Birtenshaw

Data Protection (GDPR)

Policy and procedure

Legislation References	
General Data Protection Regulation (GDPR) 2016/679	Data Protection Act 2018

Table of Contents

Document Title	Data Protection (GDPR) Policy
Reference Number	GP 07
Version Number	Version 3
Date of Issue	01/01/2016
Latest Revision	02/10/2018
Distribution	All employees
Owner	Chief Executive
Policy Lead(s)	Head of Service: HR
Department	HR

Policy Statement

This Policy sets out the obligations of Birtenshaw regarding data protection and the rights of employees and customers ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of Birtenshaw.

Birtenshaw is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Definitions

- 'Data' refers to all personal data stored both manually and on computer records.
- 'Data subject' – living and identifiable individuals about whom information is stored.
- 'Data controller' – an organised body or person who decides how and why such data is processed (the Company)
- 'Data processor' - any person who processes data on behalf of the data controller.
- 'Staff' – all employees/agents of the Company.

The Act regulates the processing of data relating data subjects. Data processors must comply with the data protection principles of good practice which underpin the Act.

The Data Protection Principles

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the ‘right to be forgotten’)
- The right to restrict processing
- The right to data portability
- The right to object and
- Rights with respect to automated decision-making and profiling

Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR

states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

Specified, Explicit and Legitimate Purposes

Birtenshaw only collects and processes and holds personal data for the specific purpose as is required or for other purposes expressly permitted by GDPR
Data subjects are kept informed at all times of the purpose or purposes for which the company uses their personal data.

Accuracy of Data and keeping up to date

The company shall ensure that all personal data collected, processed and held is kept accurate and up to date. This includes but is not limited to, the rectification of personal data at the request of a data subject.

Data Retention

The company shall not keep personal data for any longer than is necessary in the light of the purpose or purposes for which that data was originally collected, held and processed.

When personal data is no longer required all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the company's approach to data collection and retention please refer to our Privacy Policy.

Keeping Data Subjects informed

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

If the personal data is used to communicate with the data subject, when the first communication is made; or if the personal data is to be transferred to another party, before that transfer is made; or as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

Subject Access Requests

Data subjects may make subject access requests (SAR's) at any time to find out more about the personal data which the company holds about the, what it is doing with that personal data and why.

Data subjects wishing to make a SAR should do so using a Subject Access Request Form, sending the form to enquiries@birtenshaw.org.uk

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

Birtenshaw does not charge a fee for the handling of normal SARs. Birtenshaw reserves the right to charge reasonable fees for additional copies of information that

has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of personal data

Data subjects have the right to require Birtenshaw to rectify any of their personal data that is inaccurate or incomplete.

Birtenshaw shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of personal data

Data subjects have the right to request that Birtenshaw erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for Birtenshaw to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject objects to Birtenshaw holding and processing their personal data and there is no overriding legitimate interest to allow the Company to continue doing so.
- The personal data needs to be erased in order for Birtenshaw to comply with a particular legal obligation

Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

Personal Data Collected, Held and Processed

The Act does not set out any specific minimum or maximum periods for retaining personal data. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Birtenshaw is required by law to:

- review the length of time we keep personal data;
- consider the purpose or purposes which we hold the information for in deciding whether (and for how long) to retain it;

- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Data is collected, held and processed by Birtenshaw in line with our data register and all personal data is held in accordance with the Company's Data Retention Policy. For details about data retention, please refer to Birtenshaw's Data Retention Policy.

Transferring personal data to a country outside EEA

Birtenshaw does not knowingly transfer personal data to countries outside of EEA

Data Breach Notification

All personal data breaches must be reported immediately to Directorate Management Team (DMT)

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), Birtenshaw must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, Birtenshaw must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Responsibilities for staff
During the course of their duties with the Company, staff will be dealing with clients' and prospective clients' personal data passed to us in relation to the carrying out of our contracted services. We have a duty to protect that data as well as our own. To this end, staff must do the following:

- Put away any client/potential client related documentation in a drawer/cupboard before leaving the building. This should not be left on desks overnight.

- Lock your computer when you move away your desk, even if just for a very short period of time;
and
- When posting/emailing/faxing documents, ensure that the information is sent to the intended recipient and not incorrectly sent to another data subject.

Compliance
Compliance with the Act is the responsibility of all staff. The Company will regard any unlawful breach of any provision of the Act by any staff as a serious matter which may result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the line manager.

Implementation of Policy
This policy shall be deemed effective as of 25 May 2018. No part of this policy shall have a retroactive effect and shall thus apply only to matters occurring on or after this date.

The company reserve the right to amend this policy with little or no notice.