GDPR
CHECKLIST

So you have determined that GDPR applies to your business, now what?

b:web

INTRODUCTION

This checklist is for the purposes of enterprises that have determined that GDPR does apply to them because they process personal data (including cookies which often store IP addressees which combined with other data it can be used to identify a real person) for individuals within the EU.

As part of our Website GDPR Compliance Service we complete all sections relating to the website and it's third-parties, you will be responsible for other area's of your business including employees and your Terms of trading with your customers.

The full wording of GDPR can be found here **https://gdpr-info.eu/**

Please note that his checklist has been produced in good faith by b:web and does not replace proper legal advice. As with many area's of the law there can be more than one interpretation of the GDPR documentation.

1. **WHAT DATA** DO I PROCESS AND FOR WHAT PURPOSE?

Please see our blog post here: **https://www.bwebsites.co.uk/gdpr-compliance-small-business/**
A full data inventory should be created for the entire organisations including employees, customers, website users and suppliers.

As part of our Website GDPR Compliance Service we will provide you with a Data Inventory for the website.

2. DO I PROCESS **SENSITIVE DATA**?

Sensitive data is data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data concerning health or data concerning a person's sex life or sexual orientation.

As part of our Website GDPR Compliance Service we will highlight sensitive data processed by the website in the Data Inventory.

3. HOW IS THE DATA COLLECTED COVERED **BY LAW**?

There are a number of reasons that you must legally process data. If any items applies then you can list more than one:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes,
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- Processing is necessary for compliance with a legal obligation to which the controller is subject,
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person,
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

As part of our Website GDPR Compliance Service we will indicate the legal reasoning for all data listed in the Data Inventory.

4. WHAT **THIRD-PARTIES** PROCESS OR CONTROL MY DATA?

You will need to list all Third-party that process or control your data – this can include software services like Mailchimp and also suppliers like Freelancers. You will need to show due-diligence in your checking each third-party for their own GDPR compliance including the physical location of all stored data. There are strict rules on transfers to third parties outside of the EEA. If the company is operating outside of the EEA they maybe covered under the Privacy shield or similar.

As part of the Website GDPR Compliance Service we will provide you with a Processor Agreement from b:web and look for evidence of processor agreements and compliance from third-parties of the website.

5. DO I HAVE A GDPR-COMPLIANT **PRIVACY POLICY** DISPLAYED CLEARLY ON THE WEBSITE?

Chances are that even if you have a privacy policy, it is not GDPR-compliant as GDPR prescribes numerous things that need to be included in the privacy notice.

As part of the Website GDPR Compliance Service we will audit and provide amended wording for your Privacy Policy and make sure it is visible on all pages.

6. DO I HAVE A GDPR-COMPLIANT **COOKIE POLICY** DISPLAYED CLEARLY ON THE WEBSITE?

You cookie policy should list all of the cookies used by the website and all of the details collected in your data inventory including the purpose of the cookie. You cookie policy should be reviewed regularly as cookies used may alter from time to time.

As part of the Website GDPR Compliance Service we will audit your website cookies and provide amended wording to your Cookie Policy.

7. IS THE WORDING ON MY **SIGN-UP** GDPR-COMPLIANT?

If you have a sign-up panel on your website that collects email addresses etc in return for your newsletter or other free opt in, ensure that you have GDPR-COMPLIANT opt in wording at the point of collection (i.e. underneath the sign-up panel) together with a link to your Privacy Policy.

8. DO I HAVE GDPR-COMPLIANT CONSENT FOR **EMAIL MARKETING** CAMPAIGNS?

If you do not have compliant consent you will need email your list for fresh consent. Your email campaigns probably already include an option for opting out since this has been a requirement for a long time.

As part of the Website GDPR Compliance Service we can advise as required.

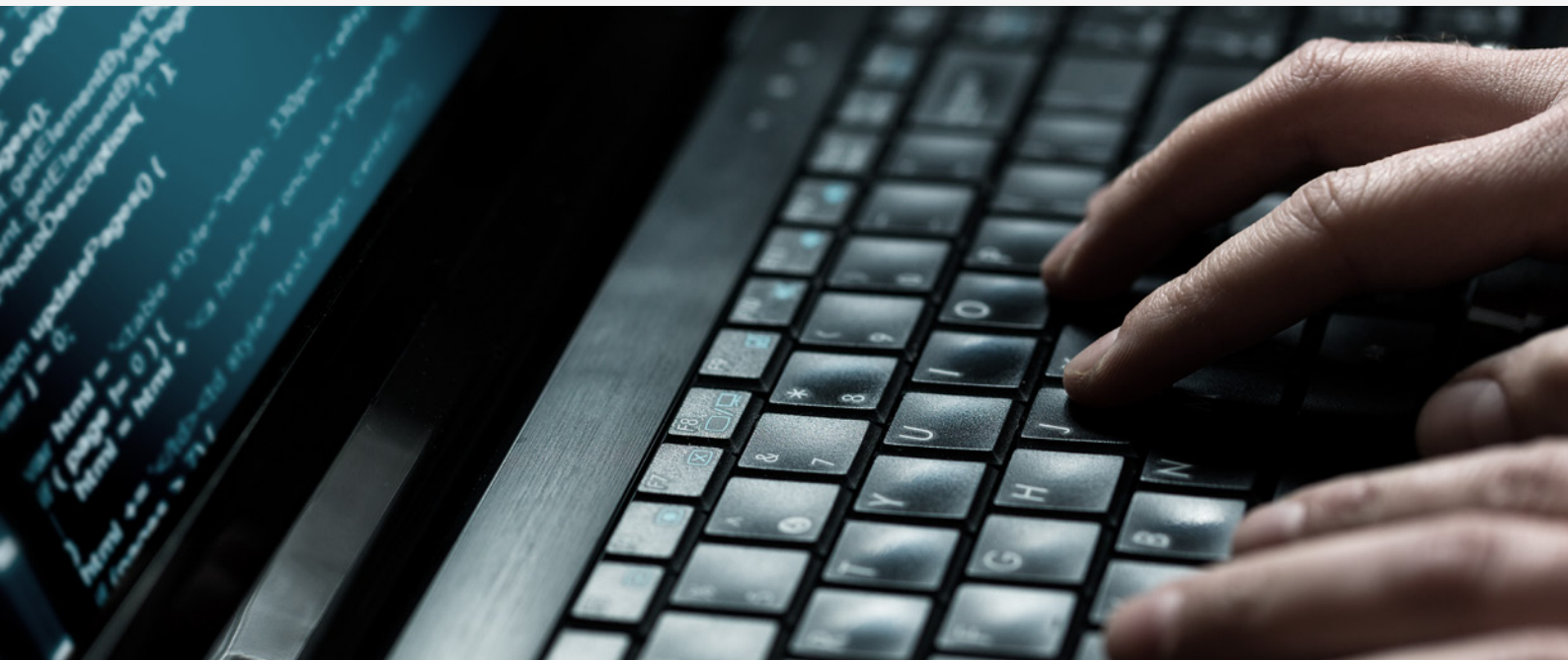
9. HAVE I OBTAINED GDPR-COMPLIANT **CONSENT** FOR PROCESSING SENSITIVE DATA?

Processing sensitive data requires explicit consent – this could be by the data subject signing the form where data has been collected or a double verification process.

As part of the Website GDPR Compliance Service we can advise as required re the website but this is much more likely to be relevant to your own customer and employee data/processes.

10. WHAT IS THE SYSTEM FOR **DATA BREACH** NOTIFICATION?

A data breach occurs where there is a loss alteration, unauthorised disclosure of or access to personal data AND there is a risk to the rights and freedoms of individuals. If there is a data breach, you must notify the ICO within 72 hours of the breach.



11. IS MY DATA **SECURE**?

In order to show GDPR compliance you must document the steps that you have taken to ensure that all data is secure. This relates to mobile phone, cloud emails, your website and all instances of where you store or access data.

As part of the Website GDPR Compliance Service we will provide a statement of the Website Security measures that you have in place.

12. IF I HAVE EMPLOYEES, HAVE I WORKED OUT LAWFUL GROUNDS FOR PROCESSING AND OBTAINED SIGNED COPIES OF THE **EMPLOYEE PRIVACY POLICY**?

Historically you may have relied on consent in an Employment Agreement to process employee data. Post GDPR you will need to work out separate lawful grounds of processing for each processing activity (e.g. payroll processing for contractual purposes, social security processing for requirements of law etc).

Grounds other than consent should be relied on where possible as consent can be withdrawn at any time. Where consent is necessary, this should be in a separate document to the Employment Agreement.

13. IF I HAVE EMPLOYEES, HAVE I ARRANGED FOR **DATA PROTECTION TRAINING** FOR THEM?

Employees will need to be aware of how to properly process data, record consents, how long to store data, when to report data breaches, how to respond to data subject requests.

14. IF I HAVE EMPLOYEES, HAVE I PUT IN PLACE SYSTEMS FOR EMPLOYEE **SUBJECT ACCESS REQUESTS**?

Subject access requests are most commonly submitted from employees and often in the context of a dispute. Ensure that you have a process in place to deal with such requests and to have appropriate templates for the employee to make the request and for your reply.

Published by b:web ©2018

b:web

info@bwebsites.co.uk
www.bwebsites.co.uk