IMDRFP/01

GDPR WORDPRESS WEBSITE GUIDE

Discover what's involved in reviewing your WordPress website on its journey to becoming GDPR compliant.

PREPARED BY

Martin Coates
Technical Director

ESSEX
01268 858292

LONDON
020 3355 8747

www.impactmedia.co.uk

impactmedia®

Supporting Your Digital Journey™

TABLE OF CONTENTS

01. INTRODUCTION

WHAT IS GDPR?

The **General Data Protection Regulation** (GDPR) is the new EU regulation coming into force on **May 25th 2018.**

In our fast-moving world of IoT (Internet of Things), personal data can be moved automatically 24 / 7 through a variety of websites, devices and systems, which increases the risk of data breach to an individual's personal data.

The aim of GDPR is to give citizens of the EU control over their personal and sensitive data, in that it changes the approach that businesses need to take towards collecting, managing, storing and processing that data.

GDPR applies to the use of personal data, which relates to a person or "data subject" that can be used to directly or indirectly identify an individual.

After reading this article, you should be receive the following key benefits:

01. Understand what GDPR is and how it could affect your business.

02. Understand what actions need to be taken for your WordPress website.

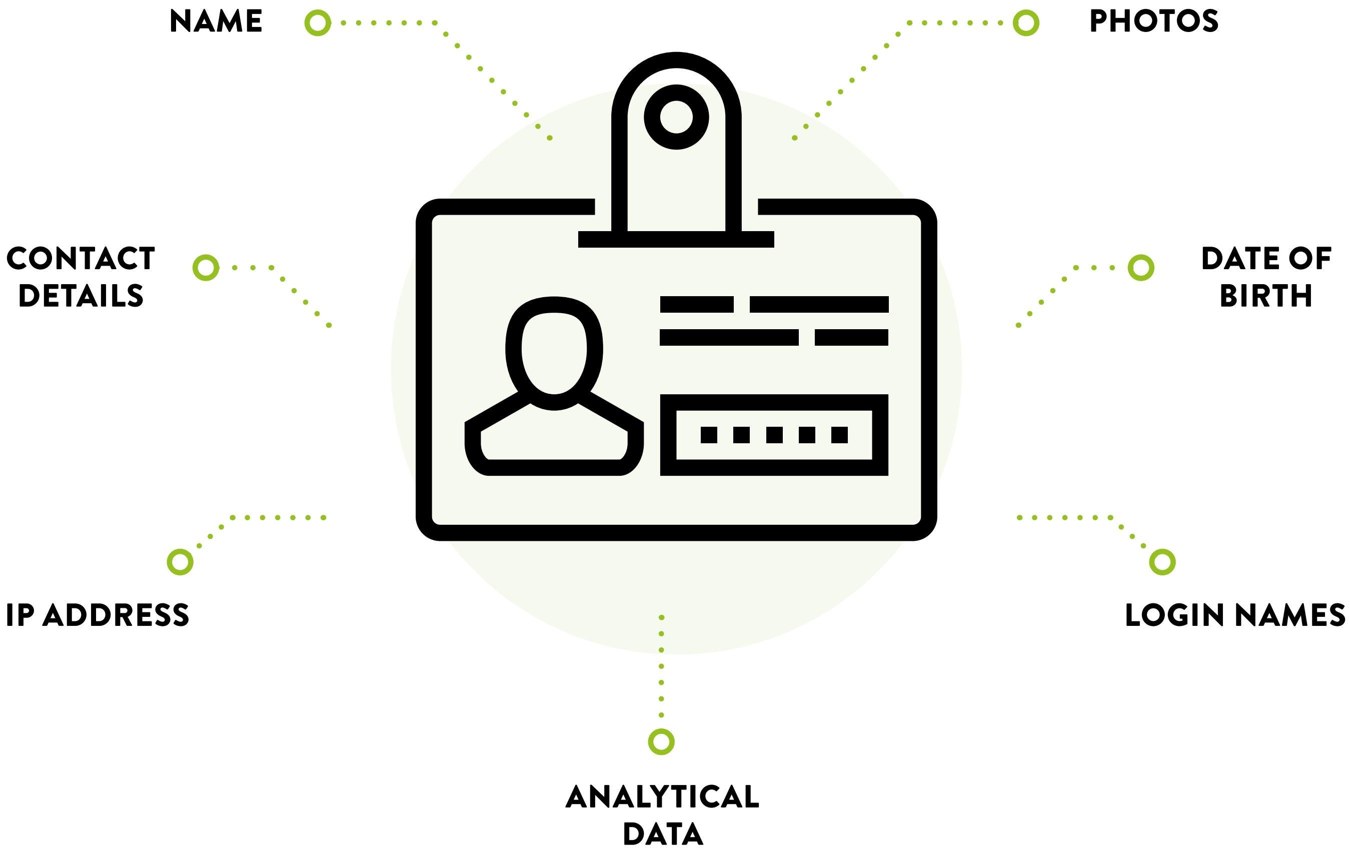
03. Gain access to further resources to help with auditing your WordPress website.

