Data Protection Policy

Key details:

Policy prepared by:	Lucy Smith, MD, Clarity Umbrella Ltd
Approved by board / management on:	1st October 2019
Policy became operational on:	1st October 2019
Reviewed &/or Updated:	1st April 2020 7th September 2020 1st October 2021 6th September 2022
Next review date:	October 2023

Introduction

Clarity Umbrella Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data is collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Clarity Umbrella Ltd;

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 1998 describes how a business must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The head office of Clarity Umbrella Ltd
- All employees of Clarity Umbrella Ltd
- All contractors, suppliers and other people working on behalf of Clarity Umbrella Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals including National Insurance details, PAYE details, Bank Information and Right to Work ID verification checks and documentation

Data Protection Risks

This policy helps to protect Clarity Umbrella Ltd from some very real data security risks, including:

- **Breaches of confidentiality:** For instance, information being given out inappropriately.
- **Failing to offer choice:** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage:** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Data Security

- we have put in place measures to protect the security of your information; details of these measures are available upon request.
- third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.
- we have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.
- we have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data Storage

When data is **stored on paper,** it is kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files are kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

- **Data printouts should be shredded** and disposed of securely when no longer required. When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Responsibilities

Everyone who works for or with Clarity Umbrella Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that Clarity Umbrella Ltd meets its legal obligations.

- The **Data Protection Officer, Lucy Smith,** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Clarity Umbrella Ltd holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Managing Director, Lucy Smith, in conjunction with our IT supplier** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The **Director, Lucy Smith,** is responsible for:
    - Approving any data protection statements attached to comms such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy are those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- Clarity Umbrella Ltd **will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Providing Information

Clarity Umbrella Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company [A version of this statement is also available on the company's website].

Data Use

Personal data is of no value to Clarity Umbrella Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The Managing Director can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

How is your personal information collected?

- we collect personal information about employees through the application and recruitment process or background check provider. We may sometimes collect additional information from third parties including:
    - companies that introduce you to us (such as employment agencies, corporates, public bodies)
    - recruitment consultants
    - agents, suppliers, sub-contractors and advisers
    - our existing employees and clients
- we will collect additional personal information in the course of job-related activities throughout the period of you working for us.

Data Accuracy

The law requires Clarity Umbrella Ltd take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Clarity Umbrella Ltd will make it **easy for data subjects to update the information** Clarity Umbrella Ltd holds about them.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the director's responsibility to ensure **marketing databases are checked and updated** every six months.

How we process sensitive personal data…

We may also collect, store and use the following more sensitive types of personal information:

- information about your health, including any medical condition, health and sickness records, including:
- where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision.
- details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
- where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Information about criminal convictions and offences.
- "special categories" of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:
    - in limited circumstances, with your explicit written consent.

- where we need to carry out our legal obligations or exercise rights in connection with employment.
- where it is needed in the public interest, such as for equal opportunities monitoring.

- less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent?

- we do not need your consent if we use special categories of your personal information to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- we may only use information relating to criminal convictions where the law allows us to do so.
- we will hold information about criminal convictions, if it is appropriate, given the nature of the role and where we are legally able to do so.
- where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:
  - we may disclose criminal convictions if you are assigned to a project for another organisation that requires criminal background checks;
  - if you have disclosed criminal convictions, we may not put you forward for projects that your convictions would disqualify you for the project;
  - we may share the information with another organisation if you consent (for example, if you consent to disclosure in connection with your services being made available to an agency).

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Clarity Umbrella Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

How we will use information about you

- we will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:
  - where we need to perform the contract we have entered into with you.
  - where we need to comply with a legal obligation.
  - where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.
- we may also use your personal information in the following situations, which are likely to be rare:
  - where we need to protect your interests (or someone else's interests).

- where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

- The personal information we may hold on you is a follows:
  - name, address and contact details
  - date of birth
  - marital status
  - employment application
  - curriculum vitae
  - history with the company
  - job title
  - areas of expertise
  - details of salary (including your payslips and tax forms) and benefits
  - National Insurance number
  - bank details
  - performance appraisals
  - disciplinary records
  - salary reviews
  - records relating to holiday and other leave
  - working time records
  - next of kin details
  - logs of our communications with you
- we need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.
  - making a decision about your recruitment or appointment. We use the information you provide in your application
  - checking you are legally entitled to work in the UK.
  - paying you and deducting tax and National Insurance contributions (NICs).
  - providing the employee benefits which the company offers from time to time, if you opt for them.
  - enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties or in accordance with the preferences you express when you join.
  - administering the contract we have entered into with you and related contracts with organisations that use your services.
  - dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
  - complying with health and safety obligations.
  - to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
  - equal opportunities monitoring.

- some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.
- if you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

- we will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis, which allows us to do so.
- please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Automated decision-making

- automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.
- we use third party databases to verify your identity and proof of address.

Data sharing

- we may have to share your data with third parties. For example, we share your information with other companies who provide shared services that allow us to perform the functions outlined in this notice.
- we require third parties to respect the security of your data and to treat it in accordance with the law.
- we may transfer your personal information outside the UK and outside the European Union. Some overseas countries do not have data protection legislation equivalent to GDPR. However, your data will be treated at all times in line with GDPR requirements and will only be transferred internationally on an accepted lawful basis such as the Privacy Shield or standard contractual clauses mandated by GDPR. For specific details about your specific data, please contact your point of contact here at Clarity Umbrella.
- to be employed by Clarity Umbrella, you agree to a general authorisation to process your data outside the United Kingdom or outside the European Union. We will notify you of any intended changes or the addition of other processors and provide you with an opportunity to object.
- we will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. For example, we will share payroll information with HMRC and with pension providers. And we may also share, upon request, your payroll and employment information, including payslips, with your agency and end hirer (if applicable).

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

- it is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

- under certain circumstances, by law, and subject always to our statutory obligations, you have the right to:
    - **request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
    - **request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
    - **request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
    - **object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes which is covered under a separate consent form that we provide for you to accept (or not).
    - **request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
    - **request the transfer** of your personal information to another party.
- if you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact your point of contact here at Clarity in writing.

Subject Access Requests

All individuals who are the subject of personal data held by Clarity Umbrella Ltd are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**. If an individual contacts the company requesting this information; this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at info@clarityumbrella.com. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will aim to provide the relevant data within 14 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

No fee usually required

- you will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

- we may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

- in the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact your point of contact here at Clarity. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

- we reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.