# Data Protection Policy

**Document Control**
**Reference: Data Protection**
**Issue No: 1**
**Issue Date: 25/04/2018**

## 1. Purpose

iSAMS Ltd has made the security of personal data a priority within the organisation as well as the personal data we process on behalf of our clients. During our day-to-day activities we collect, store and use personal data – we need to ensure that the personal data is kept safe to protect the rights of individuals.

This Data Protection Policy applies to all employees and contractors of iSAMS Ltd and acts as an overview of the GDPR and how data can be protected. The policy covers the following sections:

- Data Protection – An Overview
- Data Protection at iSAMS Ltd
- What you need to know
- Responsibilities

Further information, procedures, policies, logs and records can be found in the 'Information Security & GDPR' section on SharePoint. The iSAMS Information Security Team can be contacted for further assistance or advice.

Having a Data Protection Policy ensures iSAMS Ltd complies with data protection law, that we follow good practice and protect the rights of individuals.

## 2. Data Protection – an Overview

What is GDPR?
The General Data Protection Regulation, 'GDPR', comes into force on the 25th May 2018. In the UK, the GDPR will replace the Data Protection Act 1998, 'DPA'. The GDPR will have a major impact on how we store and use personal data. The aim of the new law is to give individuals new rights over their data. As an overview, the GDPR sets out 6 data protection principles:

- Fair, Lawful and Transparent
  The first principle is that personal data shall be processed fairly, lawfully and transparently. The GDPR shouldn't prevent the processing of personal data but to ensure that we process if fairly without adversely affecting the rights of individuals.
- Only used for a limited purpose
  The second principle is that personal data shall only be collected for specific, legitimate purposes and not processed in a manner not in line with those

purposes. Data can only be used for what is was collected for and not used for other purposes.

- Data Minimisations
  The third principle is that personal data shall be adequate, relevant and limited to what is necessary. In other words, we cannot collect and process data which has no relevance or isn't needed.

- Accuracy
  The fourth principle is that personal data shall be accurate and, where necessary, up to date. Data should be checked at point of collection and at regular intervals.

- Data Retention
  The fifth principle is that personal data should only be kept as long as necessary. Please see the iSAMS Independent Ltd policy and schedule for data retention.

- The Security Principle
  The sixth principle is that personal data shall be processed in a manner that ensures appropriate security of the data including protection against unlawful use, accidental loss, destruction or damage. GDPR says we must use 'appropriate, technical and organisational measures to keep data secure'

*What is personal data?*
Personal data is any data which relates to a living individual who can be identified from that data. The most common types of personal data include name, address, phone number and so on.

*What is sensitive data?*
Certain types of data are known as sensitive data and can include information concerning an individual's racial or ethnic origin, political opinions, religious beliefs, sexual life, details of criminal offences and so on.

*Who regulates the GDPR in the UK?*
Each member state of the EU provides an independent public authority to be responsible for monitoring the GDPR regulation. These public authorities are known as the Supervisory Authority. The Supervisory Authority for the UK is the Information Commissioner's Office (ICO).

*What happens if we get it wrong*
The ICO has a wide range of powers and can issue enforcement notices to organisations to remedy a breach. If iSAMS Ltd were to get something 'wrong' or breach the GDPR regulation, the ICO may publicise the breach on its website which would impact our reputation. The ICO also has the right to audit iSAMS Ltd and can impose fines up to €20 million or 4% of our global turnover.

*Who do I contact to speak about Data Protection issues or queries?*
iSAMS Ltd has an Information Security Team and an appointed Data Protection Officer who oversees the compliance with the legislation along with the associated

policies. Any queries or concerns which are not covered the iSAMS Ltd security policies can be directed to the Data Protection Officer. Issues can also be raised to the Data Protection Officer.

*Who are controllers and processors?*
Controller and Processors refers to those organisations, persons or authorities who either decide how the data is processed or carry out the processing.

*The Controller – the person or persons who determine the purposes for which and the way personal data is to be processed. In our context, the controller is the client.*

*The Processor – the persons or persons who processes the data on behalf of the data controller. In our context, iSAMS Ltd is the processor. iSAMS Ltd processes data on behalf of the client under their instructions.*

*What is processing?*
In short, processing means obtaining, recording, holding or carrying out any operation on the data.

For breaches, access requests, privacy impact assessments, pri2vacy notices and associated information please refer to the iSAMS Ltd security policies.

## 3. Data Protection at iSAMS Ltd

The following points outline some key areas for you to be aware of. However, please read the policies and documents located in the Information & GDPR section in SharePoint for further information.

New uses of Personal Data – Privacy Impact Assessment
You may want to introduce something new to iSAMS Ltd such as a change to how existing data is used, a new piece of software or some new technology. Under GDPR these changes must include data protection by design. We need to ensure that data protection is built into new uses of data and sometimes this may require a Privacy Impact Assessment (PIA). Please see the iSAMS policy on PIA.

Data Breaches
However far we implement the protection and security of personal data we may at some point experience a security breach leading to the accidental or unlawful loss of personal data. It could be the result of a cybercrime, someone could have left their laptop on a train or accidently shared personal data with a third person in error. If you become aware of a data breach you must report the issue or incident as soon as possible following the Data Breach Process located in the Information and GDPR section on SharePoint.

