Fat Beehive

GDPR Compliance

GDPR Compliance

Clauses

GDPR

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a privacy and data protection regulation in the European Union (EU). It became enforceable from May 25 2018.

The GDPR imposes new obligations on organisations that control or process relevant personal data and introduces new rights and protections for EU data subjects.

The GDPR applies to data processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Fat Beehive welcomes the introduction of GDPR and complies with the GDPR as a processor and controller of data. The hosting services that Fat Beehive provides are GDPR compliant and based within the EU. Fat Beehive has always taken all information security seriously, including that of personal data, regardless as to whether Fat Beehive is considered a processor or controller.

Assessment

Fat Beehive has assessed the GDPR regulations and matched its own activities and products in four key areas we consider relevant:

1. A data controller of its own employee data.
2. A data controller or processor of third party data such as activity relating to direct marketing.
3. A Software as a Service (SaaS) supplier.
4. A business that develops software.

Fat Beehive has reviewed all our systems and employed external consultants to help us meet compliance and to ensure that our customers can be certain that they are dealing with a compliant GDPR business. This included producing a GDPR Statement and holding a training event at the House of Commons. As part of our commitment to security Fat Beehive has had a GDPR Health Check from the British Assessment Bureau to identify any gaps and assist with remedial action. Fat Beehive is also undergoing ISO 27001, Information Management and Security, accreditation again via the British Assessment Bureau.

GDPR Clauses

1. Awareness

1.1. The Senior Management Team and decision makers are aware of the GDPR changes and the potential impacts.

1.2. We have used external consultants to do a GDPR gap analysis and currently in the process of ISO 27001 accreditation.

1.3. Staff have all undertaken specific, certifiable, third party, e-learning training modules on GDPR in addition to general GDPR awareness raising.

1.4. GDPR / Security Management is part of all new staff and contractors induction training.

1.5. All staff have to sign our data protection and server security agreement.

1.6. We have updated our risk register, to include GDPR compliance.

2. Information we hold

2.1. We have policies in place to support data protection compliance, including a Security Policy, Clear Desk / Screen Policy, ISO 27001 Business Management System and a Data Breach Policy.

2.2. Data Security is reported to the Board on a monthly basis as a KPI, which includes spot checks to ensure Password and Clear Desk / Screen Policies are being followed.

2.3. As a Data Controller we have documented all personal data that we hold, where it comes from and who we share it with.

2.4. As a Data Processor we have undertaken an information audit which identifies data flow mapping for all client data that is processed via the websites we produce and via any third party utilities that are used to process data, such as mailing lists, payment processors, CRMs'/ etc..

2.5. We have undertaken a review and documented where data may be stored. This includes servers (EU based), third party applications, desktop machines and within backup systems.

3. Communicating Privacy Information

3.1. We have updated our Privacy Policy which, inclusive of our Terms of Service, explains what personal data we collect, how we use personal data, reasons we may need to disclose personal data to others and how we store personal data securely. This is on every page of our website.

3.2. For clarity, Fat Beehive may be both data controller and data processor for personal data under certain circumstances. We are registered with the Information Commissioner's Office (registration number A8313621) and have an appointed Data Protection Officer.

4. Individuals Rights

4.1. The GDPR includes the following rights for individuals:

4.1.1. The right to be informed

4.1.2. The right of access

4.1.3. The right to rectification

4.1.4. The right to erasure

4.1.5. The right to restrict processing

4.1.6. The right to data portability

4.1.7. The right to object

4.1.8. The right not to be subject to automated decision-making, including profiling.

4.2. Our procedures have been reviewed to enable us to cover all the rights individuals have, including how we can delete personal data or provide data electronically in a commonly used format and ensuring personal data is portable if required.

4.3. We have identified (clause 2 above) via our data mapping flow where all data is stored and have procedures in place to enable us to delete all personal data if requested. Our processes ensure that we can respond to a request for erasure without undue delay and within one month of receipt.

4.3.1. We are aware of the circumstances when we can extend the time limit to respond to a request.

4.3.2. We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.

4.3.3. We have procedures in place to inform any recipients if we erase any data we have shared with them.

4.3.4. We have appropriate methods in place to erase information[1];

4.3.5. Requests from individuals, whose data Fat Beehive holds as a data controller, will be authorised by the CEO (data will be deleted without due delay, unless there are legal or regulatory reasons why data has to be kept).

4.3.6. Requests from clients (Data Controllers) to Fat Beehive (as the Data Processor), to erase personal data will be authorised by the Head of Technology.

[1] Individual personal data stored in backups will be deleted when the backups are replaced. Unless other laws or regulations require us to keep the data longer, backups are normally deleted within two months up to a maximum of 6 months

4.3.7. Requests from clients will for data deletion will need to be in writing and clients will be informed if, where and how any personal data is stored on Fat Beehive systems. Clients may be advised that third party applications could also hold data, although it is the Data Controller's responsibility to liaise with them direct.