GDPR DEADLINE
25TH MAY 2018

PERSONAL DATA

WHAT IS PERSONAL DATA?

Some Examples of Personal Data



NAME

PHOTOS

CONTACT DETAILS

DATE OF BIRTH

IP ADDRESS

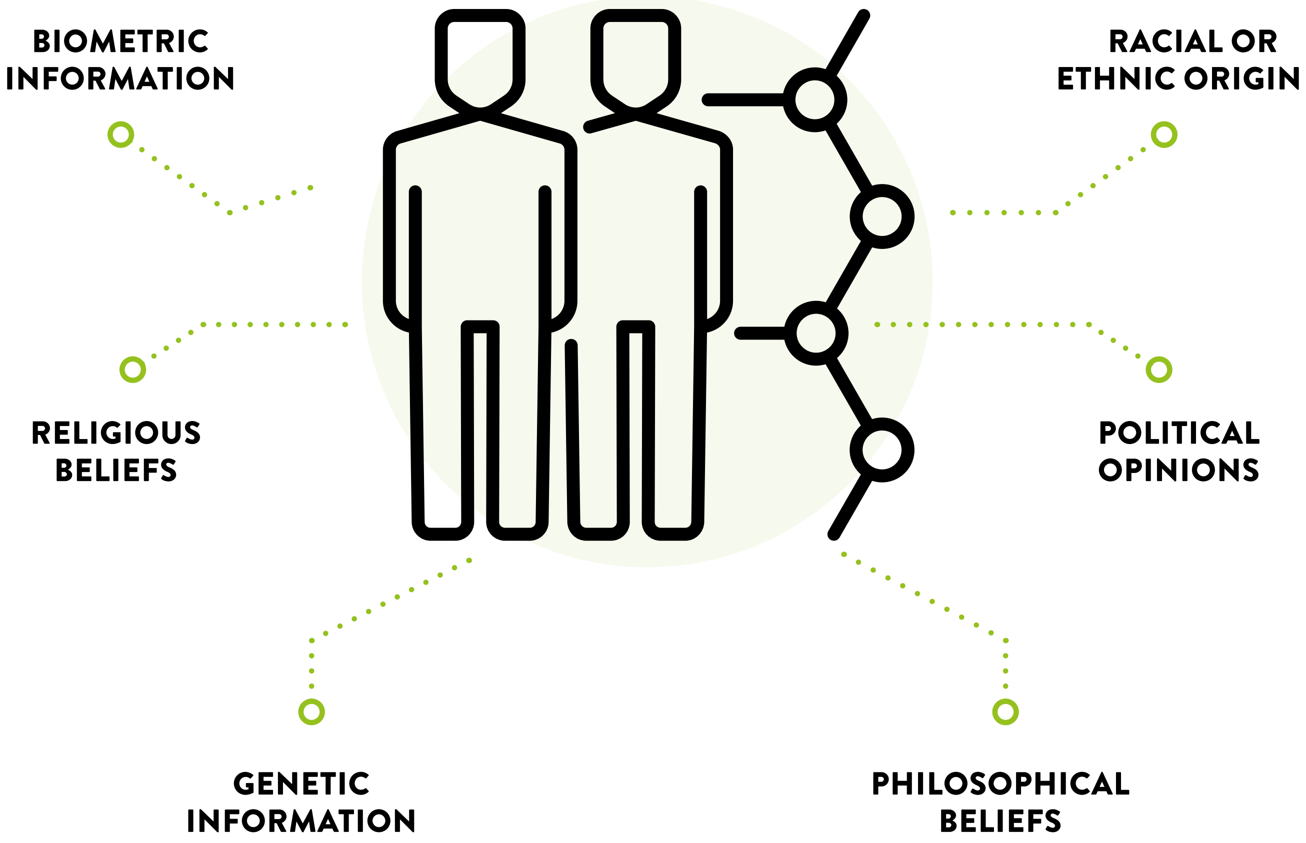
LOGIN NAMES

ANALYTICAL DATA

SENSITIVE DATA

WHAT IS SENSITIVE DATA?

