Getting your sites ready for GDPR

Heather Burns for WP Glasgow • 23 January 2018

GDPR overview

Deadline day

25 May 2018 (122 days…)

What it does

- Replaces the 1995/1998 DPA
- Preserves existing principles
- Expands and modernises

After Brexit

- GDPR will remain the UK's data protection standard
- Data Protection Bill currently winding its way through Parliament
- Equivalence is necessary

What is personal data?

Personal data

- “Any information relating to an identified or identifiable natural person.”
- This can be one piece of information or multiple data points combined to create a record.

Sensitive personal data

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life or sexual orientation
- Past or spent criminal convictions

1995: eight principles of data protection

Personal data must be:

- Processed in a manner which is fair and lawful;
- Used only for the manner in which it was intended to be used;
- Processed in a manner which is adequate, relevant, and not excessive;
- Accurate and kept up to date;
- Not kept for longer than its intended purpose;
- Processed in accordance with the rights of the people the data is about;
- Protected by technical and organisational security measures;
- Not transferred to third countries outside the EU which do not guarantee an adequate measure of data protection.

GDPR is an opportunity to...

- Improve your internal processes
- Maintain your competitive advantage
- Protect your users from data risks
- Protect your users from political uncertainty

What you have

How you engage

How you work

What you have

Awareness

The most basic step involved in GDPR compliance is **awareness**.

You can create a culture of healthy data protection by involving everyone in awareness of the ways the law is changing and how these changes will impact your work.

Awareness

- Do you understand what GDPR continues from the old Data Protection Act, and what is new?
- Are you confident that you are compliant with the existing Data Protection Act?
- Do your staff receive data protection training, and is that documented?
- Have you allocated appropriate human and technical resources to GDPR implementation both before and after May 2018?
- Have you spoken with your contractors and suppliers about their own GDPR implementation plans?

Documentation

The next step in your GDPR journey is auditing **what information you hold and process**, where it is stored, what kinds of data it comprises, and whether it is still needed.

If your data collection and processing is regular (meaning it is a core part of your business), includes sensitive personal data, or could threaten people's rights and freedoms, you must keep a full record of all of your data collection and processing activities.

Documentation

In-house

- What information do you hold online?
- What information do you hold offline?
- What information do you hold in archives?

External

- What information do you share with third parties?
- What information do you receive from third parties?

Auditing your data

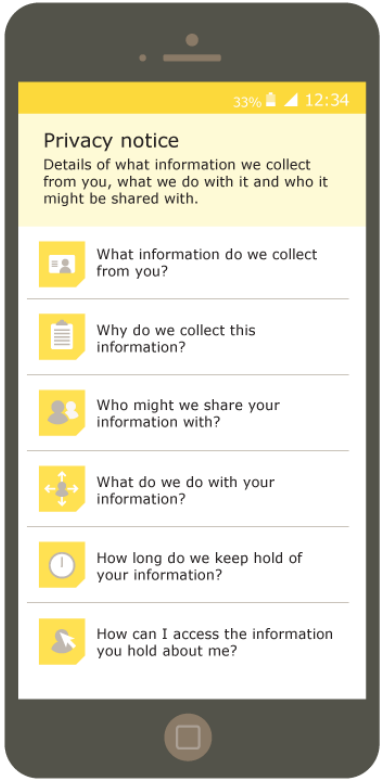
What you collect	Describe what data you collect, about whom, in what categories
Why you collect it	What you need it for, and if that's by consent or lawful basis
What you planned	Any Privacy Impact Assessments you have carried out
How you protect it	Technical/security measures; breach reporting; deletion
Who receives it	Third parties and partners; international transfers and safeguards
Who processes it	Documentation of staff training (HR)

Privacy notices

Under the previous data protection regime, privacy information notices become long, lazy, and legalistic.

GDPR reclaims privacy notices as concise, transparent, and intelligible dialogues with your users.

Everything you are doing with your users' data - *everything* - needs to come out into the open.



Privacy notices

Ensure that yours are:

- Written in plain English, with no “legalese”;
- Broken down into clear sentences and short paragraphs;
- Contain granular, non zero-sum options

Ensure that you:

- Review the privacy notices of the third parties you sent data to, or receive data from
- Include all the information and any formatting required…

Information required

The data itself	What data is collected, how data is processed, how data is used
Why you collect it	Consent or lawful basis
Who it is shared with	Specific named parties, what you share and why you share it
What rights users have	Subject access requests, complaints
Clear options	For consent, individual rights, and subject access requests
Your information	Contact details for your business and your DPO

Information about children

Ensure that you

- Provide extra safeguards for under-16s data
- Document evidence of parental consent
- Delete minors' data with no hassle

If you are collecting data directly from children, your privacy notices must be written in a way they can understand. This includes information about how you are using their data as well as the consent process.

How you engage

Individual rights

We have always had rights over the uses of our information under the existing data protection regime. Under GDPR these **individual rights** are greatly expanded.

For you, this means respecting those rights, implementing them into your planning structures, and being prepared to meet users' invocation of these rights in an open and fast way.

