Introduction

Our Data Protection Policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data. This policy applies to all personal data processed by Bragd LLP. Pam Stirling, as the GDPR Owner shall take responsibility for Bragd's ongoing compliance with this policy. Any enquiries about data protection shall be referred to the GDPR Owner. This policy shall be reviewed at least annually in line with our BQMS update and review procedure BPR 001. We are registered as Bragd LLP with the Information Commissioner's Office as a Data Controller. Our registration reference is Z9511826.

Scope

This policy applies to personal data processed in a structured file system whether automated or paper-based. This policy applies to all EU citizen personal data pertaining to a natural person that Bragd LLP holds and processes. It also applies to office(s) outside of EU that offer goods, services or monitors behaviour of EU citizens. Generally, transfer of personal data to a non-EEA country is strictly prohibited, unless explicit consent has been sort from the data subject.

Definitions

Asset and Risk Register
Our tool for understanding the infrastructure and data within Bragd LLP.

Children
If the data subject is under the age of 13 then they are classified as a child and parent/guardian consent must be gained before processing, their data (see Safeguarding Policy BPO 020).

CIA Triad
Bragd's approach to ensure information and data:

- Confidentiality – preventing unauthorised disclosure of information
- Integrity – preventing unauthorised modification of information or files
- Availability – ensuring timely access to resources.

Data Controller
The natural person or legal entity which alone or jointly with others, determines the purpose and means of the processing of personal data.

Data Processor
A natural person or legal entity who processes data with the specific authority of the data controller.

Data Flow Map
The process of data flow mapping identifies where all data within Bragd LLP originates, and tracks it on its journey through Bragd to the point at which it is destroyed.

Data Subject
Any living individual whose personal data is processed by Bragd LLP.

Data Subject Consent
Consent can only be regarded as obtained if it is freely given, specific, unambiguous. It should reflect the wishes of the data subject given by clear, affirmative action.

Natural Person
An individual who is alive, does not apply to other legal entities.

Personal Data
Any information referring to an identified or identifiable natural person, an identifiable natural person is someone who can be identified directly or indirectly by reference including:

- Name
- ID Number
- Location data – Address, GPS location, Online location
- Online Identifier – persistent cookies, RDIF tags, IP address etc.
- Factors relating to physical, economic, cultural, social identity.

Personal Data Breach
Breach of security leading to accidental or unlawful:

- Destruction
- Loss
- Alteration
- Unauthorised disclosure
- Unauthorised access.

This list is non-exhaustive. Please see BPR 042 Data Breach Procedure and also BTR 014 Data Security Breach Register.

Processing
Any operation or set of operations including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consolidation, disclosure by transmission, making available, alignment or combination, restriction, erasure or destruction.

Profiling
Automated processing intended to evaluate certain personal aspect relating to a natural person to analyse or predict performance at work, economic situation, location, health, personal preference, reliability or behaviour.

Special Category Personal Data
Personal Data that relates to:

- Beliefs (religious, philosophical, trade union, political)
- Racial or ethnic origin
- Health
- Genetic information
- Biometric data
- Sexual activity and orientation.

Policy Statement

The Partners and management of Bragd LLP are committed to compliance will all UK and EU regulations in respect to personal data and the protection of the "rights and freedoms" of the data subject's information held by Bragd LLP.

This policy applies to all personal data held by Bragd LLP and all processing activities of such data. This policy applies to all employees of Bragd LLP included outsource suppliers. Any breaches of this policy or related policies and procedure will be dealt with using Bragd LLP disciplinary procedures. Sub-contractors and any third parties working with or for Bragd LLP, and who have access to personal data must have read, understood and comply with this policy. (See Contracting Policy BPO 023). Sub-contractors and third parties may only access the personal data held by Bragd LLP after signing a confidentiality agreement (see BFO 062 Mutual NDA).

Compliance with the General Data Protection Regulations (GDPR) (as enacted by the Data Protection Act (2018)) is described in this policy and other relevant policies. Pam Stirling, as GDPR Owner is responsible for reviewing the register of processing annually considering changes of processing performed by Bragd LLP

Roles and Responsibilities
Depending on the contract, Bragd LLP can be both a data controller or a processor under the Data Protection Act (2018). The GDPR Owner is responsible for the development and implementation of the GDPR as required by this policy and security and risk management in relation for compliance with this policy. The GDPR Owner has specific responsibilities in respect to Subject Access Requests and complaints, they are also the first point of contact for employees seeking clarification on any aspect of data protection compliance.

Compliance with this policy and the data protection regulations is the responsibility of all employees who process personal data. Employees of Bragd LLP are responsible for ensuring the accuracy of any personal information supplied by them and processed by Bragd LLP.

