Data Protection Policy

General Data Protection Regulations 2018

Data protection policy

Key details

- Policy prepared by: Sally Dale Director 12.2.2018.
- Approved by: Sean Stokoe Director 13.2.2018.
- Policy became operational on: 1st March 2018
- Next review date: 31 January 2021

Introduction

As part of our business, we at ioda Ltd need to gather and use certain information about individuals including our:

- Customers
- Learners
- Apprentices
- Suppliers
- Business contacts and partners
- Employees and
- Other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be 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 ioda Ltd:

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

Data protection law

The General Data Protection Regulation 2018 (GDPR) describes what and how organisations, including ioda Ltd, must collect, handle and store personal information, including its disposal and when it must be deleted.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information collected must be used fairly, stored safely, not disclosed unlawfully and deleted within stipulated timescales.

The GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date

5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. 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 - Scope of policy

This policy applies to:

- The head office of ioda Ltd
- All locations where ioda Ltd staff work including home office accommodation
- All staff and associates of ioda Ltd
- All contractors, suppliers and other people working on behalf of ioda Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2018 it will be treated as coming under them. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Data protection risks

This policy helps to protect ioda 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.

Responsibilities

Everyone who works for or with ioda Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each individual or team 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 **board of directors** is ultimately responsible for ensuring that ioda Ltd meets its legal obligations.
- The Directors, Sally Dale and Sean Stokoe are responsible for:
    - Keeping themselves and staff 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 ioda 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.
    - Ensuring data is deleted within agreed and appropriate timescales.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Evaluating any third-party services, the company is considering using to store or process data and ensuring, as partners, they perform regular checks and scans to ensure security hardware and software is functioning properly, for instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with staff to ensure marketing initiatives abide by data protection principles

Data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data breach process

If a personal data breach is experienced by any ioda employee, this must be reported to the Head of Training and Operations (HTO) within 24 hours. The HTO will consider whether this poses a risk to the individual(s) concerned. The HTO will consider the likelihood and severity of the risk to people's rights and

freedoms, following the breach. When this assessment has been made, if it's likely there will be a risk then the HTO must notify the ICO; if it's unlikely then the HTO does not have to report it to the ICO. Every breach does not have to be reported to the ICO.

The breach of information should be recorded on a Data Breach form and saved on the shared drive.

General guidelines for staff

- 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, employees can request it from their line managers.
- **ioda 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. Only the person whose password it is and the Directors should be aware of the passwords.
- 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.
- Data **must always be stored and erased** as outlined in this policy.
- Employees **should request help** from their line manager or Director if they are unsure about any aspect of data protection.

Data storage rules

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to their line manager or company Directors.

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 **unoccupied**, **the main office** must always remain locked and secure with the alarm system activated.
- When not required and working from home, any paper or files should be kept

in a locked drawer or filing cabinet.

- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, e.g. on a printer, or in classrooms where delegates are present.
- **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, in line with the company's standard backup procedures.
- All company laptops must be kept in a secure place when not in use. They must not be left in vehicles overnight and if travelling during the day and the vehicle is unattended must be stored out of sight in the boot.
- All company laptops must be encrypted through password access and data saved directly to this device erased in line with the erasure rules detailed in this policy
- All laptop data must be saved directly onto the companies secure shared cloud facility.
- Data should **never be saved directly** to mobile devices such tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.
- Data will be stored for the following periods:
    - Employee Details: During terms of employment and a period of 3 years after contract termination.
    - General Client Data: 5 years for all clients other than research related
    - Learner Details: For those attending accredited programmes – 5 years. Non-accredited 3 years. From completion date.
    - Research data and findings: All data from confidential research – 7

years.

- Supplier Details: 5 Years after termination of business relationship.
- Business Partner Details: 5 Years after termination of business relationship.

Data erasure and off boarding rules

All persons whose details are held by ioda have the right to request erasure and the right to be forgotten from data subjects. Client off boarding is defined as the proactive management and removal of redundant, obsolete or incorrect information and data held by ioda.

In order to meet these requests in an adequate and timely fashion ioda will apply the following procedure.

1. **Assess request**

Once the request is received from a data subject, ioda will assess the request and determine if it has legal basis to hold onto the data. If not, then ioda must strive to identify all the repositories and systems that contain this personal information on the data subject.

2. **Determine the impact of off boarding on the data subject**

If it is decided to off board the data, then it is important to check for any interdependencies on the data that may impact on other data subjects. Once a full understanding of the data subject's associations and activities is gained, the process to disassociate reliant parties can commence.

3. **Off boarding the data**

To ensure full auditability of the process, ioda will add in a reason why off boarding is taking place (e.g. request for erasure by data subject). A Director should approve the off boarding process before being marked as complete.

4. **De-activating from IT systems**

The final step in the off-boarding process involves ensuring that the information cannot be further used by ioda. This should include a notification that the data has been successfully off boarded or quarantined from all related IT systems.

5. **Confirm erasure of data**

The final step involves a confirmation in writing to the data subject that the data has been effectively erased or quarantined from all internal systems in compliance with their request under GDPR.

6. **Offboarding breach response**

Staff must report a breach of this off boarding rule to a Director "without undue delay and where feasible no later than 72 hours once a breach has been identified, except where the personal data breach is unlikely to result in a risk to the rights and freedoms of a data subject".

Data use

Personal data is of no value to ioda Ltd unless the company 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**. Guidance will be provided if required.
- Personal data should **never be transferred outside of the European Economic Area**.
    - Employees **should try not save copies of personal data to their own computers** by **accessing and updating the central copy of any data.**
    - However if personal data is saved, then the outlined security and deletion protocols must be observed.

