GDPR Compliance Statement

Introduction

The EU General Data Protection Regulation (GDPR) came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new regulation aims to standardise data protection laws and processing across the Europe; affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

BPTT is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection programme which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this programme to meet the demands of the GDPR and the UK's Data Protection Bill.

BPTT is committed to safeguarding the personal information we hold and to developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for current and future regulations. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

BPTT is fully compliant with the GDPR and this is how we prepared for it:

A. Information Audit

Carried out an organisation-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

B. Policies & Procedures

Data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

1. Data Protection

   Our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and

evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

2. Data Retention & Deletion

We have updated our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated deletion procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.

3. Data Breaches

Our data breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

4. International Data Transfers & Third-Party Disclosures

Should BPTT store or transfer personal information outside Europe, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of that data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

5. Subject Access Request (SAR)

We have revised our SAR procedures to accommodate the revised 30-day time frame for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

6. Legal Basis for Processing

We are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.

7. Privacy Policy

We have revised our Privacy Policy to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who information is disclosed to and what safeguarding measures are in place to protect their information.

8. Obtaining Consent

We have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We provide an easy way to withdraw consent at any time.

9. Direct Marketing

We have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out.

10. Data Protection Impact Assessments (DPIA)

Where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

11. Processor Agreements

Where we use any third-party to process personal information on our behalf (ie. Payroll, Recruitment, Hosting etc), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

C. Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via email of an individual's right to access any personal information that BPTT processes about them and to request information about:

a. What personal data we hold about them

b. The purposes of the processing

c. The categories of personal data concerned

d. The recipients to whom the personal data has/will be disclosed

e. How long we intend to store your personal data for

f. If we did not collect the data directly from them, information about the source

g. The right to have inaccurate or incomplete data about them corrected or completed and the process for requesting this

h. The right to request deletion of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making

i. The right to lodge a complaint or seek judicial remedy and who to contact.

D. Information Security & Technical and Organisational Measures

BPTT takes the privacy and security of individuals and their personal information very seriously and takes all reasonable measures and precautions to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction.

E. GDPR Roles and Employees

BPTT has made it the responsibility of every member of staff to ensure that all parties comply with the new data protection regulations. The whole team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures. BPTT understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR. We have implemented an employee training programme, and this forms part of our induction and annual training programmes.

F. Statement Review

This statement will be reviewed annually on the anniversary of the May 2018 GDPR implementation date.