BEYONDLY

G-1

Data Protection and GDPR

Policy Statement

Beyondly is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the Data Protection Act 1998 and the General Data Protection Regulation (GDPR). This policy sets out how Beyondly deals with personal data and employees' obligations in relation to personal data and responsibilities under the policy.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy requires employees to ensure that either the Brand, Solutions and Innovation Manager or Managing Director (who have been allocated responsibilities as Data Protection Officers) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

This policy should be adhered to in conjunction with the Information Security Policy (G-8).

Definitions

Personal data
This any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Sensitive personal data
This is information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health or condition; or
- sex life.

Criminal records data
This means information about an individual's commission or alleged commission of any criminal offence; and proceedings for any offence committed or alleged to

have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Use of Personal Data

'Processing' includes obtaining personal data, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it. The purpose for which personal data may be used by the company is for recruitment and selection, HR, administrative, financial, payroll, business development and business operational purposes.

Data Protection Principles

The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These principles require that personal data must:

- Be processed in a fair, lawfully and transparent manner
- be processed for limited purposes and not in any manner incompatible with those purposes
- be adequate, relevant and not excessive
- be accurate
- not be kept longer than is necessary
- be processed in accordance with individuals' right
- be secure; and
- not be transferred to countries without adequate protection.

The GDPR includes the following rights for individuals:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object.

How Beyondly will Protect Personal Data

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Data Security
Beyondly will store data securely to ensure protection against loss or misuse.

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The Systems Developer must approve any cloud used to store data.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should not be taken off site unless unavoidable. In these cases data should always be password protected.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data Retention
The company will retain personal data for no longer than is necessary.

Transferring Data Internationally
The company will not transfer data internationally or anywhere outside of the United Kingdom without first consulting with the DPO. It is important to recognise that the company operates internationally, therefore, it will process client data in order for the business to operate successfully in line with GDPR.

Privacy Notices
Privacy notices are available for employees, existing customers and visitors to the Beyondly website. The notices include:

- The purposes for which we hold personal data
- A highlighted statement that our work may require us to give information to third parties
- Individual's right to have access to the personal data that we hold about them

Data Audit and Register
Quarterly data audits to manage and mitigate risks will inform the data register, which is stored on the shared drive and managed and monitored by the Brand, Solutions and Innovation Manager and Managing Director. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. The ICO may request for access to the data register, therefore each department must keep the data register updated on a quarterly basis.

Responsibilities

All Employees
If an employee acquires any personal data in the course of his or her duties, he or she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.

In particular, an employee should ensure that he or she:

- accesses data that they have authority to access and only for authorised purpose;
- keeps data secure by use of password-protected and encrypted software for the transmission and receipt of emails, secure file storage and destruction; and
- sends fax transmissions to a direct fax where possible and with a secure cover sheet.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or junk folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin without having been shredded first.

If an employee acquires any personal data in error by whatever means, he or she shall inform the Managing Director immediately and, if it is not necessary for him or her to retain that information, arrange for it to be handled by the appropriate individual within the company.

Where an employee is required to disclose personal data to any other country, he or she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the DPO.

An employee must not take any personal data away from the company's premises except in circumstances where he or she has obtained the prior consent of senior management to do so. If an employee is in any doubt about what he or she may or may not do with personal data, he or she should seek advice from the Systems Developer. If he or she cannot get in touch with the Systems Developer, he or she should not disclose the information concerned.

Where laptops are taken off site, employees must follow the company's Information Security and Flexible Working policies.

Reporting data breaches
All employees have an obligation to report actual or potential data protection compliance failures.

If a breach occurs, this must be reported immediately to the Brand, Solutions and Innovations Manager or Managing Director. Any person investigating a breach must complete the Record of Data Breach.

This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioners Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures within 72 hours.

Consequences of Non-Compliance
All employees are under an obligation to ensure that they have regard to the eight data protection principles (see above) when accessing, using or disposing of personal data. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority,

Data Protection and GDPR

the company will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

The Brand, Solutions and Innovations Manager and Managing Director will be responsible for:

- Keeping the company updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all employees
- Answering questions on data protection from employees, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held by them
- Checking and approving with third parties that handle the company's data any contracts or agreements regarding the data processing

The Systems Developer is responsible for:

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware regularly to ensure it is functioning properly
- Researching third party services, such as cloud services the company is considering using to store or process data

The Brand, Solutions and Innovations Manager is responsible for:

- Approving data protection statements and other marketing copy
- Addressing data protection queries from clients, targets audiences or media outlets
- Ensuring all marketing initiatives adhere to data protection laws and the company's Data Protection Policy necessary to deliver our services
- Abiding by any request from an individual not to use their personal data for direct marketing purposes

Employee Data

Personnel Files
An employee's personnel file is likely to contain information about his or her work history with the company and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal data about the employee including address details and national insurance number.

There may also be other information about the employee located within the company, for example in his or her line manager's inbox or desktop, with payroll or within documents stored in a relevant filing system.

The company may collect relevant sensitive personal data from employees for equal opportunities monitoring purposes. Where such information is collected, the company will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal data. If the information is to be

used, the company will inform employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the company who will have access to that information and the security measures that the company will put in place to ensure that there is no unauthorised access to it.

The company will not retain sensitive personal data without the express consent of the employee in question.

The company will ensure that personal data about an employee, including information in personnel files, is securely retained. The company will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary. The company will hold personal data for the duration of employment. The periods for which employee data is held after the end of employment is ten (10) years.

Data on the company HR System (BambooHR)
The company's HR system enables employees to check their personal data so that they can correct, delete or update any data. If an employee becomes aware that the company holds any inaccurate, irrelevant or out-of-date information about him or her that they cannot amend themselves on the system, he or she must notify the Talent and Culture Coordinator immediately and provide any necessary corrections and/or updates to the information.

Employees must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required.

The company will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles. If the company enters discussions about a merger or acquisition with a third party, the company will seek to protect employees' data in accordance with the data protection principles. In most cases where we process sensitive personal data, we will require the person's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Data Subject Access Requests

- Individuals have the right to make a subject access request. If an individual makes an access request, the company will tell him or her: the types of information that it keeps about him or her;
- the purpose for which it is used; and
- to whom and the types of organisation that it may be passed to, unless this is self-evident (for example, it may be self-evident that an employee's national insurance number is given to HM Revenue & Customs).

The company will allow the employee access to hard copies of any personal data. However, if this involves a disproportionate effort on the part of the company, the employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by the company.

The company may reserve its right to withhold the employee's right to access data where any statutory exemptions apply.

The company will not charge for allowing individuals access to information about them and will respond to any data subject access request within 30 calendar days.

Data that is likely to cause substantial damage or distress
If an employee believes that the processing of personal data about him or her is causing, or is likely to cause, substantial and unwarranted damage or distress to

him or her or another person, he or she may notify the company in writing to the Managing Director to request the company to put a stop to the processing of that information.

Within 21 days of receiving the employee's notice, the company will reply to the employee stating either:

- that it has complied with or intends to comply with the request; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

Monitoring

The company may monitor employees by various means including, but not limited to, checking emails and internet usage, listening to voicemails and monitoring telephone conversations. Any such monitoring will be conducted in line with the Communications, Email, Internet and Social Media policy (E-12). If this is the case, the company will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him or her. The company will not retain such data for any longer than is necessary.

In exceptional circumstances, the company may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the company by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means). Covert monitoring will take place only with the approval of the Managing Director.

Issue Number: 2
Issue Date: 31 March 2023
Issued by (Name): Jessica Aldersley
Issued by (Signature):

Position: Managing Director