MSS-DP-DOC-11.1

DATA PROTECTION POLICY

Time to Reply Ltd

Version 1.0 August 2019

Classification:	Private		
Version:	1		
Document title:	MSS-DP-DOC-11.1 Data Protection Policy		
Document management	Dane Spear	**Authorised by:**	Dane Spear
Revision interval:	Annually	**Last revision:**	24/10/2019

Revision History

Contents

1. Management Summary

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). This Data Protection Policy forms the basis for complying with legal data protection requirements as well as the protection of the processed personal data of Time to Reply Ltd

Data protection is essential for Time to Reply Ltd in order to meet the legal requirements for handling person-al data. This data protection Policy is therefore made binding on all the organisation's internal pro-cesses. This is data protection by design and is fundamental to the company's policy and attitude to data protection.

Time to Reply Ltd is both a data controller and a data processor as defined under the Act. The former because we hold necessary data on our staff, subcontractors, suppliers and customers. The latter because we provide cloud processing services for government and private sector customers.

Under the Act, everyone responsible for using personal data has to follow strict rules called data protection principles. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

This Data Protection Policy regulates the handling of personal data. In particular, it is intended to:

- Assign responsibilities and obligations for all relevant privacy issues,
- Raise awareness of the need for strategic, technical and organisational measures to ensure data protection requirements, and
- Define the procedure for dealing with data Breach incidents.

2. Principles

2.1 Policy Statement

Time to Reply Ltd commits to the following:

- To comply with the Data Protection Act 2018 and with best practice.
- To respect the rights of individuals.
- To be open and honest with individuals whose data is held.
- To provide training and support for staff who handle personal data so that they can act confidently and consistently.

- To notify the Information Commissioner and any affected persons and organisations of any breach.

2.2 Management Commitment

The management of Time to Reply Ltd considers this Data Protection Policy to be part of its corporate strategy. The Board has reviewed and fully supports the objectives and principles of the data protection policy in line with business strategy and objectives.

2.2 Policy

Data protection management is the responsibility of all staff but is managed and controlled by the Data Protection Officer on behalf of the Board for all relevant legal, technological and organisational matters.

The purpose of the policy is to:

- Comply with the Data Protection Act 2018
- Implement of Good Practice
- Protect Clients, Suppliers, Staff and other individuals
- Protect the company

2.3 Scope

This policy applies to all staff and all staff locations, all contractors and sub-contractors and all suppliers. Suppliers are required to implement their own Data Protection policies which fully conform to the Data Protection Act of 2018 or equivalent GDPR regulations if the supplier's main business location is outside the UK.

2.4 Data Protection Officer

The company has appointed a Data Protection Officer who is responsible for ensuring that the provisions of the Act are adhered to and for monitoring the adherence to policies and processes. The responsibilities of the DPO include:

- Staff awareness of Data Protection, including staff training.
- Briefing the Board on their Data Protection responsibilities.
- Reviewing Data Protection and related policies.
- Handling subject access requests.
- Approving unusual or controversial disclosures of personal data.
- Approving contracts with Data Processors.
- Monitoring compliance with legal requirements.
- Monitoring compliance with procedures for the protection of personal data.
- Data protection impact assessment.
- Cooperation and liaison with the supervisory authority.
- Contact point for the supervisory authority on work-related issues.
- Point of contact for reporting breaches of data protection

2.5 Users

Each employee is responsible for complying with the Data Protection Policy.

2.6 Summary

Appropriate technical and organisation measures should be taken against unauthorised or unlawful processing or disclosure of personal data and against accidental loss, destruction of or damage to personal data. These measures include:

- Encryption of data
- Ongoing security reviews
- Appropriate backup and restore capabilities
- Regular testing of business continuity plans and data security
- Process for recording security breaches to management and to the Information Commissioner's Office (ICO)
- Staff training: all staff are required to complete Data Protection and Cybersecurity training annually
- Monitoring of adherence to the policy
- Assessing and monitoring supplier's adherence to the Act

In addition, this policy and associated procedures includes the management of:

- Smartphone security, password protection and erasure if lost.
- Laptop encryption and extent of data held on laptops.
- Physical security of paper documentation and office computers.
- Password protection and resetting.
- Internet security and spyware protection.
- Email encryption, secure messaging and secure file-sharing.
- Information held online via third-party servers.
- Back-up drives.
- Secure document disposal.
- Visibility of computer screens.
- Telephone conversations in public or insecure environments.
- Bring your own device (BYOD) policies.
- Staff training about hacking, phishing and malware.
- Secure file sharing.
- Unencrypted email.

4. Processing of data

Personal data may only be obtained for established, unambiguous and lawful purposes and may not be processed in a manner that is incompatible with these purposes. It must therefore only be processed to the extent that it is essential for legitimate business activities.

As part of our operations, we need to obtain and process information. In order to provide our email analytics and email reply time metrics service we process and store email header information that includes the TO, FROM, CC, SUBJECT LINE, TIME STAMPS and MESSAGE IDs located in the email headers (email meta information). In order to access the email header information we require user credentials. The type of credentials that we require and store are dependent on how a mailbox is added to our service. For o365 and G Suite/Gmail we require authentication credentials in the form of Oauth access tokens and usernames. For IMAP and MS Exchange we require server details, username and password and for Mimecast we require an access token. This information includes any offline or online data that makes a person identifiable such as names, addresses, email addresses, usernames and passwords, access tokens, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply:

Our data will be:

- Accurate and kept up to date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)
- In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs.

Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

5. Exercising Data Protection

To exercise data protection, we're committed to:

- Restrict and monitor access to sensitive data (such as authentication credentials)
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

6. Data confidentiality

All data related to the company, its activities, personnel, customers and suppliers and any other sensitive data must be kept secret and not disclosed to any individual or organisation that does not have a legitimate reason to access the data.

Company confidential data must not be allowed to leave the company without the express permission of the Management.

There are areas that are covered in Data Confidentiality and are subject to this clause, that are not part of the Data Protection regulations, including:

- Information about the company (and its plans or finances, for example);
- Information about other organisations, since Data Protection only applies to information about individuals;
- Information which is not recorded, either on paper or electronically;
- Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act.

6. Data protection impact assessment

Prior to the implementation of new technology or procedures, a privacy impact assessment must be conducted to ensure that data security is not compromised. The Data Protection Officer must be informed before such changes are made is responsible for ensuring that the Impact Assessment is conducted and logged and that mitigating actions are conducted.

7. Data Breach

In the event of a breach of data protection from any cause including human error, malicious attack, system failure, the Information Commissioner's Office (ICO) – the supervisory authority - must be notified within 72 hours of the breach. Any member of staff identifying a breach should notify their line manager and the Data Protection Officer immediately so that an assessment can be conducted, and appropriate action taken.

8. Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.