Broadbean
6th Floor
The South Quay Building
189 Marsh Wall
London
E14 9SH

Client Services
T: 0800 169 6932
support@broadbean.com

www.broadbean.com

Broadbean GDPR preparation

Broadbean is committed to continuous improvement and ensuring we hold ourselves to appropriate standards with regards to the new GDPR legislation in advance of the regulation becoming enforceable in May 2018. We will also be making a number of changes to the services and products we provide to our customers in order that they can assist our customers on their GDPR compliance journey. Broadbean have four main areas of focus, and these are outlined below along with examples of some of the high-level features they contain.

Contractual

The GDPR has a more formalised definition of the controller/processor relationship and specific responsibilities defined for each of the roles. Broadbean have rewritten our standard Data Processing Agreement to clearly define the contractor/processor relationship and roles within the agreement.

The DPA also now contains schedules defining in detail the personal data Broadbean processes on behalf of our clients, the purpose of that processing, a schedule describing any Broadbean sub-processors and a summary of the high level technical and organisational measures taken with respect to information and data security.

As data processors Broadbean would not be entitled to retain customer personal data should a contract expire or be cancelled for any reason. A number of technical changes will streamline our processes in this area, to alert customers when they are approaching account expiry, and to deleting all necessary account information once expired.

Policy and Audit

Broadbean are reviewing and revising aspects of our Information Security policies and Incident Management process as part of our standard policy review process and to ensure that they remain in line with GDPR regulations and industry best practice.

We will be formalising Data Protection Impact Assessments into our standard product development processes and introducing enhanced logging of any access to Personally Identifiable information within Broadbean services, in order that we can more effectively monitor and audit appropriate access within the system.

In addition to the standard information security and data protection awareness training we already provide all staff, we will also be providing training to all existing and new staff on the GDPR and how it impacts their roles.

Information Security

Broadbean continually update and improve our information security controls and practices. The GDPR and WP29 recommendations highlight some specific areas we will be prioritising as part of this roadmap.

The GDPR recitals state that organisations should have measures to provide data protection by default and by design. Broadbean will be minimising the data held in our systems by providing enhanced policies and tooling to manage data retention, test accounts and account expiration. DPIAs will be used in all new product development to help identify risk to personal data early in the process, minimise access and processing, and identify any additional information security measures necessary.

Wherever possible we will be implementing encryption at rest for systems storing PII and updating our integrations with job board partners to better support encryption in transit for candidate applications.

Existing processes for backup and Disaster Recovery as well as infrastructure and patch management are being reviewed and updated to provide greater resilience to malicious attacks and to reduce RPO and RTA times in a DR situation.

Client tooling

As data processors, Broadbean hold Personal Data on behalf of our clients. As such, we need to be able to provide suitable means for our clients to manage their data and compliance measures. We recognise that different customers will have different needs in this regard and so we will be providing a range of configurations, tools and features to accommodate these different requirements.

For example, we will be allowing customers to define their own data retention periods and provide automated methods to remove expired data; provide extra ways to capture candidate consent and re-assert candidate consent; and provide candidate detail retrieval, export and delete facilities for clients to manage their Data Subject Access Requests, Data Portability and Data Erasure requests.