Individual rights

- The right to be **informed** about what you are doing with data through privacy notices
- The right of users to **access** a copy of the data you hold on them;
- The right to **correct** any data that you hold;
- The right to **erasure**, meaning the right to request deletion of certain kinds of data you hold;
- The right to **restrict processing**, or the right to ask you to stop using data in certain ways;
- The right to **data portability**, or the right to take the data you hold about them to another service provider;
- The right to **object** to your uses of their data; and
- Their rights in relation to **automated decision making and profiling**, including data you use or share for the purposes of advertising, marketing, and behavioral analysis.

Individual rights

How they work

- Individual rights are granular – any one can be invoked at any time
- You cannot charge users any administrative fee for invoking these rights, or any costs for the time you require to meet them

How to meet them

- Publicise these rights in your privacy notices
- Review your internal processes for handling these requests
- Remember time limits

Subject access requests

One way people can invoke their individual rights is known as a subject access request (SAR).

The people whose data you store or process can file a SAR with you to receive

- Confirmation that you are processing their data;
- Access to a copy of the personal data that you hold on them;
- Any other information, such as details of the data you have passed to third parties that has already been confirmed in your privacy notice.

Subject access requests

How they work

- Detail your process in your privacy notices
- Review your third parties' SAR processes
- Review your systems

Internal documentation

- How are SARs tallied in your organisation? Who receives them as the central point of contact? Who is informed of their receipt, their progress, and their completion?
- Is your SAR process documented in a way that would meet ICO approval?

Consent and legal basis

In most circumstances, the data collection and processing you perform must be done with the **consent** of the people that data is about.

If consent is not the basis, your use of data must be grounded in a **legal basis**.

The consent mechanisms and legal bases you use to collect and process data must be clear, documented, and verifiable.

Consent must be…

Consent

You must document

- Who gave their consent;
- How consent was given;
- What information they were given,
- What they agreed to;
- When they consented (ideally a timestamped record); and
- Whether or not the user has withdrawn their consent

Lawful bases for processing data

- Necessary for the **performance of a contract**;
- Necessary to **comply with a legal obligation**;
- Necessary to **protect the person's vital interests** (for example, providing someone with emergency medical help);
- Necessary for **the performance of a task in the public interest** or in the exercise of official authority;
- Necessary for the purposes of the "**legitimate interests**" pursued by the controller or third party.

