Infosec Cloud
Data Protection Policy

Context and overview

Key details
- Policy prepared by: Andy Hanson
- Approved by board / management on: 28th October 2016
- Policy became operational on: 1st January 2017 22nd
- Last Review date: December 2018 31st
- Next review date by: December 2019

Introduction

Infosec Cloud 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 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 Infosec Cloud:

- Complies with data protection law and follow 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 organisations — including Infosec Cloud— 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:

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

Policy scope

This policy applies to:

- The head office of Infosec Cloud
- All remote locations for Infosec Cloud
- All staff and volunteers of Infosec Cloud

* All contractors, suppliers and other people working on behalf of Infosec Cloud
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

Data protection risks

This policy helps to protect Infosec Cloud 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 Infosec Cloud 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 roles have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that Infosec Cloud meets its legal obligations.

- The Data Protection Officer is responsible for:
    o Keeping the Board 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 Infosec Cloud holds about them (also called 'subject access requests').
    o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The Chief Technical Officer is responsible for:
    o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    o Performing regular checks and scans to ensure security hardware and software is functioning properly.
    o Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- The Marketing Manager is responsible for:
    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 staff to ensure marketing initiatives abide by data protection principles.

General staff 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, employees can request it from their line managers.
- Infosec Cloud 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.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

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.
- 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, in line with the company's standard backup procedures.
- 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.
- All data provided through the SATT platform is only stored in the UK in our secured data centres.

Data use

Personal data is of no value to Infosec Cloud 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, this data should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager 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.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Data accuracy

The law requires Infosec Cloud 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 Infosec Cloud should 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.

- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Infosec Cloud will make it easy for data subjects to update the information Infosec Cloud holds about them.

Produced in confidence by Infosec Cloud Ltd. Version 1.6

- 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 marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.
- When a customer ceases to become an Infosec Cloud customer, data contained in non-CRM solutions (for example SATT) relating to their employees, for instance email addresses and phone numbers will be removed from the Infosec and Infosec partners' records.
- All data stored or passing through our SATT partners is encrypted in transit using TLS/SSL. This includes system logs, email address lists, and other confidential information.

Subject access requests

All individuals who are the subject of personal data held by Infosec Cloud 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 Infosec Cloud 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 support@infosec-cloud.com. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals may be charged to a maximum of £10 per subject access request. The data controller will aim to provide the relevant data within 28 days.

The data controller 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 Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Infosec Cloud 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.

Providing information

Infosec Cloud 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