Some Examples of Sensitive Data



BIOMETRIC INFORMATION

RACIAL OR ETHNIC ORIGIN

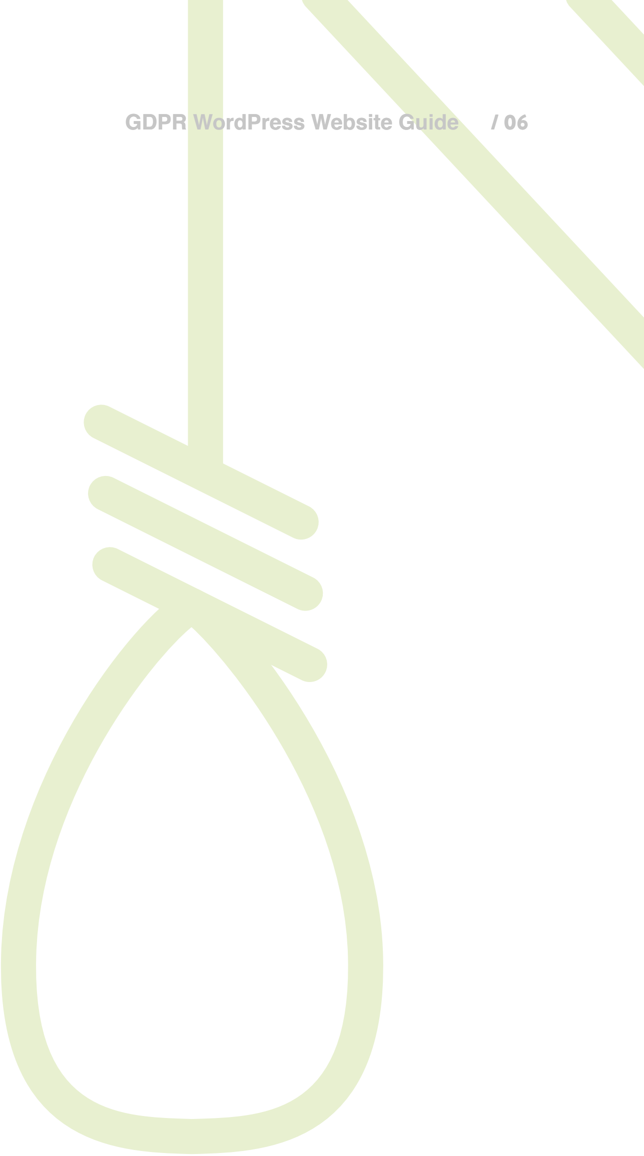
RELIGIOUS BELIEFS

POLITICAL OPINIONS

GENETIC INFORMATION

PHILOSOPHICAL BELIEFS

THE PENALTY FOR BREACHING GDPR.



The ICO state that fines can be as high as 10 million Euros, or 2% of global business turnover, whichever is higher.

More information regarding personal data breaches can be found at the link below:

› https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

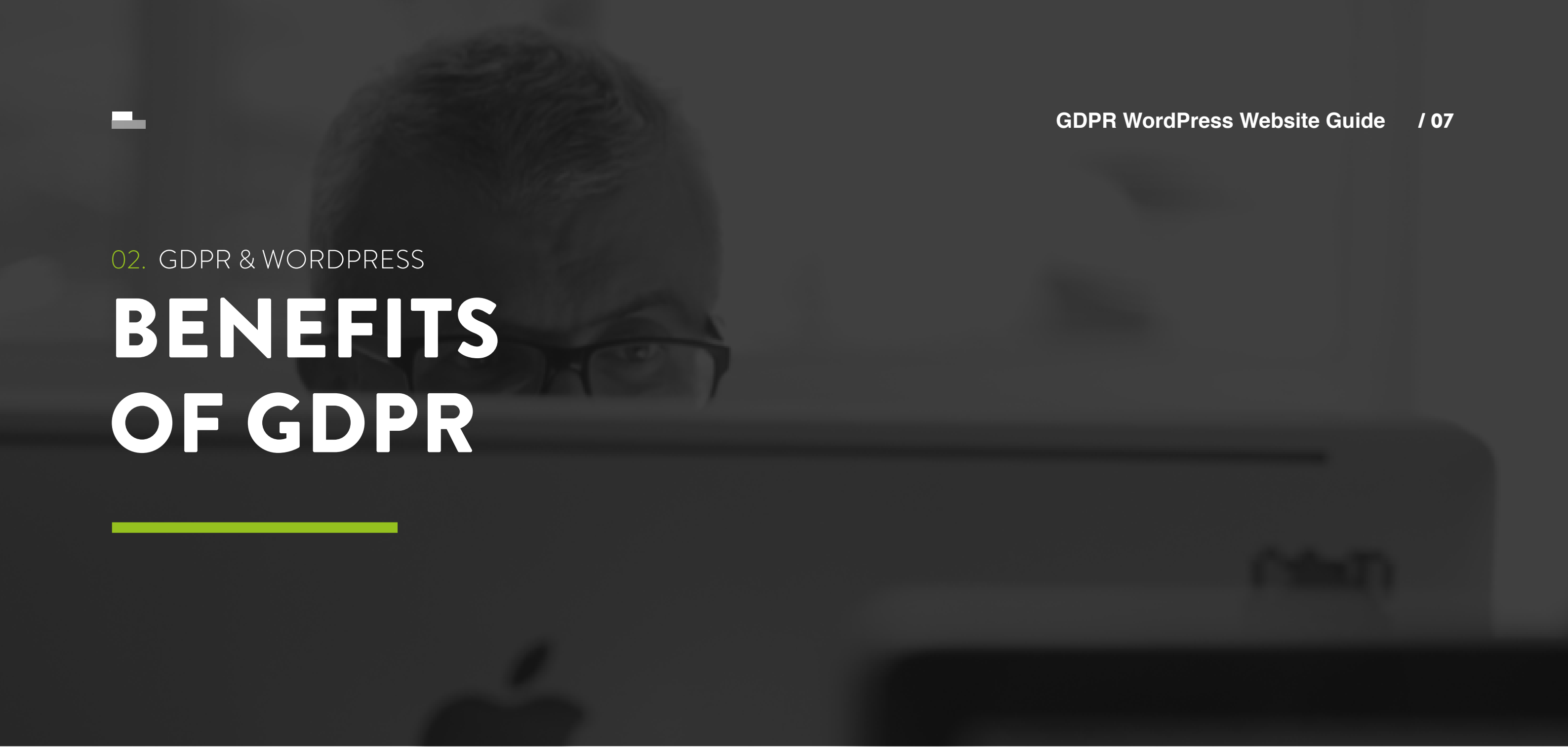
What is a personal data breach?