Data accuracy

The law requires ioda Ltd to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort we at ioda will put into ensuring its accuracy.

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.
- ioda Ltd will make it **easy for data subjects to update the information** we hold about them. For instance, via the company website.
- 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 Directors responsibility to ensure **marketing databases are checked** against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by ioda 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 Director(s) at info@ioda.com A Director can supply a standard request form, although individuals do not have to use this.

Individuals can make an initial request for information free, and subsequent requests, or requests that are deemed manifestly unfounded or excessive will be charged £10 administration fee per subject access request. The Director(s) will aim to provide the relevant data within 14 days.

The Director(s) will always verify the identity of anyone making a subject access request before handing over any information.

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 data subject.

Under these circumstances, ioda Ltd may disclose requested data. However, the Directors(s) will ensure the request is legitimate, seeking guidance from the company's legal advisers where necessary.

Providing information

ioda Ltd aims to ensure that individuals are aware that their data is being processed, and they understand the following:

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

To these ends, the company has a privacy statement, (See appendix one) setting out how data relating to individuals is used by the company and is available on request

Appendix One

ioda Ltd - Privacy Policy

This privacy policy explains how ioda Limited of 4 Grimston Grange Offices, Grimston Park, Tadcaster, LS24 9BX, company number 3352708 ('ioda Ltd', 'We', 'Us'), uses information about current and prospective customers, Learners and apprentices.

Our Privacy Policy explains:

1. What information do we collect about you?
2. How will we use the information about you?
3. Access to your information, correction and deletion
4. Cookies
5. Changes to our privacy policy
6. How to contact us

If you have any questions, please contact us and we will be happy to explain or discuss any concern you may have.

What information do we hold about you?

Students - Learners - Apprentices

- We collect information about you when you enrol on an accredited training programme or apprenticeship. This includes your full name, contact details; date of birth, for apprentices your National Insurance number, as well as equality monitoring data.
- In order to meet the Public Sector Equality Duty of the Equality Act 2010 ioda will collect equality data for Apprentices. This will include information relating to the Equality Act Protected Characteristics. This information enables us to gain an overview of our learners' profile, benchmark our services against local and national statistics and identify any potential areas for improvement.

Customers

- We hold information that you have provided to us directly via our website, via direct contact with one of our employees or associates, or via one of our partners if you have provided consent for them to pass on your details to ioda Ltd.
- This can include your full name, job title, business email and postal addresses and business phone numbers.
- We also collect information when you buy our services and when you provide feedback.

How we use the information about you?

Students – Learners – Apprentices

- We only collect what is needed for the delivery and if necessary for funding and auditing purposes of the programme or apprenticeship you are enrolling on
- This information helps us to tailor our programmes to suit your learning needs, evidence the training you have received and demonstrate to auditors and qualification awarding organisations that compliance and quality requirements are being stringently met.
- To deliver this agreed standard, ioda will need to provide your data to a limited number of organisations involved in the delivery of services to you such as accredited qualifications, apprenticeship or in some rare occasions, work related training. These organisations include:
    - Technology suppliers
    - Education & Skills Funding Agency (ESFA)
    - Ofsted
    - Relevant qualification awarding bodies e.g. Chartered Management Institute (CMI) or the Institute of Leadership and Management (ILM).
- Please note that for apprenticeships we are required by the Education and Skills Funding Agency to retain your personal information for ten years for auditing and funding purposes. This is stored securely and fully deleted from our systems once this time has passed.
- ioda Ltd will not use or share your information for marketing purposes.

Clients and customers

- We will only use the information to contact you about ioda's training services that may be relevant to your organisation.
- Your information may be shared with a limited number of secure organisations such as our technology suppliers GCI.
- If you buy our services (or products) we will only use your information to carry out the requirements of the contract. In some cases, we will need to provide your data to a limited number of organisations involved in the delivery of an apprenticeship, such as our technology suppliers, the Education & Skills Funding Agency, Ofsted and the relevant qualification awarding bodies.
- We are required by the Education and Skills Funding Agency to retain your information for ten years for auditing and funding purposes. This is stored securely and fully deleted from our systems once this time has passed.

Access to your information, correction and deletion

- You have the right to request a copy of the information that we hold about you. If you would like a copy of some or all of your personal information, please email or write to us at the address below.
- It is important that your personal information is accurate and up to date. Please contact us to make any corrections or ask us to remove information you think is inaccurate.
- You can unsubscribe from our emailing list at any time by email or phone number below. Your information will be removed from all email lists but will be held on a secured suppression list so that we can check against this before mailing out to any newly obtained contact lists.
- For **apprentices** who have started one of our apprenticeship programmes, we will not be able to remove your data for ten years due to contractual, auditing and compliance purposes.

Cookies

- Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity. For further information visit www.aboutcookies.org or www.allaboutcookies.org. You can set your browser not to accept cookies and the above websites tell you how to remove cookies from your browser. However, in a few cases some of our website features may not function as a result.

Changes to our privacy policy

We keep our privacy policy under regular review and we will place any updates on this web page. This privacy policy was last updated in February 2018.

How to contact us

Please contact us if you have any questions about our privacy policy or information we hold about you via the following: Email

Email: info@ioda.com

Telephone: 01937 831414

By post: ioda Ltd

Data Privacy

4 Grimston Grange Offices, Grimston Park

Tadcaster

LS24 9BX

Review date: 31 January 2021

Approved by: 

Sally Dale, Company Secretary


Sean Stokoe, Chief Executive