQUIREMENT	Individuals have the right to obtain confirmation that their data is being processed, and access to their personal data.
SUGGESTED APPROACH	Receipts for transactions (e.g. a submission number or ID and providing a copy of Consultee consultation responses when possible).
DESIGN CONSIDERATIONS	Consultees will need to be clearly identifiable by reasonable means for the request to be authenticated. All attributable data will need to be easily extracted from responses. The information should be provided **free of charge and within one month of the request**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
IMPLICATIONS FOR CONSULTATION	There is a transfer of power to the Consultee in terms of exercising their rights on the personally identifiable data that is held. Consequently, there is an added burden when thinking about how data will be handled or how these requests will be processed, or if and how consent was gained. In this sense, digital systems - such as Darzin - which help Consultors log and analyse interactions, may be beneficial in terms of processing requests and providing Consultees with evidence of their submissions.

RIGHT	The Right to Rectification
REQUIREMENT	Individuals are entitled to have personal data rectified if it is inaccurate or complete.
SUGGESTED APPROACH	Introduce a more flexible approach to responses and two additional types - *Replacement responses* and *removed responses* (removed responses are no longer processed).
DESIGN CONSIDERATIONS	Consultees will need to be clearly identifiable by reasonable means for the request to be authenticated. Requests must be fulfilled within one month.
IMPLICATIONS FOR CONSULTATION	Consultors will need to have an audit trail of removed responses (and reasons why). Ideally, Consultees can edit their own details as stakeholders in the process. Consultors will need to think about their ability to audit stakeholder records. The notion of a stakeholder database or Consultee portal is compelling in terms of self-service.

RIGHT	The Right to be forgotten
REQUIREMENT	An individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. There is an emphasis on the right to have personal data erased if the request relates to data collected from children.
SUGGESTED APPROACH	The GDPR specifies two circumstances where you should tell other organisations about the erasure of personal data:- * the personal data has been disclosed to others; or * the personal data has been made public in an online environment (for example on social networks, forums or websites). The right to erasure does not apply if processing is necessary for the establishment, exercise or defence of legal claims.
DESIGN CONSIDERATIONS	Consultees will need to be clearly identifiable by reasonable means for the request to be authenticated. The enforcement of this right will depend on this will be limited for certain types of consultations. Requests must be fulfilled within a month.
IMPLICATIONS FOR CONSULTATION	Consultors should have the ability to erase part of all of an attributable response. Consultors are likely to want to retain information until after the window for judicial review.

RIGHT	The Right to restrict processing
REQUIREMENT	Where processing is restricted you are permitted to store the personal data but no further processing of it. You can retain just enough information about the individual to ensure that the restriction is respected in the future. This is not an absolute right and only applies in certain circumstances.
SUGGESTED APPROACH	Consultors will need to decide on additional factors relating to personally identifiable data such as a retentions policy etc. Traceability of how the information has been used will be important.
DESIGN CONSIDERATIONS	Bear in mind that, ordinarily, attributable consultation responses are those which arrive by specific routes such as email. However, that is not to say that attributable data is used during processing.
IMPLICATIONS FOR CONSULTATION	Consultors often ask if they can retain contact details for the purpose of following-up comments or "feed-forward" at the end of the consultation. GDPR may introduce a reason why this is no longer a favourable approach.

RIGHT	The Right to data portability
REQUIREMENT	Individuals can obtain and reuse their personal data for their own purpose across different services. Individuals can move, copy or transfer personal data easily between IT environments in a safe and secure way, without hinderance to usability.
SUGGESTED APPROACH	You must provide the personal data in a structured, commonly used and machine-readable form. Open formats include CSV files.
DESIGN CONSIDERATIONS	Consultees will need to be clearly identifiable by reasonable means for the request to be authenticated. Consultation responses (where online) should be exportable to a compatible format (such as Excel).
IMPLICATIONS FOR CONSULTATION	Any technology solutions that handle Consultee data must have easy data import and export capabilities. (Note: Darzin Software does have this easy import/export)

RIGHT	The Right to object
REQUIREMENT	Individuals have the right to object to processing on grounds related to their particular situation.
SUGGESTED APPROACH	Using requests.
DESIGN CONSIDERATIONS	Consultees will need to be clearly identifiable by reasonable means for the request to be authenticated. This right is complex as the organisation may be conducting research where the processing of personal data is necessary for the performance of a public interest task and does not therefore have to comply with an objection to the processing.
IMPLICATIONS FOR CONSULTATION	Consultors need the ability to invalidate a record based on an objection and handle data requests

RIGHT	The Right related to automated decision making and profiling
REQUIREMENT	The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.
SUGGESTED APPROACH	This would be a feature of the privacy note and additional/explicit opt-in questioning.
DESIGN CONSIDERATIONS	Analytics services are personal data agnostic. Analytics services are based on analysing large sets of free text data/images. This means that, while processing personal data is not the core point of the Analytics Services, it is likely that there is personal data in the database. As far as consent and data use is concerned, these will be effectively covered by the terms and conditions and privacy notices of each of these software tools.
IMPLICATIONS FOR CONSULTATION	If you choose to use automated decision-making tools as part of the analysis of consultation responses then we recommend making Consultees aware of them and asking for their consent.