“A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is about more than just losing personal data.”

› http://www.ico.org.uk

€10M

Companies that breach GDPR can be fined up to **10,000,000** Euros or **2%** of their global annual turnover - whichever is higher.



02. GDPR & WORDPRESS

BENEFITS OF GDPR

Personalised & Efficient Marketing

Under the new law, you will need to ensure the personal data you hold is current, accurate and structured.

Carrying out a data audit on your website will improve the position you have with customers as you build personalised offers for them.

Furthermore, customers who give permission for you to use their data in line with GDPR are more likely to engage with your campaigns.

This should help your business become more efficient in its marketing efforts, and can even lead to higher conversion rates.

Greater Consumer Confidence

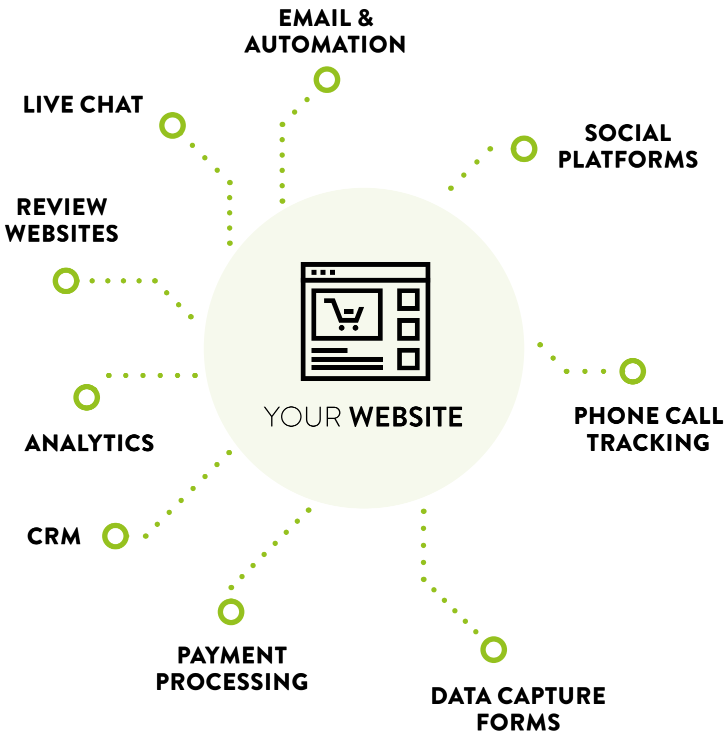
Being transparent how you will collect and use personal data from the outset will help you build more confidence and trust with individuals.

Goodbye Mr Spammer!

In time, as more businesses start to comply, we should hopefully see the downfall of those spammy communications we receive that we know we have never consented to.

GDPR FOR YOUR WEBSITE

Your website may not only be collecting personal data, but possibly also communicating with multiple systems & applications.



A few examples are listed below:

- Live Chat
- Phone Call Tracking
- Analytics
- Remarketing and Targeting
- Payment Processing
- CRM
- Email and Automation
- Social Platforms
- Review Sites
- Affiliate Networks
- Data Capture Forms
- Online Ordering Systems
- User Tracking

50,000

The number of plugins in the **WordPress** repository.

There are over 50,000 plugins in the WordPress repository.

Hopefully this will give you an idea of how much data can be passed through plugins and away from the website to 3rd party applications, such as:

- Job Boards
- Event Booking
- Property Portals
- Hotel & Restaurants Systems
- Travel Booking Systems
- Subscriptions & Memberships
- Financial Feeds
- Insurance Systems

GDPR For Your Website

It's paramount that the following key areas are reviewed in your website:

- **Accountability**
- **Data Collection (Consent)**
- **Data Security**
- **Data Backups & Retention**
- **Data Storage**
- **Right of Access**
- **Data Portability**
- **The Right to be Forgotten**

Accountability

Ensure that a Data Processing Officer is assigned to your business to handle compliance.

