

GDPR Policy.

1. Context and Overview

Key Details:

Policy prepared by: Dan Ison

Approved by Dan Ison and Lynne Fitzharris: Policy Operational Date: 26/1/2019

Next review: 26/01/2022

Introduction.

Ordit needs to gather and use certain information about individuals.

Individuals can include customers, suppliers, business contacts, employees and other people we have a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet data protection standards — and to comply with the law.

Please take a moment to read the '**Privacy Policy**' we provide to our customers and our enquiries from the footer of any of our websites.

Why this policy exists.

This data protection policy ensures that we:

Comply with data protection law and follow good practice;

Protect the rights of staff, customers and partners;

Are open about how we store and process individuals' personal data; Protect the firm from the risks of a data breach

Data protection law

The General Data Protection Regulation describes how we 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 General Data Protection Regulation is underpinned by six important principles. These say that personal data must:

1. Be processed fairly, lawfully and in a transparent manner;
2. Be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Be accurate and, where necessary, kept up to date;
5. Be kept for no longer than is necessary for the purposes for which the personal data is processed; and
6. Be processed in a way that ensures appropriate security of the personal data.

Ordit 29 Dovedale road, Bolton, BL2 5HT.

2. People, risks and responsibilities.

This policy applies to:

Dovedale offices and associates vehicles

All staff and volunteers

All contractors, suppliers and other people working on behalf of Ordit.

It applies to any information which we hold relating to an individual from which an individual can, directly or indirectly, be identified. This can include:

Names of individuals Postal addresses Email addresses Telephone numbers Training records and Data protection risks

This policy helps to protect Ordit from some very real data protection risks, including:

Breaches of confidentiality. For example, information being given out inappropriately.

Excess information collection. For, example collecting more personal information than is necessary for the firm to provide the service.

Failing to offer choice. For example, all individuals should be free to choose how the company uses data relating to them.

Out of date. For example, storing out of date and inaccurate information.

Data retention. For example, keeping personal information indefinitely when no longer in use.

Reputation damage. For example, Ordit could suffer if hackers successfully gained access to sensitive data.

Responsibilities.

Everyone who handles personal information within Ordit has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

The Founders (Daniel Ison and Lynne Fitzharris) are ultimately responsible for ensuring that Ordit meets its legal obligations.

The Compliance Officer. (Ruth Case) is responsible for:

Processes:

- o Keeping associates updated about data protection responsibilities, risks and issues.
- o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- o Arranging data protection training and advice for the people covered by this policy.
- o Handling data protection questions from staff and anyone else covered by this policy.
- o Dealing with requests from individuals to see the data Ordit holds about them (also called 'subject access requests').
- o Dealing with requests from individuals who want to exercise their rights under GDPR (e.g. request erasure of their personal information)
- o Checking and approving any contracts or agreements with third parties that may handle Ordit's sensitive data.
- o Carrying out data protection risk assessments.
- o Carrying out internal data protection audits.

Ordit 29 Dovedale road, Bolton, BL2 5HT

Information technology

- o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- o Performing regular checks and scans to ensure that security hardware and software is functioning properly.
- o Evaluating any third-party services Ordit is using to store or process data. For instance, cloud computing services.
- o Evaluating any third-party services and companies Ordit is using to store or process data. For instance, IT services, trainers and consultants.

Marketing

- o Approving any data protection statements attached to communications such as emails and letters.
- o Addressing any data protection queries from journalists or media outlets like newspapers.
- o Where necessary, working with other associates to ensure marketing initiatives abide by the data protection principles.

3 General associate guidelines

The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required, associates can request it from Dan Ison, Lynne Fitzharris or Ruth Case.

Ordit will provide training to all associates to help them understand their responsibilities when handling data.

Associates 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 Ordit 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.

Associates should request help from the Compliance Officer if they are unsure about any aspect of data protection.

Ordit 29 Dovedale road, Bolton, BL2 5HT

4 Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to a Compliance Officer.

When data is stored on paper, it should be 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 should be kept in a locked drawer or filing cabinet.

Associates 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:

- o Data should be protected by strong passwords that are changed regularly and never shared between employees.

- o If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

- o Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.

- o Servers containing personal data should be sited in a secure location, away from general office space.

- o Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- o Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

- o All servers and computers containing data should be protected by approved security software and a firewall.

5 Data use.

Personal data is of no value to Ordit unless we 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:

- o When working with personal data, associates should ensure the screens of their computers are always locked when left unattended.

- o Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.

- o Data must be encrypted before being transferred electronically. The compliance officer can explain how to send data to authorised external contacts.

- o Personal data should only be transferred outside of the European Economic Area if the receiving firm has adequate data security measures.

- o Associates should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Ordit 29 Dovedale road, Bolton, BL2 5HT

6 Data accuracy.

The law requires us to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all associates who work with data to take steps to ensure it is kept accurate and up to date.

- o Data will be held in as few places as necessary. Associates should not create any unnecessary additional data sets.

- o Associates should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

- o Ordit will make it easy for data subjects to update the information it holds about them. For instance, via the websites.
- o Data should be updated immediately inaccuracies are discovered. For example, if a customer can no longer be reached on his stored telephone number, it should be removed from the database.
- o It is the Compliance officers responsibility to ensure marketing databases are checked against industry suppression registers every 12 months.

7 Individuals' rights.

All individuals who are the subject of personal data held by Ordit are entitled to:

1. Obtain confirmation about what information we hold about them and to access copies of that information.
2. Request the correction of inaccurate personal information.
3. Request the erasure of their personal information.
4. Restrict how their personal information is used.
5. Receive their personal information in a legible and transferable format. For example, in an Excel format.
6. Stop the use of their personal data.
7. Object to their personal information being used for an automatic decision.

8. Be informed about why their personal information is being collected and how it will be used.

Ordit must make it easy for individuals to exercise their rights in relation to their personal information. Where an individual makes any of the above requests we must comply within one month.

Ordit cannot charge a fee to an individual for exercising his rights unless the request from the individual is excessive. For example, because it is a repetitive request that has previously been complied with. Any charge should be limited to the administrative cost of complying with the request.

The Compliance Officer will always verify the identity of anyone making a request to exercise his individual rights before actioning the request.

8 Disclosing data for other reasons.

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the individual.

Under these circumstances, Ordit will disclose the requested data. However, the Compliance Officer will ensure the request is legitimate, seeking assistance from the founders and Ordit's legal advisers where necessary.

Ordit 29 Dovedale road, Bolton, BL2 5HT

9 Providing information.

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

- o How the data is being used
- o Who their data is being shared with
- o How long their data will be stored
- o How to exercise their rights
- o How to lodge a complaint with the Information Commissioner's Office

To comply with the above, Ordit has a privacy statement, which sets out how data relating to individuals is used by Ordit.

This is available on request. A version of this is also available on our website.

10 Declaration.

I agree I have read and understood the GDPR Policy above and agree to abide by the principals:

Name: :.....

Signed:.....

Date:..... Positon:

.....

Ordit 29 Dovedale road, Bolton, BL2 5HT