Data Protection Principles
All personal data processing activities must adhere to the data protection principles, as laid out in Article 5 of the GDPR. These principles are:

All processing must be "fair, lawful and transparent"
Fair- for the processing to be fair, the data controller has to ensure that certain information is made available to the data subjects at point of collection or if the personal data was collected indirectly (See "Transparent" below).

Lawful – The processing of each piece of personal data must have a lawful basis before processing can begin.

Transparent – Privacy notices describing the purpose of use of the personal data being collected must be given to the data subject when collecting data, this includes

- Identity and contact details of the controller
- Purposes of processing
- Lawful basis for processing
- The retention period of the data
- The rights of the data subject in respect of access, rectification, erasure, restriction and objection
- The categories of personal data being collected
- The recipients of the personal data, if applicable
- Whether the data will be transferred to a third party.

See BPR 040 Privacy Notice Procedure, including the need for date and time of consent, for more details.

Data can only be collected for specific, explicit and legitimate purposes
Bragd LLP will ensure that data is only obtained for specific purposes will not be used for purposes that are different from the purpose for which it was originally obtained.

Personal data must be adequate, relevant and limited for what is necessary for purposes
Bragd LLP will ensure that it will not collect more data than is necessary to perform the processing.

Personal data must be accurate and kept up to date with every effort to erase or rectify without undue delay
Bragd LLP will ensure that stored data must be reviewed and updated as necessary. Data will not be kept unless it is reasonable to assume that it is up to date. The GDPR Owner is responsible for responding to requests for rectification within 1 month of receipt of the request. The GDPR Owner is responsible for ensuring that if data is rectified then all organisations that the data has been past to have been notified of the change.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
Personal data will only be kept for the retention period identified and recorded in the Asset and Risk Register (see BTR 013 GDPR Asset and Risk Register). Once expired, personal data will be securely disposed of as detailed in Asset and Risk Register. When personal data is deleted this should be done safely such that the data is irrecoverable. Where personal data is kept beyond the processing date it shall be encrypted and minimised to protect the identity of the data subject. The GDPR Owner must specifically authorise any data retention beyond the retention periods defined in the Asset and Risk Register and must ensure that any justification is recorded and is in line with the GDPR (see BTR 013 GDPR Asset and Risk Register).

Personal data must be processed in a manner that ensures the appropriate security of the data
The GDPR Owner is will carry out a risk assessment taking into account all of Bragd LLP data security controls and processing procedures (see risk rating section in BTR 013 GDPR Asset and Risk Register). The GDPR Owner will assess the risks against the requirements of the company and risks to the data subjects and ensure that the risks are mitigated (including technical controls) and signed off by the Partners. Bragd shall also ensure that personal data is stored securely using modern software that is kept-up-to-date. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information. Appropriate back-up and disaster recovery solutions are in place.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Bragd shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

General Provisions
Accountability
The GDPR Owner must be able to demonstrate compliance with the GDPR's other principles to show accountability and governance; these complement the data protection principles and allows the controller or processor to demonstrate compliance with the data protection principles.

Bragd LLP demonstrate compliance by:

- Implementing the Data Protection Policy and associated procedures including our BPR 019 Computer Security Procedure and BPR 041 Information Security Procedure.
- Adhering to relevant codes of conduct
- Implementing appropriate technical and organisation controls to protect the data*
- Documenting the use and location of personal data in Bragd LLP*
- Mapping the flows of personal data into and out of Bragd LLP (See BDF documents in our BQMS).

* See BTR 013 GDPR Asset and Risk Register.

Data Subject Rights
Bragd LLP has procedures in place to ensure that the data subjects rights are upheld (See BPN 001 Customer Privacy Notice) including.

- The right to access the personal information held about them, along with the purpose and legal basis for holding the data
- The right to rectify inaccurate data held about them
- The right to restrict processing of data if they suspect it is being used unlawfully
- The right to has data that is held about them erased if there is no other lawful reason to keep it
- The right to object to data being processed under legitimate interest
- The right to object to automated profiling using their personal data

- The right to raise a complaint to the ICO if they feel Bragd LLP has contravened a provision of the GDPR.

If data is corrected, erased or restricted from processing, then all recipients of the data must be informed. Data subjects have the right to complain to Bragd LLP about how their data is being handled, contact for complaints must be made clear at the point of collection of the data.

As part of our approach to continuous improvement, this policy will be regularly monitored and reviewed on an annual basis.

Signed: Date: 03 October 2021

Jason Rudgley *Pam Stirling*

Jason Rudgley
Partner

Pam Stirling
Partner