Data Collection (Consent)

Review all areas of your website that you collect personal data. This could be from newsletter, download or application forms to name a few.

- Draw a diagram or map of how your website links with other systems.

- Check to ensure you allow users to "Opt In" rather than forcing them to "Opt Out".

- Do not pre select checkboxes on behalf of individuals.

- Be specific to what details you are collected and what you are using them for.

- Allow individuals to easily be able to withdraw consent.

  This could be in the form of unsubscribe links in communications or *"Opt Out"* pages on your website.

- Create privacy & cookie policies defining:

  - What personal data you collect;

  - What legitimate reasons you have for using it;

  - Information on an individual's rights to opt out.

  - Only collect data you <u>need</u> to reduce risk.

Knowing Right from Wrong

It is no longer acceptable to auto enrol users into your mailing lists. You must ask their permission and give them a choice to select or leave unchecked.

☑ Please keep me updated with news & tips

Example shown with box pre-checked.

□ Please keep me updated with news & tips

Example shown with box unchecked.

GDPR For Your Website

Data Security

- Ensure that your website is running optimally with the latest security patches and plugin updates.
- Ensure an SSL certificate is used across the site and with connected external sources to ensure data is encrypted in transit.
- Use a Dedicated Website Firewall. If you don't already use a website firewall solution to protect yourself from attacks, head over to sucuri.net to get protected.
- Where possible, try to mask any personal data with Pseudonymisation techniques.

For example:
Terry Bowden would be replaced with **N9345** in the database.

TERRY BOWDEN

↓

N9345

Data Backups and Restoration

Ensure your WordPress agency manages website backups, including databases, in case the site needs to be restored.

Ensure backup schedules are documented.

Data Storage

It is more than likely that personal data will be stored in more than one database or source. Please ensure you reference all data storage points.

For example:

Your CRM (Customer Relationship Management) system stores personal data, as well as your website. The Email Marketing Solution that your website is linked with also stores personal data in its database.

Please ensure that the systems you integrate with are GDPR Compliant, or at least working towards GDPR Compliance.

GDPR For Your Website

Right of Access

- Data subjects have the right to find out what information is being held and processed.
- This information must be provided free of charge.
- From a website point of view, businesses should provide details on how to obtain this data.
- A possible login to a CRM or GDPR-compliant plugin in the website could provide this data to a user more efficiently.

Data Portability

- Data subjects have the right to obtain their data electronically with the ability to port it to another data controller.

The Right To Be Forgotten

- If you have no legal reason to be storing or processing an individual's personal data then they have a right to be forgotten.
- Streamline the process by creating Opt Out landing pages.
- Apply further procedures to remove data from other systems such as databases, data forms, 3rd party applications and backups.

THE ROLE OF YOUR AGENCY

You may find that you will work with multiple departments and companies on your journey to becoming GDPR compliant.

Unfortunately, the onus is on the business owner to become compliant; however, we can appreciate that there may be some technical expertise required to review what personal data your WordPress website collects and how.

Find out if your WordPress agency may be able to offer you a WordPress GDPR Audit.

The WordPress GDPR Audit

With most websites and businesses using 3rd party systems to collect and process data, a website audit should be carried out.

All contact forms, plugins and 3rd party applications, like payment providers, should be audited to see if they store or process personal data.

By working with your appointed Data Officer, a WordPress development roadmap is proposed to evolve your website towards becoming GDPR compliant.

03. ACTIONS

WORDPRESS GDPR AUDIT

The WordPress GDPR Audit

A typical WordPress GDPR audit would involve the following:

✓ Data Audit

An audit is carried out on your WordPress website to map out:

- What personal data you have collected;
- Where it is held;
- Who holds it;
- What other applications could hold it, and
- How it is processed.

✓ Data Security Check

A data security check is carried out on the website's database to see if Pseudonymisation is in place, Pseudonymisation helps mask personal identifiers, such as by turning "Terry Bowden" into "N9345" with reversible processes in place where applicable.

A further data security check is carried out to ensure all transmission of data is processed using encryption technology.

✓ Data Collection Check

A review of all data capture forms on your WordPress website is carried out to ensure that the data capture is consensual.

✓ WordPress Plugin Check

Your WordPress website will use various plugins to carry out its operations. These will range from Data Capture form plugins through to 3rd party integration plugins like booking systems, recruitment portals etc.

Each plugin is assessed on:

- If it stores or manages personal data;
- Where it is held;
- If the plugin submits data outside the site (i.e into other applications), and
- What further checks may be necessary to ensure compliance.

WordPress GDPR Audit

✓ Data Storage Check

This check provides a list of all areas and possible 3rd party applications that hold data on your behalf.

