CONTENTS

DISCOVER, MANAGE, REPORT, PROTECT.

2 What is GDPR and when is it happening?
3 Key changes you should know about
4 Strategy for getting started
5 Discover
6 Manage
7 How we’re managing GDPR requirements at Jadu
13 Tips to meet requirements
14 How secure is the data you hold?
15 Report
16 GDPR checklist
**WHAT IS GDPR?**

The General Data Protection Regulation (GDPR) applies to organisations who have a day-to-day responsibility for data protection. It imposes new rules on organisations that offer goods and services to people in the EU, or that collect and analyse data connected to EU citizens, no matter where they are located.

This guide will help you understand what needs to be done and how we’re undertaking work in the Jadu Continuum platform to ensure we comply.

**How is it changing?**

1. **Enhanced** personal privacy rights
2. **Increased** duty for protecting data
3. **Mandatory** breach reporting
4. **Significant** penalties for non-compliance

**When is it happening?**

GDPR will apply in the UK from the **25th May, 2018**.

You must be compliant by then.
Key changes you should know about

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

Controls

- Protect personal data using appropriate security practices
- Notify authorities within 72 hours of breaches
- Receive consent before processing personal data
- Keep records detailing data processing

Transparent policies

- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

IT & Training

- Train privacy personnel & employees
- Audit & update data policies
- Employ a Data Protection Officer
- Create & manage processor/vendor contracts

PROCESSOR OBLIGATIONS
Strategy for getting started

Step 1: Discover
Identify what personal data you have and where it resides.

Step 2: Manage
Govern how personal data is used and accessed.

Step 3: Protect
Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches.

Step 4: Report
Keep required documentation, manage data requests and breach notifications.
WHAT information do you hold?
Any identifying DATA:
  • Name, Email address,
  • Social media posts
  • Physical, physiological, or genetic information
  • Medical information
  • Location
  • Bank details
  • IP address
  • Cookies
  • Cultural identity

WHERE is the DATA?
All places that store personal DATA:
  • Emails
  • Documents
  • Databases
  • Removable media
  • Metadata
  • Log files
  • Backups

HOW do you collect and share?
DATA you collect:
  • User accounts
  • Online forms
  • 3rd Party integrations
  • Social media
  • Analytics
  • Advertisements
DATA you share:
  • Data exports
  • Back office integrations
  • Data shared with 3rd parties

This information should be stored for future reference in an inventory of personal data held, and referenced in your privacy policy.
WHAT you need to cover?
GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act (DPA).
Your policies and procedures need to cover:
- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

Ask these questions:
How would you..?
- Process a request to delete someone’s personal DATA?
- Provide DATA where the right to DATA portability is invoked?
- Manage a correction to DATA that you hold?
- Allow access to personal DATA?
- Record consent for DATA to be processed?
- Verify the age of individuals to account for special protection for children?
# How We’re Managing GDPR Requirements at Jadu

<table>
<thead>
<tr>
<th>The Requirement</th>
<th>CMS Feature</th>
<th>Estimated Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The right to be informed</strong></td>
<td>A privacy note can be maintained in the CMS as a document, a link to the privacy note can be added using Navigation Widgets.</td>
<td>Delivered</td>
</tr>
<tr>
<td><strong>The right of access</strong></td>
<td>Local CMS registration provides a standard user home screen with links to update the customer’s profiles. Where using a CMS homepage for the user’s MyAccount, user account widget can be used to display links through to display and edit their account information. Additional Widgets can be used to surface data relevant to the signed in user account where necessary.</td>
<td>Delivered</td>
</tr>
<tr>
<td><strong>The right of rectification</strong></td>
<td>Change details form available to update user account details held locally (when using local CMS registration process).</td>
<td>Delivered</td>
</tr>
<tr>
<td><strong>Right to erasure</strong></td>
<td>User accounts can be deleted on request by an administrator with access to the Marketing section of the CMS.</td>
<td>Delivered</td>
</tr>
<tr>
<td></td>
<td>Login data is governed by a data retention policy and removed automatically after a year.</td>
<td>Delivered</td>
</tr>
<tr>
<td></td>
<td>A possible future feature being assessed is around feasibility to provide a Delete account feature via the MyAccount page (when using local CMS registration process).</td>
<td>TBD</td>
</tr>
</tbody>
</table>

_A privacy note should be provided to individuals, detailing how their data is to be used._

_Individuals should be able to access their personal data, see a privacy notice and receive confirmation that their data is being processed._

_Individuals are entitled to have personal data rectified where it is inaccurate or incomplete._

_This is also known as “the right to be forgotten” and is essentially the right of an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing._
The Requirement

The right to data portability
 Allows individuals to obtain and reuse their personal data for their own purposes across different services.

