

# General Data Protection Regulation (GDPR) Statement

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a privacy and data protection regulation in the European Union (EU). It will be enforceable from May 25 2018 and requires no enabling legislation so automatically becomes binding and applicable on that date.

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 will be complying with the GDPR as a processor and controller of data. We have been planning and developing a programme of works which will deliver what is required by the legislation. This will involve working with our suppliers and partner organisations to ensure they can meet these obligations.

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.

In terms of the GDPR, Fat Beehive has been working towards compliance to ensure that our customers can be certain that they are dealing with a compliant GDPR business. The work will conclude prior to the May 2018 date for introduction of the regulation.

## 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.

Should any customer have a detailed question in respect of compliance, a public document will be made available that details the policies and activities that Fat Beehive employs matched to the clauses of the GDPR.

Fat Beehive will also provide a document that details the features of the SaaS provision. This means you can be confident that the organisation and software you are working with are GDPR compliant.

Fat Beehive sites are hosted solely from EU data centres.

As we work towards compliance our programme falls into these areas:

1. Policy Development: We will review our range of policies including, but not limited to: Data Breach Policy, Business Continuity Plans, DPO appointment, Subject Access Requests, Individuals Rights, ICO Good Practice.
2. Website Data Collection & Consent, Privacy Policy: We will provide an updated framework and privacy policy to incorporate the GDPR obligations. This will include legal framework gap analysis arising from the reviews we undertake as the plan progresses.
3. Data Impact Assessments & Data Inventory: We are already undertaking a systematic review of the data we store, manage, maintain, collect, process and control. This includes offline storage and paper records. Assessments of the data will review information flow, any data transfers, risk reviews, and structural position in relation to Lawfulness, Purpose, Minimisation, Accuracy, Consent, Limitation, Integrity & Confidentiality, Record Keeping and Accountability.
4. Training & Awareness: We will undertake training across the Fat Beehive team on the GDPR and its impact on the new policies, procedures, and responsibilities of staff & stakeholders in this new regime.
5. Controls & Gap Analysis: Running alongside the work already underway, we will be reviewing the controls in place, or required.
6. Supplier & Partner relationships: Where relevant and related, we will be using all reasonable endeavours to ensure that our third party and suppliers are complying with the GDPR.
7. Technology: we will be reviewing our technology platforms to analyse their operation, security and compliance in order to ensure that they meet the standards we have laid down, and identify any gaps and risks.
8. Accreditation: Fat Beehive will be seeking ISO 27001 accreditation that demonstrates its commitment to information security, including personal data.

Fat Beehive Senior Management Team and advisors will continue to monitor the programme up to the target date in May 2018 and beyond.

Activity so far

- Fat Beehive is amending its activities and associated policies and procedures as necessary in order to comply with GDPR following a thorough assessment.
- Fat Beehive is amending its customer and supplier contracts to ensure the GDPR reaches throughout the supply chain.
- Fat Beehive is reviewing all of its suppliers for compliance with GDPR paying very close attention to its marketing activity suppliers.
- Fat Beehive is carrying out Privacy Impact Assessments as necessary.
- Fat Beehive organised a public event at the House of Commons whereby clients were briefed further on GDPR.
- Fat Beehive has updated its Hosting and Support package in order to better meet GDPR requirements. All clients were placed on the new package as at 1st April 2018.
- Fat Beehive will be initiating additional cyber security options for all our clients eg: server encryption.
- The Fat Beehive website and direct marketing activity is being updated so that customers have the assurance that they will be contacted and treated in accordance with GDPR requirements. The website will contain Fat Beehive's privacy policies clearly identified.