5. Subject access request

5.1. Fat Beehive has processes in place to respond to subject access requests.

5.2. For personal data we hold as a Data Controller our Data Protection Officer will comply within one month.

5.3. Subject access requests (SAR) from a client (Data Controller) to Fat Beehive (as Data Processor) must be made in writing (email) to our Head of Technology who will liaise with clients to identify any personal data held on our systems and provide data in a timely manner for clients to respond to individuals.

6. Lawful basis for processing personal data

6.1. As a controller Fat Beehive only process personal data for the purposes of doing business. This is set out in our Privacy Policy.

6.2. Fat Beehive uses CCTV to detect and deter crime within its office. The CCTV only operates outside office hours and a data privacy impact assessment has been undertaken. Data is stored for no longer than is necessary.

6.3. As a Data Processor we process data on behalf of Data Controllers (clients). Data Controllers are responsible for ensuring that they have a lawful basis for processing personal data.

7. Consent

7.1. As a Data Controller, Fat Beehive has reviewed how we seek, record and manage consent and refreshed any consents that we did not believe met the GDPR standard.

7.2. All personal data consent is clear, informed, unambiguous and freely given. Additionally all consents are verifiable.

7.3. As a Data Processor, Fat Beehive has written to all existing clients providing support and information on making consent forms GDPR compliant. However it is up to Data Controllers to ensure that existing consents meet the GDPR standard.

7.4. All new proposals for websites include GDPR information and support on ensuring that we build websites that are GDPR compliant. Whilst we do not give Data Controllers legal advice, we can support clients with the following to help you make sure their site is compliant:

7.4.1. Privacy information notices

7.4.2. Just in time notices

7.4.3. Forms that enable clients to get consent in an active, granular and unbundled way. This includes consent notices which are clear, prominent, specific, opt-in and unambiguous.

7.4.4. All consents will be properly documented and easily withdrawn.

7.4.5. Building in account management functions for users such as changing or erasing their personal data

7.4.6. Secure data storage methods

7.4.7. Hosting within the EU

8. Children

8.1. For the first time GDPR will bring special protection for children's personal data. Any organisation that offers online services to children and relies on consent to collect information about them will now need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK).

8.2. Fat Beehive does not collect personal data from children however, we do work with clients that might. We will work with these clients to produce forms that enable clients to get consent in an active, granular and unbundled way. Additionally the consent will need to be properly documented, verifiable and written in language that children understand.

9. Data Breaches

9.1. GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases to individuals. However organisations only need to to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

9.2. Fat Beehive has a **Data Security Breach** policy which sets out our procedures we have in place to detect, report and investigate a personal data breach. At Fat Beehive

9.2.1. We understand that a personal data breach isn't only about loss or theft of personal data.

9.2.2. We have prepared a response plan for addressing any personal data breaches that occur.

9.2.3. We have allocated responsibility for managing breaches to a dedicated person or team.

9.2.4. Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

9.3. Should Fat Beehive detect or become aware of a personal data breach:

9.3.1. We have in place a process to assess the likely risk to individuals as a result of a breach.

9.3.2. We know who is the relevant supervisory authority for our processing activities.

9.3.3. We have a process to notify ICO / clients of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

9.3.4. We know what information we must give clients / ICO about a breach.

9.3.5. We have a process to inform affected clients / individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

9.3.6. We know we must inform affected clients / individuals without undue delay.

9.3.7. We know what information about a breach we must provide to clients / individuals, and that we should provide advice to help them protect themselves from its effects.

9.4. The Fat Beehive Data Security Breach Policy includes forms for reporting and documenting all personal data breaches, even if they don't all need to be reported

10. Data Protection by Design / Data Protection Impact Assessments

10.1. Fat Beehive has always adopted a Privacy by Design approach but has implemented additional measures to integrate data protection into our processing activities.

10.2. Fat Beehive has undertaken a Data Privacy Impact Assessment on how we use CCTV.

10.3. All our hosting and support packages now include Mandatory site maintenance and security updates including:

10.3.1. WordPress / Drupal core security releases

10.3.2. WordPress / Drupal Plugin and Module security releases

10.3.3. Keeping PHP version at fully-supported secure level including updating code to match, occasionally updating ahead of schedule for best performance

10.3.4. Keeping MySQL version at fully supported secure level including updating code to match, occasionally updating ahead of schedule for best performance

10.3.5. General server operating system (Ubuntu) updates and upgrades to latest fully supported secure level

10.3.6. Additional separate off-site backups stored securely

10.3.7. SSL certificate (https://) for security, trust, and SEO

10.3.8. CloudFlare add-on for attack mitigation

10.3.9. Additional Server encryption

10.4. Fat Beehive will work with clients to produce a risk assessment and Data Protection Impact Assessments where appropriate.

11. Data Protection Officers

11.1. Fat Beehive has appointed a Data Protection Officer and has registered with the Information Commissioner's Office.

11.2. Fat Beehive conducts a Information and Security Management review on a quarterly basis.

12. International

12.1. Fat Beehive’s main establishment is in the UK and our lead data protection authority is the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF