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 special category data and employees' obligations in relation to personal data and responsibilities under the policy.

Beyondly holds personal data about our employees, clients, suppliers and other individuals for a variety of business purposes and collects and processes personal data relating to its employees to manage the employment relationship. Beyondly is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

This policy requires employees to ensure that either the Head of IT 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

For the purposes of this Policy :

- "**Company**" (referred to as either "the Company", "We", "Us" or "Our" in this policy) refers to – Beyondly Global Ltd. For the purpose of the GDPR, the Company is the Data Controller, which alone or jointly with others determines the purposes and means of the processing of Personal Data.
- "**Personal Data**" is any information that relates to an identified or identifiable individual – including sensitive personal data. For the purposes of GDPR, Personal Data means any information relating to you such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
- "**Service Provider**" means any natural or legal person who processes the data on behalf of the Company. For the purpose of the GDPR, Service Providers are considered Data Processors.
- "**You**" can also be referred to as the 'Data Subject' or as the 'User' as you are the individual whose personal data is collected, held, or processed by an organisation. Essentially, you are the data subject is the individual to whom the personal data pertains.

Personal data

The company collects and processes a range of information about you. This includes :

- your name, address and contact details, including email address and telephone number, date of birth and gender
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover
- details of your bank account and national insurance number
- information about your marital status, next of kin, dependants and emergency contacts
- information about your nationality and entitlement to work in the UK
- language or linguistic skills
- information about your criminal record
- details of your schedule (days of work and working hours) and attendance at work
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence

Sensitive personal data

The company can also collect sensitive personal data (also referred to as special category data) about you. This is information that is inherently more sensitive in nature and, therefore, requires additional protections due to its potential to impact individuals' privacy or fundamental rights if mishandled. Article 9 of GDPR specifies these categories, and processing such data is generally prohibited unless explicit consent is obtained or another legitimate basis is met. This data can include the following :

- equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or spiritual beliefs.
- information about dietary requirements and medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments.
- sexual orientation or sex life information.
- biometric data (when used to uniquely identify an individual)

- political affiliations or opinions
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).

Data will be stored in a range of different places, including in your personnel file, in the organisation's HR management systems ‘Employment Hero’ and in other IT systems (including the company’s primary data management and email system within Microsoft Office 365).

Criminal records data

Under GDPR, criminal records data is subject to special protection and can only be processed under specific legal bases and with strict safeguards to ensure the data's security, confidentiality, and the rights of the individuals involved. This type of data is 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.

Processing of criminal records data is only permitted under very specific conditions, such as:

- ***Explicit consent*** from the individual, although reliance on consent alone may not always be sufficient in employment contexts or public authority matters.
- ***Compliance with legal obligations*** : Processing is allowed when required by law, such as in background checks mandated by national legislation.
- ***Performance of tasks in the public interest or exercise of official authority*** : In some cases, public bodies, law enforcement, or regulatory agencies may be permitted to process such data for specific purposes.
- ***Employment law*** : Processing may be allowed if required under employment laws, particularly in sectors like healthcare or education where background checks are legally required.

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.

The company may collect personal data in a variety of ways. For example, data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

The company seeks information from third parties with your consent only. Such as references supplied by former employers, information from employment background check provider ‘The referencing Agency’ and information from criminal records checks permitted by law.

When processing data, we meet the requirements of the data protection principles, as set out in data protection legislation :

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

To stay compliant with this principle we will:

- Make sure that we only process personal data lawfully and where we have identified a clear lawful basis to do so.
- Process personal data fairly and make sure that data subjects are not misled about the purposes of any of our processing.

Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

To stay compliant with this principle we will:

- Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice.
- Not use personal data for purposes that are incompatible with the original purpose

Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

To stay compliant with this principle we will:

- Ensure that we do not collect data that we do not need and will only collect the minimum personal data that is necessary for the purpose for which it is collected.
- We will ensure that the data we do collect is adequate for our purpose and relevant.

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.

To stay compliant with this principle we will:

- Make sure that the personal data we hold is accurate
- Ensure there are processes for us or individuals to correct and keep data up to date where necessary.

Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

To stay compliant with this principle we will:

- Only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so.

Principle 6 - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against personal data breaches.

To stay compliant with this principle we will:

- Make sure that there are appropriate organisational and technical measures in place to protect personal data.

Why does the company process personal data

The company needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer [benefit, pension and insurance entitlements].

In some cases, the company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, the company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows us to :

- run recruitment and promotion processes
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled
- ensure effective general HR and business administration
- provide references on request for current or former employees; and
- respond to and defend against legal claims.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities).

Where the company processes other special categories of personal and sensitive data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that we use for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Who has access to data

Your information may be shared internally, including with members of the Talent & Culture & Finance teams, your line manager, managers in the business area in which you work and IT / Systems staff if access to the data is necessary for performance of their roles.

The company shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. We may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The company also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.

The company will not transfer data internationally or anywhere outside of the United Kingdom without first consulting with the Data Protection Officer. 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.

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' rights
- 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

Protection of Personal Data

The company 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.

