Axiomata's Data Protection Policy

Introduction

Axiomata Limited is committed to being transparent about how it collects and uses the personal data including, in particular, the data of our employees, sub-contractors, people we engage on a freelance basis and actual and potential Clients of our services.

This policy applies to the personal data of all such persons.

Our Data Protection Principles

Axiomata processes personal data in accordance with the following Data Protection principles:

- Axiomata processes personal data lawfully, fairly and in a transparent manner.
- Axiomata collects personal data only for specified, explicit and legitimate purposes.
- Axiomata processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Axiomata keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Axiomata keeps personal data only for the period necessary for processing.
- Axiomata adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Axiomata tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where Axiomata relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Legal Basis on which Axiomata holds Personal Data

We hold personal data under the following permitted reasons provided by the GDPR so one of these reasons will apply to your data:

Consent: the individual has given clear consent for Axiomata to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract Axiomata has with the individual, or because Axiomata has asked the individual to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for the individual to comply with the Law (*not* including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for the individual to perform a task in the public interest or for the individual's official functions, and the task or function has a clear basis in Law.

Legitimate interests: the processing is necessary for the individual's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Individuals have the right to make a *subject access request*. If an individual makes a *subject access request*, the organisation will tell him/her:

- Whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- To whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- For how long his/her personal data is stored (or how that period is decided);
- His/her rights to rectification or erasure of data, or to restrict or object to processing;
- His/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- Whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

Axiomata will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a *subject access request*, the individual should send the request to response@axiomata.uk or use the organisation's form for making a *subject access request* which is available on request. In some cases, Axiomata may need to ask for proof of identification before the request can be processed. Axiomata will inform the individual if it needs to verify his/her identity and the documents it requires.

Axiomata will normally respond to a request within a period of one month from the date it is received. In some cases, such as where Axiomata processes large amounts of the individual's data, it may respond within three months from the date the request is received. Axiomata will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a *subject access request* is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, Axiomata can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

A *subject access request* is likely to be manifestly unfounded or excessive where it repeats a request to which Axiomata has already responded. If an individual submits a request that is unfounded or excessive, Axiomata will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data.

They can require the organisation to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

  To ask Axiomata to take any of these steps, the individual should send the request to the email address above or on Axiomata's website.

Data Security

Axiomata takes the security of personal data seriously.

Axiomata has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Data Breaches

If Axiomata discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Axiomata will record all data breaches regardless of their effect.

Individual responsibilities

Individuals are responsible for helping Axiomata keep their personal data up-to-date.

Individuals should let Axiomata know if data provided to Axiomata changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of Axiomata's Customers and Clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, Axiomata relies on individuals to help meet its data protection obligations to staff and to Customers and Clients.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes;
- Not to disclose data except to individuals (whether inside or outside Axiomata) who have appropriate authorisation;
- To keep data secure (for example, by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove personal data, or devices containing or that can be used to access personal data, from Axiomata's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- Not to store personal data on local drives or on personal devices that are used for work purposes; and
- To report data breaches of which they become aware to Yanina Barry immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Axiomata's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.