Where possible, links to 3rd party GDPR policies will be reviewed to ensure they are compliant, or at least working towards compliance.

✓ Rights of Access Check

This is a check to see if your WordPress website provides data subjects with a way to access their data upon request.

✓ Privacy Policy Check

It is a legal requirement to ensure your website has a Privacy Policy in place.

✓ Cookie Policy Check

With today's modern websites, there are normally multiple tracking solutions running behind the scenes such as:

- Google Analytics
- Hot Jar Analytics
- Lead Forensics
- Visual Website Optimiser
- Live Chat Software
- Remarketing & Advertising Tracking.

To ensure GDPR compliance, a cookie policy should define what tracking cookies are being used and how users can opt out of having their data tracked.

✓ Existing Data Check

This check is to ensure the existing data is compliant. If it is not compliant, then recommended steps are provided to assist with becoming compliant.

✓ Data Portability Check

This check is to see if there is a procedure in place that allows data subjects to receive their data.

✓ The Right to Be Forgotten Check

This check is to see if there is a procedure in place that allows data subjects to be removed from your website.

PRIVACY & COOKIE POLICIES

Privacy & Cookie Policy Updates

Once you have mapped out what is actually happening behind the scenes of the website, it's time to update your Privacy and Cookie policies to reflect this.

This area of work may require more technical consultancy from your WordPress agency, but a great set of guidance templates can be found online.

Cookie Lookup Tool

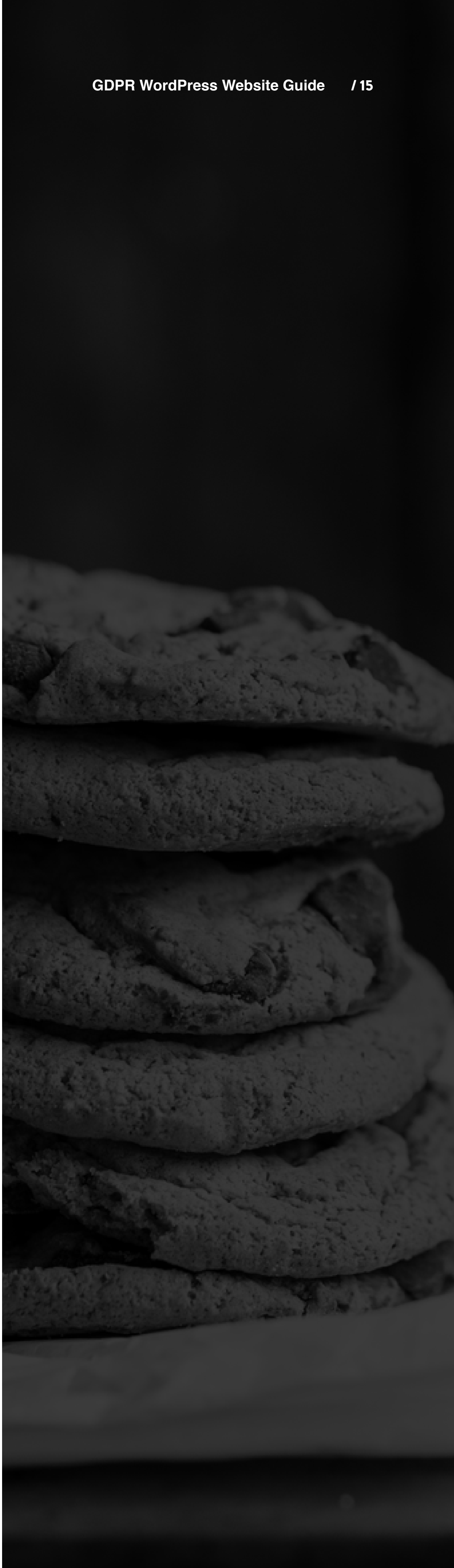
This handy tool will provide website cookie scan abilities, as well as some other great features:

- www.cookiebot.com

Privacy & Cookie Policy Templates

Another great resource for help when compiling updated Privacy and Cookie policies is:

- gdprprivacypolicy.org



IMPLEMENTATION Putting it all into action.

WordPress Audit Actions

Upon review of your WordPress GDPR Audit, there could be development work required to ensure compliance.

This could involve with tasks such as:

- Updating consent notices on data capture forms
- Updating website customer & sales journeys to fall in line with GDPR compliance
- Removing or replacing plugins or 3rd party applications that are not becoming GDPR compliant
- Adding policy pages to the site
- Creating Opt-Out landing pages
- Implementing consent banners

> *“Remove or replace plugins that are not becoming GDPR compliant.”*

04. SUMMARY

GDPR SUMMARY

WordPress GDPR Summary

In review, carrying out this exercise on top of your other daily tasks may feel quite daunting at first.

Once you have mapped out what your website does behind the scenes, it will be much easier to determine what you will need to action next.

