Ensite Business Technology: GDPR & General Data Protection Policy

Data protection policy

Context and overview

Key details

- Policy prepared by: Robert Polland (Director)
- Approved by board / management on: 02/05/2018
- Policy became operational on: 02/05/2018
- Next review date: 02/04/2019

Introduction

Ensite Business Technology Ltd, needs to gather and use certain information about individuals. Ensite Business Technology Ltd, also needs to manage or process personal and non-personal sensitive data for its clients as part of its service offerings.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

As such, Ensite Business Technology Ltd, is registered with ICO (Information Commissioner's Office) as both data controllers & processors. Our Policy Registration Document and our "Statement Of Registration Entry" can be found on our website at www.ensite.co.uk/gdpr/

This policy describes how this personal data and other non-personal data, must be collected, handled and stored to meet the company's data protection standards which adhere to both GDPR and the Data Protection Act 1998

Ensite Business Technology Ltd, as an IT Support Company, also has remote access to other companies' data, but since it neither acts as controller or processor (except in the case of backup services) is not strictly accountable to specific GDPR but is bound by Data Protection laws and ethics.

Why this policy exists

This data protection policy ensures Ensite Business Technology Ltd:

- Complies with data protection law, The Data Protection Act 1998
- Complies with GDPR (*General Data Protection Regulation*)
- 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

GDPR & Data protection law

The Data Protection Act 1998, and General Data Protection Regulation April 2016, describes how organisations — including Ensite Business Technology Ltd— must collect, handle and store personal information and other non-personal sensitive data.
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 & GDPR is underpinned by 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 Ensite Business Technology Ltd
- All branches of Ensite Business Technology Ltd
- All staff and volunteers of Ensite Business Technology Ltd
- All contractors, suppliers and other people working on behalf of Ensite Business Technology 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 and/or GDPR. This can include:

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

It applies to access of such data, even when Ensite Business Technology Ltd, do not either act as Controller or Processor of that information.

- How Ensite Business Technology Ltd, accesses data
- Protections in place when Ensite Business Technology Ltd, accesses data
- When Ensite Business Technology Ltd, accesses data
- Permissions required for Ensite Business Technology Ltd, to access data

Data protection risks

This policy helps to protect Ensite Business Technology 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 Ensite Business Technology Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data, or have "top level" file access (i.e. they will not open the file, but have access to it) 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 Ensite Business Technology Ltd meets its legal obligations.

- 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 Ensite Business Technology 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 **IT Directors** are 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.

- 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 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**. If Specific access to confidential information is required, it needs to be approved by a Director of Ensite Business Technology Ltd .

• **Ensite Business Technology 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 a Director, 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 from a Director at Ensite Business Technology Ltd.
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 devices**, and should only be uploaded to an **approved cloud computing services**.

• Devices containing personal data should be **sited in a secure location**, away from general access.

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

• All computers containing data should be protected by ESET Endpoint Antivirus **approved security software and MS Windows firewall**.

Data use

Personal data is of no value to Ensite Business Technology 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.

Partial or full personal data contained within email addresses are used on a **strict Legitimate Interest** rule, and requests to change to descriptive or non-personal format will be updated on request within 5 working days.

• Data must be **encrypted before being transferred electronically**.

• Unencrypted personal data should **never be transferred outside of the European Economic Area**.

Data Access

as an IT Support Company Ensite Business Technology Ltd, has access to other companies' data, both onsite (at a company's workplace) and via remote connections.
Usually and only under exceptional circumstances (apart from data backup) it neither acts as controller or processor, thus is not strictly accountable to specific GDPR, but is bound by Data Protection laws and ethics, and therefore implement the following specific protections.
The term TL Data will be used frequently, and as such refers to "Top Level Data". This explicitly means that we are able to see the data files (e.g. file called mydata.xls) but not the contents of that file.

- When Ensite Business Technology Ltd, accesses TL data via a remote connection, it will always use a 3rd party specialist organisation to provide the platform for remote desktop connection. Currently, it only uses two of the world's leaders in this technology, to provide secure and private connection. Any "User Not Present" access, is additionally protected by two layer authentication methods and strong login account password.
- When "onsite" at customer premises, Ensite employees will only access TL data with direct permission of account owner or senior responsible person.

- Ensite Business Technology Ltd, will only access TL data on request of “Support On Demand” or by pre-arranged support, except when required to access a system “ad hoc” for system management (such as MS Updates) and functional legitimate purpose in the interest of the client. Under no circumstance will personal data files be read, edited, opened or transferred during this process.
- Permissions required for Ensite Business Technology Ltd, to access data that contain personal information within a file, must come from the controller of that data, or a person appointed as the responsible overall Data Control Officer

Data Management for Clients and/ Partners

Ensite Business Technology Ltd, as part of its services, will manage data on behalf of a client or partner. This is almost exclusively, as part of backup and recovery processes, or email account hosting and management.

- Data backup is provided by one of two major services in this sector. Both platforms provide high levels of encryption during transfer and storage, thus even in the unlikely event of an account breach, the data within is unreadable since private encryption keys are in place.

- Both data backup platforms conform to GDPR, and if you receive this service from us, then we will communicate these details directly by email.

- Access by Ensite Business Technology Ltd, to secure data stores, will only take place on request of the data controller of that particular data, and first attempt at recovery will always be from the original PC that transmitted the data to the secure backup store. If Ensite Business Technology Ltd, has to access the account direct to recover data to another target device, then this will be under agreement of the data controller of that data, and transmission will secured via SSL connection and encrypted transfer. Data Accesses under this process, will be subject to the same rules of access as described above in “Data Access” section.

The provision of email services is through a single platform, using a UK based hosting company, who house their mail servers in the UK at **Next Generation** data centre in Newport.
The data centre conforms to the following standards.

- ISO9001 - Quality Management
- ISO14001 - Environmental Management
- ISO27001 - Information Security Management
- PCI DSS Compliance - Payment Card Industry
- SSAE16/ISAE3402 – Assurance

- Security updates, patches, script changes and implementation of latest software on the mail servers (e.g. new PHP level) are managed in a timely manner by the hosting company. During a rollout of new hardware May/June 2018, all email accounts will necessarily be required to connect via SSL connection, and no plain text email transmission will no longer be permissible in order to further enhance security.

- Access by Ensite Business Technology Ltd, to any single email account will only be on specific instruction by either the account owner (who is both Controller and Processor), or a senior responsible person within the company requesting access, who has the necessary authority to grant permissions. Access to email accounts is always via secure SSL connection. Access by Ensite Business Technology Ltd, to the contents of a specific email will follow the same guidelines, and the necessary permissions for Ensite Business Technology Ltd, to view information from the sender, will lie with the data controller/processor who requested Ensite Business Technology Ltd.'s action.

Data accuracy

The law requires Ensite Business Technology 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 Ensite Business Technology Ltd 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.
• 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.

• Ensite Business Technology Ltd will make it **easy for data subjects to update the information** Ensite Business Technology Ltd holds 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.

• Ensite Business Technology Ltd do not use **marketing databases.**

Subject access requests

All individuals who are the subject of personal data held by Ensite Business Technology 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 admin@ensite.co.uk
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.