The ICO gives us 72 hours to report a breach**. Please do not report a breach to the ICO.** The DPO or a member of the iSAMS Information Security Team will liaise with the ICO on your behalf.

*Sharing Personal Data with other Organisations*

If you're looking to engage with any new supplier and you know that the supplier will be obtaining personal data please contact the iSAMS Information Security Team or the DPO.

The GDPR requires us to vet suppliers to ensure they offer the appropriate level of security and to ensure there is a written contract which is GDPR compliant.

*Subject Access Requests*
Under GDPR an individual may submit a Subject Access Request (SAR) to have access to their personal data. A SAR is a written request asking to obtain such personal data which iSAMS Ltd may hold. There are strict timelines for complying with a SAR and to help facilitate this iSAMS Ltd have a 'request form' which you can use. Please see the SAR process within the Information & GDPR Section in SharePoint.

*Privacy Notices*
Under GDPR we must advise individuals how their personal data is processed. Individuals are advised using a 'Privacy Notice'. The iSAMS Ltd Privacy Notice explains how your data is collected, what we do with it, who we share it with and how long we keep it. The iSAMS Ltd Privacy Notice is available in the Information & GDPR section in SharePoint.

*Record of Processing*
Under GDPR we need to keep a 'Record of Processing'. The Record of Processing explains the data processing activities at iSAMS Ltd which can be used by the ICO. The policy and the records can be found in the Information & GDPR section in SharePoint. Having a Record of Processing in place helps iSAMS Ltd demonstrate compliance with GDPR.

*Data Retention*
Personal data may only be kept no longer than is necessary for the purpose it was collected for. At iSAMS Ltd we have a Data Retention Policy and a Data Retention Schedule which explains the types of employee data held by iSAMS Ltd and the retention periods (how long we keep it for).

## 4. What you need to know

*Employee Guidelines*
iSAMS Ltd will provide Information Security training to all employees along with security policies, processes and documentation.

The following are some general guidelines:

- You should only access data for legitimate work purposes
- Only share data using the approved methods – Data should not be shared informally.
- You should take steps to keep data secure especially when working remotely
- Lock your computer when not in use
- Don't leave sensitive personal data lying around the office
    - Don't leave printouts containing private personal data on your desk

    - Lock them in a drawer or shred them. It's easy to glance and see documents
    - Keep your desk tidy and documents locked away reducing risk of leaks
- Be cautious of suspicious emails and links
- Use hard-to-guess passwords
- Don't be tricked into giving away confidential personal data

    - Don't respond to emails or phone calls requesting confidential company information including employee personal data, financials or company secrets.
    - It's easy for an unauthorised person to call us and pretend to be an employee or one of our business partners.
- Don't use an unprotected computer
    - When you access sensitive personal data from a non-secure computer, like one in an Internet café or a shared machine at home, you put the personal data you're viewing at risk
    - Make sure your computer is running the latest security patches and antivirus
- Stay Alert
    - Always report any suspicious activity. We need to ensure data isn't lost or stolen
    - iSAMS Ltd depends on keeping our personal data safe
    - In case something goes wrong, the faster we know about it, the faster we can deal with it. Speak to the DPO or iSAMS Information Security Team.

**Data Storage**

Data should be stored securely using the agreed areas. When data is stored on paper it should be kept in a secure place where unauthorised people cannot access or see it.

For paper documents:

- When not required, paper files should be kept locked away
- Paper and printouts should not be left where unauthorised people can access them (i.e. left on a printer)
- Paper and printouts should be shredded and disposed of when no longer required

For electronically stored data:

- Data should be protected by strong passwords
- Data stored on removable media should be kept securely when not in use
- Data should only be stored on designated drives, network shares and cloud services
- Data shouldn't be saved directly on laptop as the only master copy

**Data Accuracy**

We need to ensure that data is kept up to date and it is the responsibility of all of us to take reasonable steps to ensure accuracy.

Such steps include:

- Not replicating data unnecessarily
- Updating data as updates become known
- Data should be updated or checked as and when inaccuracies are discovered
- Prompting employees and clients to update their details

## 5. Responsibilities

Everyone has some responsibility for the protection of data, how it is collected, stored and handled. Each team that handles personal data must ensure they are following the principles.

Board of Directors

- Ultimately responsible for ensuring that iSAMS Ltd meets its legal obligations

iSAMS Information Security Team, Data Protection Officer/Head of Service, Jason Lloyd

- Keeping the company updated about data protection responsibilities, risks and issues
- Reviewing and updating data protection procedures, policies and schedules
- Arranging Information Security Training and advice to all employees
- Dealing with SAR requests from individuals
- Checking contractual agreements
- Liaising with the ICO
- Monitoring and ensuring GDPR compliance

Network Manager, Arturs Kirsis

- Ensuring all systems, services and equipment used for storing data meets acceptable security standards
- Performing regular checks to ensure software and hardware function correctly

Head of Marketing, Lisa Evans

- Approving any data protection statements attached to communications
- Addressing and advising on any queries from journalists or social media

### Change History Record

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 0.1 | Initial issue | Head of Service and Operations | 25/04/2018 |