The Reward

By making your website GDPR compliant, you will be able to:

- Establish trust with other compliant businesses who are transparent about what data they process and how.
- Ensure appropriate security measures are in place in the event of a data breach.
- Build positive relationships & experiences moving forward to improve business growth.

Resources

The following resources are recommended for further review:

Information Commissioner’s Office

- **https://ico.org.uk/**

GDPR Policy Guidance Templates

- **https://gdprprivacypolicy.org**

Review Website Cookie Data

- **https://www.cookiebot.com**

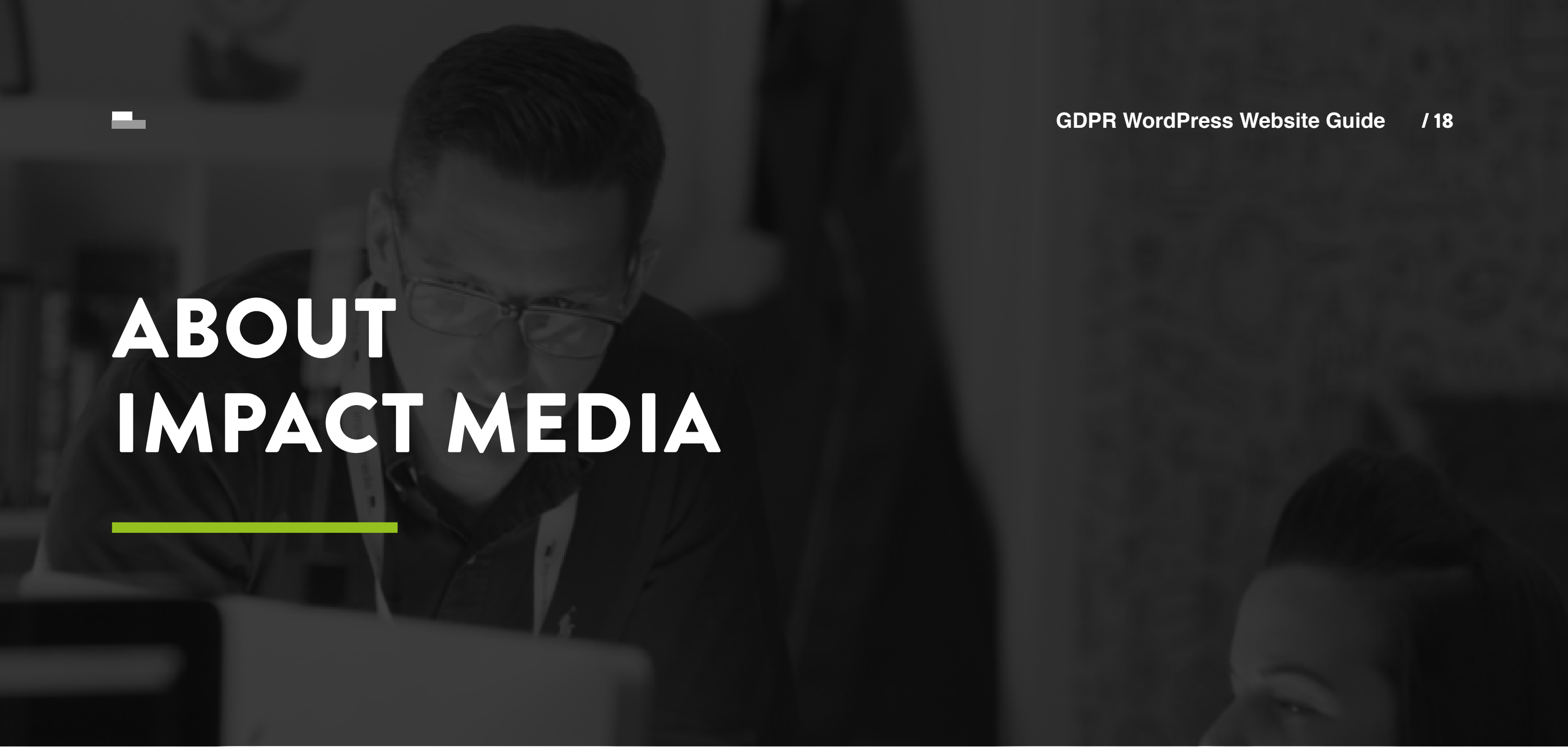
Website Firewall Service

- **https://sucuri.net/**

Disclaimer

This article has been provided with the aim of offering technical assistance from a website perspective.

We recommend seeking legal advice and conducting further research on GDPR via the ICO website to ensure your business fully complies.



ABOUT IMPACT MEDIA

Impact Media are a next-level WordPress agency that specialise in the integration of 3rd party apps & tools with fully bespoke, scalable, WordPress websites.

When your business' ambition exceeds your website's capabilities, a custom approach is required to ensure the website aligns and functions consistently with the company vision.