Right to restrict processing, Right to object
 GDPR grants individuals the right to block processing of their personal data.

Right to object
 Individuals have the right to object to direct marketing and processing for the purposes of scientific/historical research and statistics.

Rights related to automated decision making and profiling
 GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without any human intervention.

Secure handling of personal data
 GDPR places new obligations upon data processors, to control access to data, provide transparent policies and ensure individuals are trained in the proper use of personal data.

CMS Feature

- An export of a user’s details can be created where necessary via the CMS user interface, and trimmed to only the relevant user’s details. Delivered
- Users can consent to marketing activity and opt out from sent emails. The unsubscribe link is sent in the current marketing email functionality (when using local CMS registration process). Delivered
- Use targeting question functionality in marketing to manage a more extensive list of consent requirements than just consent to email marketing campaigns. Delivered
- No automated decision making takes place in the CMS. N/A
- Helper reports to audit administrative users with access to end user’s profile information. TBD
- User details are stored securely in an encrypted form, access to those details via interface is governed by role based access control. Delivered
- Report to identify Control Centre admin accounts that are dormant. Delivered
- Report to identify Customer accounts that are dormant. Delivered

Estimated Release
<table>
<thead>
<tr>
<th>The Requirement</th>
<th>XFP Feature</th>
<th>Estimated Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The right to be informed</strong>&lt;br&gt;A privacy note should be provided to individuals, detailing how their data is to be used.</td>
<td>- A privacy note can be maintained in the CMS as a document, and a link can be added in form instruction, page level instructions or text XYZ in the new form builder.</td>
<td>Delivered</td>
</tr>
<tr>
<td><strong>The right of access</strong>&lt;br&gt;Individuals should be able to access their personal data, see a privacy notice and receive confirmation that their data is being processed.</td>
<td>- Submitted &amp; In progress XFP forms linked to a user account are displayed via XFP homepage widgets that can be displayed on the user account homepage as a self-service task.</td>
<td>Delivered</td>
</tr>
<tr>
<td>- Anonymous XFP forms can be exported by Customer Services / Administrators based on form reference provided.</td>
<td>Delivered</td>
<td></td>
</tr>
<tr>
<td><strong>The right of rectification</strong>&lt;br&gt;Individuals are entitled to have personal data rectified where it is inaccurate or incomplete.</td>
<td>- An XFP form can be created to update the council regarding non-account based information supplied as a new form submission.</td>
<td>Delivered</td>
</tr>
<tr>
<td><strong>Right to erasure</strong>&lt;br&gt;This is also known as “the right to be forgotten” and is essentially the right of an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.</td>
<td>- Form submissions to be able to be deleted on request by an administrator for anonymous form users by use of a supplied form reference number.</td>
<td>Delivered</td>
</tr>
<tr>
<td>- Data retention capabilities to be added for non-form linked ad-hoc payments via PayBridge.</td>
<td>Roadmapped June</td>
<td></td>
</tr>
<tr>
<td>- An Administrative user to be able to clear down all of a specific users form data.</td>
<td>Delivered</td>
<td></td>
</tr>
<tr>
<td>- Report on users who have had data cleared down (so that back office systems could be updated separately).</td>
<td>Roadmapped June</td>
<td></td>
</tr>
<tr>
<td><strong>The right to data portability</strong>&lt;br&gt;Allows individuals to obtain and reuse their personal data for their own purposes across different services.</td>
<td>- An 'Administrative' user can generate a form submission report for a specific user account.</td>
<td>Roadmapped June</td>
</tr>
</tbody>
</table>
### The Requirement