Preparing for consent and lawful bases

Review your

- Internal documentation
- External privacy notices
- Third party contracts

Modify your

- Consent mechanisms
- Privacy notices
- Data minimisation thresholds

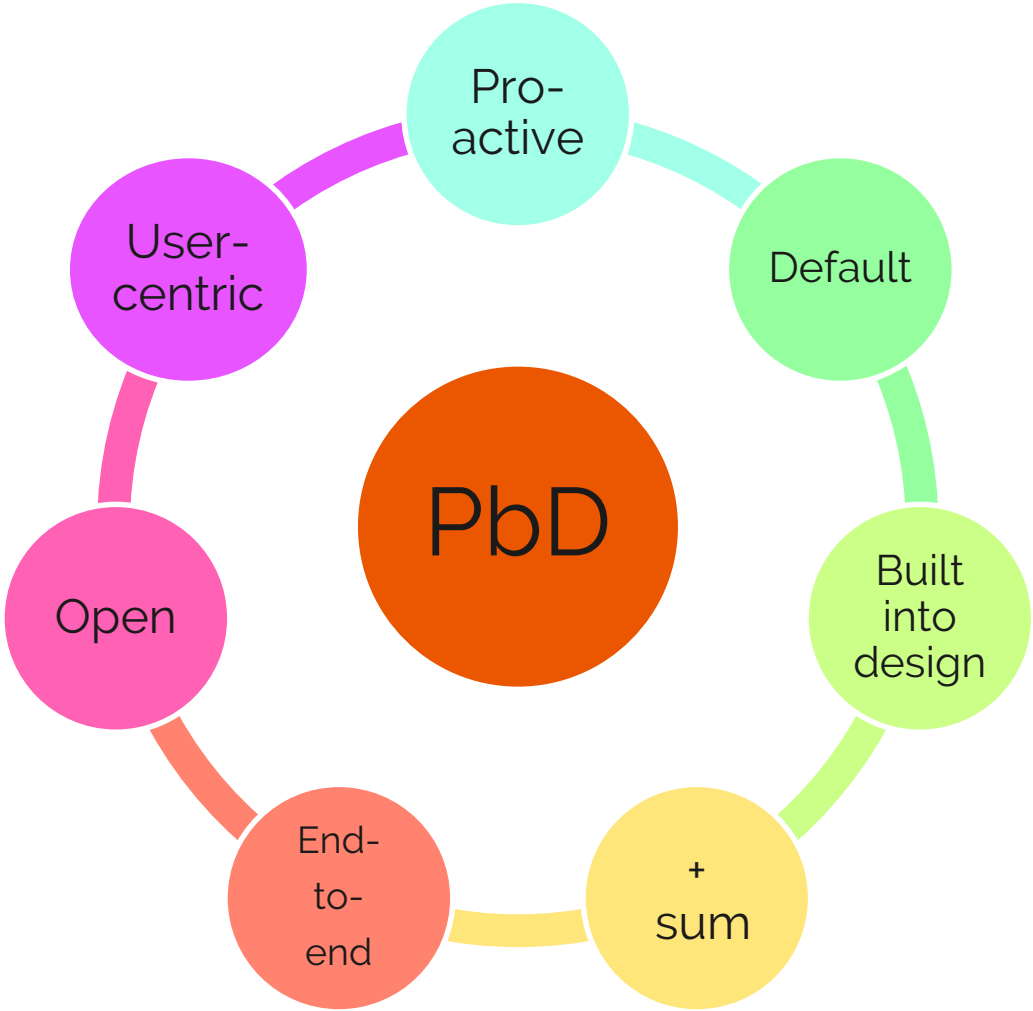
How you work

Privacy by Design / Data Protection by Default

GDPR requires the adoption of a culture of **privacy by design** and **data protection by default**.

This means that all your internal processes and procedures, as well as your external products, services, and applications, must be designed with optimal privacy and data protection built in from the start, not bolted on as an afterthought or made contingent on the user activating a series of options (assuming they had any at all.)

The seven principles of Privacy by Design



Privacy by Design / Data Protection by Default

Cultural integration

- Familiarise yourself with the basic principles of PbD (google “Smashing Magazine Privacy by Design”)
- Review your existing sites, apps, and processes for best PbD practice

Workflow integration

- Adopt the PbD standard
- Create a data minimisation and deletion policy
- Create a Privacy Impact Assessment process for data-intensive projects

A simple Privacy Impact Assessment process

What	What data you are collecting and processing
Why	The necessity of the data collection (consent or lawful basis)
How	How you are acquiring the data, from where, and to where
How much	Evaluate the proportionality of your data processing
In what way	Describe the security precautions you have taken
Risk assessment	The risks to the data subjects, and what you are doing about it

Data breaches

GDPR requires you to do everything you can to prevent data breaches from happening. That said, it also requires you to prepare for data breaches in advance.

Preparing for data breaches requires you to take an honest (and, possibly, quite uncomfortable) look at what aspects of your internal processes and cultures could contribute to a preventable breach.

Data breaches

Technical measures

- Do you regularly audit your systems and processes for potential data breach risks?
- Do you know the criteria for a “high-risk”, reportable breach, as well as the information you would be required to report within 72 hours of discovery?

Human measures

- Do you have an internal reporting mechanism in place to report potential data breaches before they happen?
- Can staff report an issue, either technical or human, which could lead to a data breach, without fear of reprisal?

Data protection officers

GDPR introduces the concept of the Data Protection Officer, or the DPO. For organisations engaging in certain kinds of processing of personal data, the DPO is a named individual who carries legal and professional responsibility for that organisation's GDPR compliance.

You are only *required* to appoint a DPO if you engage in large-scale processing of sensitive personal data. That being said, those businesses which do not strictly *require* a DPO may wish to consider appointing one voluntarily all the same.

Data protection officers

Internal responsibility

- Decide if you a) need one or b) want one
- Give the role the resources and powers it requires

Public accountability

- Publicise your DPO's details in your privacy notices
- Submit your DPO's details to ICO as the point of contact for privacy concerns

Working internationally

One of the fundamental principles of EU data protection law, both past and future, is that personal data cannot be transferred outside of the EU to third countries unless that country ensures an equal and adequate level of data protection.

This creates two issues: the safeguarding of your data at its origin and its destination, and the legal means by which that data moves between them.

Working internationally

Who you work with

- Are all of your partners and third party service providers in non-EU countries working towards GDPR compliance?
- Are your US-based partners and third party service providers Privacy Shield compliant?
- Are you including and requiring GDPR compliance in your contracts with partners and service providers?

Privacy notices

- Are all international transfers of data, and the uses of that data, made clear?
- Have you provided a means for users to object to their data being transferred outside the EU?
- If you work across European borders, have you identified your main country of establishment and lead supervisory authority in your privacy notices?

Here be dragons

#GDPRubbish

- Professional certifications
- “Accredited” courses
- Compliance software
- Consent panic
- DPOs as job creation schemes
- Finesfinesfinesfinesfinesfinesfines

Keep an eye on the whole picture

Further GDPR awareness

Regularly visit ICO's web site for new guidance

The Data Protection Bill

Follow its progress and have your say

The ePrivacy directive revamp

Cookies, metadata, device fingerprinting, marketing consent

Your action plan

1. Learn the basic principles of data protection

2. Raise awareness within your organisation

3. Assess the information you hold

4. Conduct an audit of processing activities

5. Review and revamp your privacy notices

6. Provide for users' individual rights

7. Review your subject access request process

8. Review your consent and legal bases

9. Implement PbD and DPbD principles

10. Prevent data breaches, but prepare for them

11. Decide whether you need a DPO

12. Review international data transfer structures

13. Learn the warning signs of GDPRubbish

14. Keep an eye on legal and political changes

15. Become your organisation's privacy champion

Thank you!

Heather Burns

heather@webdevlaw.uk

@webdevlaw

https://webdevlaw.uk/data-protection-gdpr