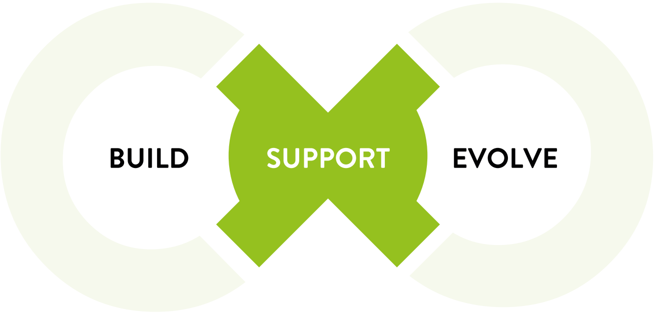
We build websites from the ground up, completely tailored to your business and your goals.

Because of our advanced development capabilities and understanding of WordPress, we can provide unbeatable support and maintenance to help you continue your digital journey.

For more information, please visit our website:
www.impactmedia.co.uk

Or connect with us socially:

Facebook.com/ImpactMedia
Twitter.com/ImpactMedia
LinkedIn.com/company/impact-media



Building, Supporting
& Constantly **Evolving**
WordPress-Powered Websites.

We're WordPress Only

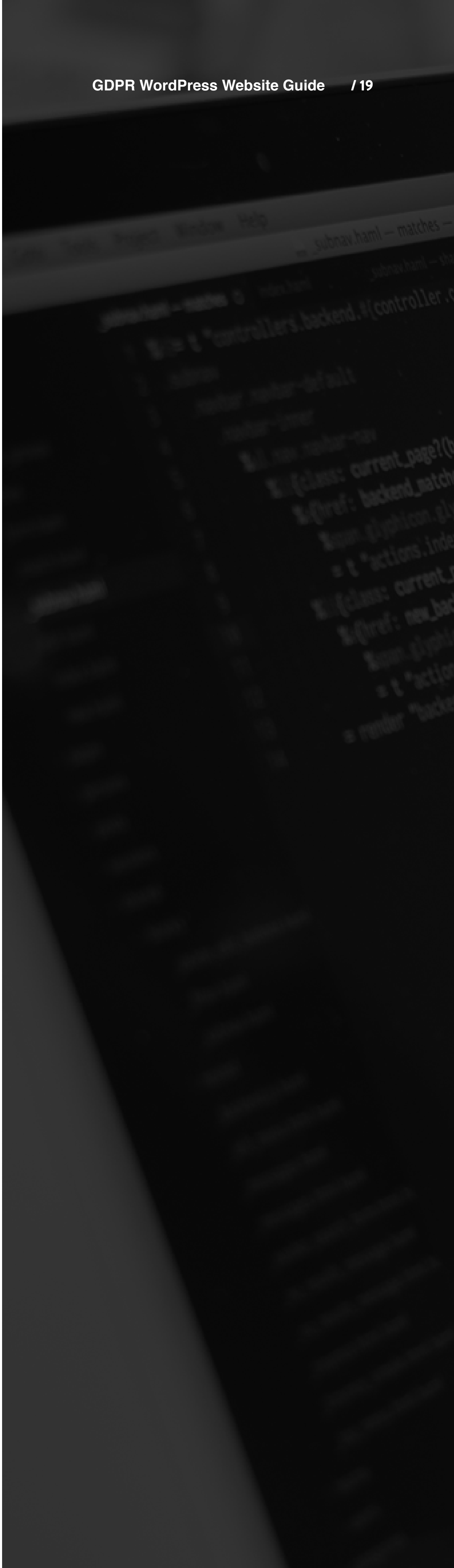
Unlike other agencies, we are solely a WordPress-only company.

We're Not Full Service

Why be average at everything when you can be the best at one thing? You wouldn't pay a plasterer to tile your floor.

15 Years Strong

We started in 2003, so we've been around since before responsive websites and smart phones!



GOT ANY QUESTIONS?

Don’t Be Shy

If you have any questions regarding this document, please feel free to email us.

- gdpr@impactmedia.co.uk

Request An Audit

If carrying out the audit yourself is either too time-consuming or not within yours or your agency’s capabilities, then please get in touch using the details below.

- +44 (0)20 3355 8747
- gdpr@impactmedia.co.uk

About The Author

–

Martin Coates
Martin is Technical Director at Impact Media and has a long history with IT, networking, development and of course WordPress. He’s also known for singing an occasional Robbie Williams number.

linkedin.com/in/martingcoates
m.coates@impactmedia.co.uk

impactmedia®

ESSEX HQ

Woodland Place,
Hurricane Way,
Shotgate, Wickford,
Essex, SS11 8YB

01268 858292
essex@impactmedia.co.uk

LONDON

86 - 90 Paul Street,
Shoreditch,
London,
EC2A 4NE

020 3355 8747
london@impactmedia.co.uk

www.impactmedia.co.uk