<table>
<thead>
<tr>
<th><strong>Right to restrict processing</strong></th>
<th><strong>XFP Feature</strong></th>
<th><strong>Estimated Release</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR grants individuals the right to block processing of their personal data.</td>
<td>- Messaging can be added within the form instructions / page level instructions.</td>
<td>Delivered</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Rights related to automated decision making and profiling</strong></th>
<th><strong>XFP Feature</strong></th>
<th><strong>Estimated Release</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without any human intervention.</td>
<td>- No automated decision making takes place in XFP.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Secure handling of personal data</strong></th>
<th><strong>XFP Feature</strong></th>
<th><strong>Estimated Release</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR places new obligations upon data processors, to control access to data, provide transparent policies and ensure individuals are trained in the proper use of personal data.</td>
<td>- XFP data retention policies can be set at a granular level for registered and unregistered user form submissions and also at a global (all forms) level.</td>
<td>Delivered</td>
</tr>
<tr>
<td></td>
<td>- User details are stored securely in an encrypted form, access to those details via interface is governed by role based access control.</td>
<td>Delivered</td>
</tr>
<tr>
<td></td>
<td>- Restrict the ability to view received forms based on form category classification of administrator account.</td>
<td>Delivered</td>
</tr>
</tbody>
</table>
The Requirement

**The right to be informed**
A privacy note should be provided to individuals, detailing how their data is to be used.

**The right of access**
Individuals should be able to access their personal data, see a privacy notice and receive confirmation that their data is being processed.

**The right of rectification**
Individuals are entitled to have personal data rectified where it is inaccurate or incomplete.

**Right to erasure**
This is also known as “the right to be forgotten” and is essentially the right of an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

**Right to object**
Individuals have the right to object to direct marketing and processing for the purposes of scientific/historical research and statistics.

---

**CXM Feature**

- Obtain consent during user account registration (including display of privacy note).
- Obtain consent for when customer services operatives create a person record (e.g., via the telephone).

- Submitted & In progress CXM cases linked to a user account are displayed via a CXM Cases widget that can be displayed on the user account homepage as a self-service task.

- Changes to existing Case details or User assigned can be provided via a link to an XFP form.

- Customers to be able to update their CXM registered personal details via self-service (currently only partial details can be edited via User account such as name, email and telephone).

- An Administrative user to be able to Remove a customer’s user account (rather than just deactivate).

- An Administrative user to be able to Remove personal data from a customer’s existing case.

- Data Retention policies for removing personal data to be implemented.

- Customers to be able to login and delete their user account via self-service.

- Customers may make their request to object by raising a case or as part of the workflow of an existing case.

---

**Estimated Release**

- Delivered
- N/A
- Delivered
- Delivered
- Before 25th May
- Before 25th May
- Post May
- Post May
- Delivered
<table>
<thead>
<tr>
<th>The Requirement</th>
<th>CXM Feature</th>
<th>Estimated Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The right to data portability</strong></td>
<td>• Semi-automated process for an Administrative user to provide data using CSV case export and manual extraction.</td>
<td>Delivered</td>
</tr>
<tr>
<td>Allows individuals to obtain and reuse their personal data for their own purposes across different services.</td>
<td>• Administrative users will be able to download data for an individual case. This includes: Messages, File attachments and Case values visible to the customer.</td>
<td>Post May</td>
</tr>
<tr>
<td>• Customer logs in to download their data via self-service.</td>
<td></td>
<td>Post May</td>
</tr>
<tr>
<td><strong>Right to restrict processing</strong></td>
<td>• Customers may make their request to restrict processing by raising a case or as part of the workflow of an existing case.</td>
<td>Delivered</td>
</tr>
<tr>
<td>GDPR grants individuals the right to block processing of their personal data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rights related to automated decision making and profiling</strong></td>
<td>• No automated decision making takes place other than those set by rules within a given Case type definition within CXM.</td>
<td>N/A</td>
</tr>
<tr>
<td>GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without any human intervention.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Secure handling of personal data</strong></td>
<td>• User details can be stored securely in an encrypted form where case fields are marked as sensitive, access case fields can be restricted based upon user role type.</td>
<td>Delivered</td>
</tr>
<tr>
<td>GDPR places new obligations upon data processors, to control access to data, provide transparent policies and ensure individuals are trained in the proper use of personal data.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TIPS TO MEET REQUIREMENTS

Check you’re meeting GDPR standards when:

**Asking for CONSENT**

**DO**
1. Be sure the request is prominent
2. Use clear plain language
3. Specify why you need the data
4. Specify what you’re going to do with it
5. Offer granular options to consent to independent processing
6. Inform individuals they can withdraw consent
7. Ensure individuals can refuse consent without detriment

**DON’T**
1. Use pre-ticked boxes

**Maintaining a PRIVACY NOTICE**

**DO**
1. Include contact details of the controller and data protection officer
2. Use easy-to-understand, clear language
3. Explain the purpose and your lawful basis for processing the data
4. Outline who data is shared with and whether it is transferred to other countries
5. Include data retention times and rights of the data subject
6. Inform individuals they can withdraw consent
7. Explain the consequences of failing to provide personal data
HOW SECURE IS THE DATA YOU HOLD?

