Jump

Data Security Policy

Introduction

Jump is legally obliged to comply with the provisions of the Data Protection Act 1998 (the Act) and GDPR (2018). Jump needs to process certain information about its employees and clients. In so doing, our business is obliged to comply with the provisions of the Data Protection Act 1998 and GDPR (2018).

The Act imposes restrictions on how Jump may 'process' personal data. This term covers the collection, recording, retrieval, consultation, use and disclosure of data.

Jump's designated Data Protection Co-ordinator is Ben Thorne, Head of Sustainability. It is the Data Protection Co-ordinator's responsibility to deal with day-to-day Data Protection matters and to encourage good information handling practice within the Company.

The Act gives to members of staff and clients the right of access (with very limited exemptions) to any personal/client company data that Jump may hold about them. It also places an obligation on our business to respond to such requests within a set time. For this reason, all formal access requests by staff and client companies must be directed through Jump's Data Protection Co-ordinator.

Jump, all staff and any others who process personal/client company information on behalf of the company, must ensure that they comply with the principles of the Act and with the provisions laid out in the Act, relating to Staff Guidelines.

Principles of Data Protection

Anyone processing data must comply with the eight enforceable principles of good practice. These say that data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the Data Subject's rights.
- Secure.
- Not transferred to countries without adequate protection.

Status of the Policy

This policy has been approved by Jump's management. Any breach will be taken seriously and may result in disciplinary action.

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Jump. Any failures to follow the policy can therefore result in disciplinary proceedings.

Contractors to Jump and all other visitors to the company will also be expected to comply with this policy insofar as they come into contact with personal data through our company.

Personnel that consider that the policy has not been followed in respect of personal/ client company data should raise the matter with our Data Protection Co-ordinator.

The Company's Responsibilities
Jump is committed to protecting the right of individuals to privacy with respect to the processing of their personal data. Under the terms of the legislation, Jump is the Data Controller and ultimate responsibility for compliance with the Act lies with the Managing Director. All Managers and Supervisors have a responsibility to ensure good information handling practice amongst all members of Jump.

Right of Access
Personnel of the Company and other parties that deal with or have access to Justly Digital has the right to access data held about them by the Company, whether in manual or electronic format. Any individual/client company wishing to exercise this right should approach Jump's Data Protection Co-ordinator.

Fair and lawful
The intention of the Act is not to prevent data processing, but to ensure that it is done fairly and without adverse effect on the individual/client company the data relates to. The Data Subject (a member of staff or client company) should be informed of:

- Who the Data Controller is (in this case, Jump).
- Who the Data Controller's representative is (in this case, the Data Protection Co-ordinator (Ben Thorne, Head of Sustainability).
- The purpose or purposes for which the data are to be processed.
- To whom the data may be disclosed.

Data processing may only take place if specific conditions have been met. These include the Data Subjects' consenting or the processing being necessary for the legitimate interests of the Data Controller. When it comes to processing sensitive personal data (data relating to ethnicity, political opinion, religion, trade union membership, health, sexuality or criminal record of the data subject) additional

conditions must be met. In most cases this will require explicit (i.e. written) consent from the individual concerned.

Purposes
Personal data processing must be in accordance with the purposes notified by Jump to the Data Protection Commissioner. Jump cannot therefore gather information for one declared purpose, and then use it for another. If any 'new processing' is to take place the Data Protection Co-ordinator must be consulted.

Adequate, Accurate, Timely
The fact that electronic information is readily available does not mean that it can be treated casually. Nor can it be gathered and held because it might be useful at some point in the future, or simply because the software allows it. The requirement that personal data should not be kept longer than is necessary means that a policy should be in place for the disposal of the data once it has reached the end of its life - there can be no holding on to data simply because it is easier to do so than to ensure its disposal.

Rights of the Data Subject
The data must also be treated with regard to the Data Subject's rights, such as the right to have inaccurate data amended. A Data Subject has the right to request access to any data held within Jump's systems. Consequently, Jump must make provision to ensure that that data is retrievable from its systems.

Security
Appropriate security measures must be taken against unlawful or unauthorised processing (including unauthorised viewing) of personal data and against accidental loss of or damage to, personal data. A Data Subject may apply to the Courts for compensation if they have suffered damage from such a loss. The Act puts Justly Digital under an obligation to have in place policies, procedures and technologies to maintain the security of all personal data from collection to destruction. This covers not only the storage, but also the transmission, of personal data (including email).

Transfer of personal data
Personal data must not be transferred to a country outside the European Economic Area unless specific exemptions apply (e.g. if the Data Subject has given consent.) This includes the publication of personal data on the internet.
Definitions

'Data' means information:

- Stored in a form capable of being processed by computer (such as word-processed documents, spreadsheets and databases).
- Recorded in any form for later processing (such as registration forms, CCTV pictures).
- Stored as part of a 'relevant filing system'. Note that this definition is very broad and covers such things as card indexes and microfiche files as well as traditional paper- based files. It would be as well to assume that any paper-based data falls under the Act.

Personal Data

Personal data are defined as data which relate to a living individual who can be identified:

- From those data; or
- From those data and other information in the possession of (or likely to come into the possession of) the Data Controller.
- Includes any expression of opinion about the individual and any indications of the intentions of the Data Controller or any other person in respect of that individual.

The Information Commissioner accepts that this definition is 'not without difficulty'. It would always be safest to assume that data is personal rather than not.

Sensitive personal data

The 1998 Act distinguishes between ordinary "personal data" such as name, address and telephone number and "sensitive personal data" which includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive personal data is subject to much stricter conditions.

Data Subject

A Data Subject is any living person who is the subject of personal data.

Data Subject Access

This is the right of an individual to see personal data relating to him or her which is held by a Data Controller.

Data Controller
A 'Data Controller' is any organisation or person who makes decisions with regard to particular personal data, including decisions about the purposes for which the data is to be processed and the way in which that processing takes place. Jump is the Data Controller, but any member of staff may also be a Data Controller if they make decisions about personal data and its processing.

Processing
Processing covers almost anything you can do with data, and includes acquiring, recording, consulting, retrieving, and making the data available to others.

Tony Napodano
Managing Director

July 2023