The company takes the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data Security

The company will store data on a secured Microsoft Office 365 tenancy to ensure protection against loss or misuse. All access to this tenancy is made through stringent Multi Factor Authentication processes and subject to cloud and endpoint protection.

Administration access to this environment is limited to the Head of IT at the company, and an external IT/Systems service provider, who ensure security oversight and maintenance.

The company's guiding principles to Data Security :

- All company data will be securely stored on a number of secured SharePoint sites. Dependant on the data (Finance, HR etc), it will be stored on the relevant secure sites, which only specific and necessary members of company staff will be able to access. Access to these secured SharePoint sites will only be given through an authorised request to the Head of IT.
- 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 via IT company policy every 3 months.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- All relevant data is backed up every 24 hours via Microsoft and also separately to an external service provider. This is 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 data should be accessed through secure company provided devices such as laptops and digital tablets, all of which will be managed through the InTune device management software.
- Accessing company emails, communication channels and files through personal mobile phone devices is only permitted through the 'Company Portal' app. This app is controlled through inTune device management, and allows staff to successfully onboard their personal device and gives

them the subsequent access to apps such as Outlook, Teams, SharePoint etc once they have signed in. The inTune device management and Company Portal app will also allow for successful offboarding of company data from a mobile device (if a member of staff leaves the company for example) without leaving a permanent digital imprint on a personal phone.
- There is to be no accessing of company data such as emails through default apps such as iOS Mail (Apple Mail), Gmail App (pre-installed on Android devices), Samsung Email (pre-installed on Samsung devices), as these default apps cannot be monitored or controlled by inTune device management software. Any access of company data via unauthorised default apps will be a breach of GDPR.
- All sites containing sensitive data must be approved by the Head of IT (prior to first use) and protected by security cloud & endpoint software, MFA where possible, and a strong onsite firewall.

Data Retention

As part of our ongoing compliance obligations, we will make sure that data is only retained for as long as is necessary. Data subjects have access to information about how their data will be handled and how long it will be retained

Where we no longer require personal data for the purpose for which it was collected, we will delete it, put it beyond use or make it permanently anonymous.

The company will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment is ten (10) years.

Accountability

The company has to be able to demonstrate that we are accountable for the personal data we process, that we are responsible for complying with our obligations under data protection legislation, and that we can demonstrate that compliance.

To demonstrate our compliance and accountability we will :

- Document our processing activities and keep these records up to date;
- Keep a record of personal data breaches;
- Have appropriate contractual arrangements in place with organisations that process personal data on our behalf;
- Complete a Data Protection Impact Assessment for any high-risk personal data processing; and
- Implement processes to make sure that personal data is only collected, used or handled in a way that is compliant with data protection legislation.

Privacy Notices

Privacy notices are available for employees, existing customers and visitors to the Beyondly website (https://www.beyond.ly). 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

Managing a data audit and data register is a crucial component of GDPR compliance, as it helps ensure that personal data is processed lawfully, transparently, and securely. A data audit involves reviewing all personal data an organisation holds, how it's processed, and who has access to it. This helps assess compliance with GDPR requirements.

The data register is a required document under Article 30 of GDPR to maintain a record of how a company processes personal data. The company will undertake quarterly data audits to manage and mitigate risks, which will inform the data register.

The data register is stored on the company Data Library (GDPR) and managed and monitored by the Head of IT.

The company's data register includes the following information :

- ***Data Controller Information*** : Name and contact details of the data controller, data protection officer (if applicable), and any joint controllers.
- ***Processing Activities*** : The purposes of processing personal data and categories of data subjects (e.g., employees, customers, etc.).
- ***Categories of Personal Data*** : The types of personal data processed (e.g., personal identifiers, financial data, etc.).
- ***Recipients*** : Any recipients of the data, including third-party processors or international transfers.
- ***Retention Periods*** : The length of time we retain each category of data.
- ***Security Measures*** : Documenting the security measures we have in place to protect personal data (e.g., encryption, access restrictions, etc.).
- ***International Transfers*** : If personal data is transferred outside of the EU, the safeguards (e.g., Standard Contractual Clauses) used to ensure GDPR compliance.

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.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from Office 365 / SharePoint, 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 IT & Systems department. If he or she cannot get in touch with this department, he or she should not disclose the information concerned. Where devices such as company laptops, tablets and mobile phones 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 and Impact 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, the company will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

The Head of IT 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 using or considering switching to, in order to store or process data
- 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 Brand and Impact 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. All information is stored electronically and 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 (Employment Hero)

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.

Your rights

As a data subject, you have a number of rights. You can :

- access and obtain a copy of your data on 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).
- require the company to change incorrect or incomplete data
- require the company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the company is relying on its legitimate interests as the legal ground for processing.

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 :

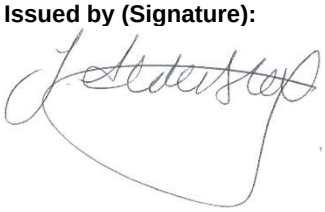
- that it has complied with or intends to comply with the request; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

If you believe that the company has not complied with your data protection rights, you can take the necessary legal steps.

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: 22 November 2024
Issued by (Name): Jessica Aldersley
Issued by (Signature):



Position: Managing Director