RIGHT	Data Security
REQUIREMENT	Personal data shall be processed in a manner that ensures appropriate security of personal data, including protect against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
SUGGESTED APPROACH	System safeguards and security policies/engineering standards.
DESIGN CONSIDERATIONS	Look at standards such as ISO 27001:2013 compliance. (Note: Darzin data centres are fully compliant)
IMPLICATIONS FOR CONSULTATION	Think about multi-factor authentication for online data and end to end encryption of online submissions. Consultors may wish to get assurances from service providers about their security arrangements and/or evidence of adequate conformance or testing - such as penetration testing.

RIGHT	Limit international transfers
REQUIREMENT	The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.
SUGGESTED APPROACH	Care over where data is held for collection & processing.
DESIGN CONSIDERATIONS	Due to existing legislation known as EU-US Privacy Shield, US organisations (including social media application providers) can self-certify and commit to this framework agreement which underpins their protection of EU citizen data entrusted to them. However, they are grey areas in terms of the adequacy of this.
IMPLICATIONS FOR CONSULTATION	To avoid confusion and additional notification burdens, we think that it is always best to collect and process data in your own country/territory This means avoiding digital services which have distributed data centres in several countries or in the USA (e.g. SurveyMonkey). Note that for European customers, Darzin Survey system is part of our application and all data in processed and held within the UK.

Readiness Checklists

How well prepared are you for the 25th of May when the GDPR comes into effect? Use these handy checklists as a guide for reviewing your data, your systems and procedures.

Checklist – Part A

- [ ] Have you identified all locations where you are storing and using Private information? (Remember the GDPR applies to existing data as well.)
  - [ ] Is the legitimate purpose and consent for the existing data clearly identified and documented?
  - [ ] Is your existing data stored with adequate security of storage (encrypted at rest and in transit), security of access, monitoring and transparent tracking of where the data is used?
  - [ ] How quickly and accurately could you comply with a request for deletion of a Stakeholder's record, or for modification of a record?
  - [ ] Are you able to provide a stakeholder with full details of all the information you have stored on them and all the areas in which their information has been used? This could be across multiple consultations if you have shared the list with others in your organisation.
  - [ ] Have you updated your Privacy and data retention policies to ensure they are GDPR compliant?
  - [ ] Have you updated all your data forms to provide granular consent requests?
  - [ ] Have you identified all areas where data is treated as pseudonymised but as a result of other stakeholder lists it may actually be possible to identify the stakeholder? Has this been rectified?

Checklist – Part B

- ☐ Does your organization have sufficient technical measures and processes in place to secure personal and sensitive data?
- ☐ Are your data collection, data processing, and supporting technologies built to include privacy and protection principles?
- ☐ How much of your personal and sensitive data is currently encrypted both at rest and in transit?
- ☐ How would you describe your organization's process for classifying and labelling end user sensitive data? Is it automated or manual?
- ☐ What data protection policies do you use to classify and label sensitive data?
  - Encryption
  - Rights restrictions
  - Visual markings
  - Restricted access
  - End user notifications
- ☐ How much control do you have over access to personal and sensitive data (e.g., physical, remote, etc.)?
- ☐ For which types of data can you apply your control policies?
- ☐ If a data breach occurred, how would your organization be able to respond?
  - ☐ Do you have a process in place to notify data subjects?
  - ☐ Could you notify them within 72 hours?
- ☐ How often does your organization test the effectiveness of technical measures and processes for ensuring security of data processing?
- ☐ How much of your data currently resides in the cloud?

Getting Help

Having a robust Stakeholder Management System like Darzin for managing your stakeholder lists can go a long way towards helping you get GDPR compliant.

As Data Processors, Darzin takes responsibility for ensuring that the data is stored in secure ways, it is encrypted at rest and in transit, tracked, and more.

Darzin also gives you the ability to

- Manage the consent for each stakeholder, at a granular level
- Control - restrict access to records where necessary
- Transparency of tracking how and where a stakeholder's information has been used
- Easy way to create a report on all data that is help on a Stakeholder
- Easy ability to provide the data in a structure, machine-readable format through the easy import and export of Stakeholder details
- Full audit tracking
- Protection of the data from accidental loss, damage or destruction
- Secure storage and transit of data, within UK/EU boundaries

If you'd like to learn more about how Darzin can help you get compliant with the GDPR requirements, please do get in touch with us at info@Darzin.com. We're not legal experts in this but we do understand consultation and data protection....and we will do our best to help you!

www.Darzin.com
+44 20 87206580 +612 94117400
71-75 Shelton Street, Covent Garden, London WC2H 9JQ