Review your security measures to make sure you’re processing data securely and up to the GDPR standards.

Three steps to secure your data:

Security
1. Audit who has access to personal data.
2. Test your security regularly.

Encryption
1. Know what data you hold in an encrypted form.
2. Be aware of what encryption algorithm is in use.
3. Ensure any data that should be encrypted - is.

Data breaches
1. Know how to detect a breach.
2. Have the correct procedures in place to detect a breach.
3. Report a breach, ensure you notify DPA as well as customers.

Tips to help protect data:

Consider
- Network security
- Storage security
- Computer security
- Identity management

Access control
- Encryption
- Risk mitigation
You’ll need to record:

- The register of personal data held and where
- Classification of data
- Which 3rd parties have access to the data
- Purpose of processing and holding the data
- Security measures you have in place
- Data retention times

Print and use following checklist to help prepare you for GDPR.
<table>
<thead>
<tr>
<th>Discover</th>
<th>Protect</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data you collect</td>
<td><strong>Encrypted data</strong></td>
<td><strong>Record-keeping</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Stored personal data</strong></td>
</tr>
<tr>
<td></td>
<td>Data breaches</td>
<td><strong>Purpose of processing</strong></td>
</tr>
<tr>
<td></td>
<td>○ Detect</td>
<td>○ Classification of data</td>
</tr>
<tr>
<td></td>
<td>○ Report</td>
<td>○ 3rd parties with access</td>
</tr>
<tr>
<td></td>
<td>○ Investigate</td>
<td>○ Security measures in place</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ Data retention times</td>
</tr>
<tr>
<td></td>
<td>Date of last security test</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date of last access audit</td>
<td></td>
</tr>
<tr>
<td>Data you share</td>
<td></td>
<td>○ East to understand</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manage</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policies &amp; process</strong></td>
<td>○ Be informed</td>
<td>○ Stored personal data</td>
</tr>
<tr>
<td></td>
<td>○ Access</td>
<td>○ Purpose of processing</td>
</tr>
<tr>
<td></td>
<td>○ Rectification</td>
<td>○ Classification of data</td>
</tr>
<tr>
<td></td>
<td>○ Erasure</td>
<td>○ 3rd parties with access</td>
</tr>
<tr>
<td></td>
<td>○ Restrict processing</td>
<td>○ Security measures in place</td>
</tr>
<tr>
<td></td>
<td>○ Data portability</td>
<td>○ Data retention times</td>
</tr>
<tr>
<td></td>
<td>○ Decline automated decisions</td>
<td></td>
</tr>
<tr>
<td><strong>Consent</strong></td>
<td>○ Prominent, not part of T&amp;Cs</td>
<td>○ East to understand</td>
</tr>
<tr>
<td></td>
<td>○ Opt in - Not pre-ticked</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Clear plain language</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Specify what happens to data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Specify why you want data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Named organisations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Can refuse</td>
<td></td>
</tr>
<tr>
<td><strong>Privacy notice</strong></td>
<td>○ Contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Lawful basis for processing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Data transfer details</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Data retention times</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Rights of the data subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Right to complain/withdraw</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ East to understand</td>
<td></td>
</tr>
<tr>
<td><strong>Record-keeping</strong></td>
<td>○ Stored personal data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Purpose of processing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Classification of data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 3rd parties with access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Security measures in place</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Data retention times</td>
<td></td>
</tr>
</tbody>
</table>
Any questions?

Do you have anything you would like to ask us regarding the impact GDPR may have on your organisation or Jadu? Simply send us an email.

marketing@jadu.net

Useful resources:

www.jadu.net/gdpr
Blog post: Yep - those 4 letters ‘GDPR’
Blog post: Jadu Continuum Platform and the GDPR
ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf