Proviso Systems Ltd

GDPR

Document

As part of Proviso Systems Ltd Compliance with the General Data Protection Regulations (GDPR) 2018

Rev 01

16th May 2018

Proviso Systems Ltd
Everton Road
Mattersey
Doncaster
DN10 5DS

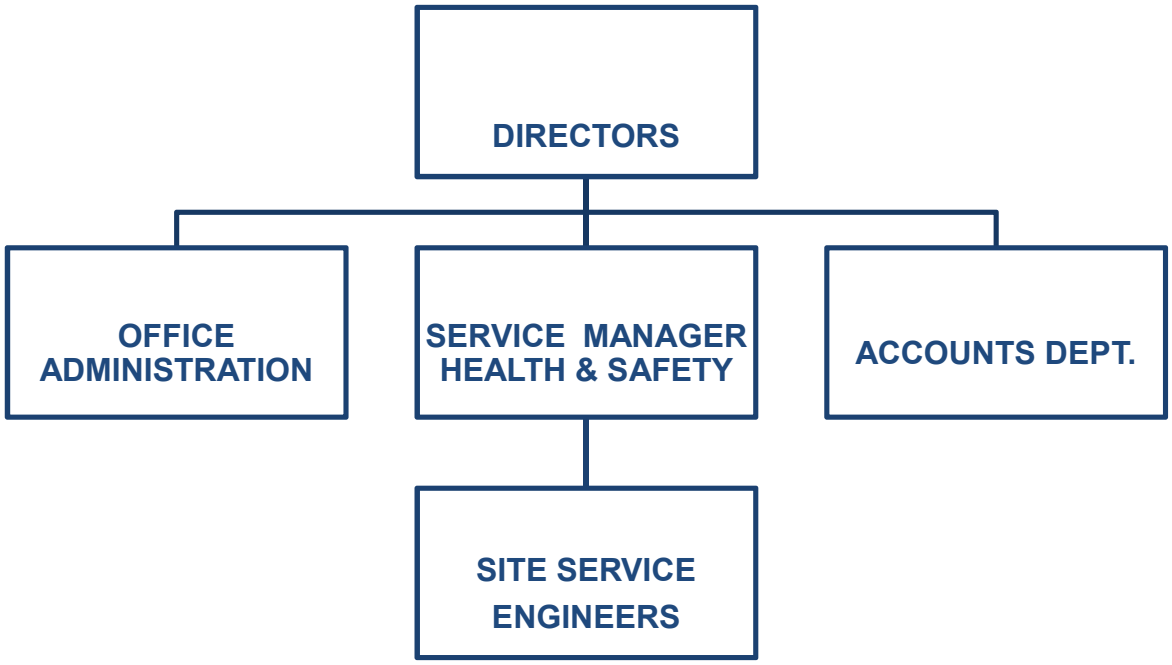
Telephone : 0 (+44) 1777 817 536 Fax : 0 (+44) 1777 816 045
Website : www.proviso-systems.co.uk

CONTENT:

CONTENT:

POLICY INFORMATION:

1.1 Organisation



The name of the employee responsible as the Data Protection Officer

Name: *Chris Deakin* Date: 16/05/2018

Signed: _____

The term "Data Protection Officer " has been used to define the person who (either alone, jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be processed

1.2 Scope of policy

This policy applies to:

- The head office of Proviso Systems Ltd
- All branches of Proviso Systems Ltd
- All staff and volunteers of Proviso Systems Ltd
- All contractors, suppliers and other people working on behalf of Proviso Systems Ltd

It applies to all data that the company holds relating to identifiable individuals, this can include:

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

Proviso Systems Ltd Offices:

Main Office: Everton Road
Mattersey
Doncaster
United Kingdom
DN10 5DS

1.3 Policy operational date

This policy is deemed operational for a maximum of a 3-year period.
The date in which this policy ceases to be operational without review is the 16th of May 2021

1.4 Policy prepared by

This policy has been prepared by…

Name: *Chris Deakin* Date: 16/05/2018

Signed: 

1.5 Date approved by Board/ Management Committee

This policy has been approved by…

Name: *Mike Deakin* Date: 16/05/2018

Position: Director

Signed: 

1.6 Policy review date

This policy will be reviewed at a minimum interval of 3 years.

The policy renewal date is set to be no later than the 16th of May 2021

INTRODUCTION:

2.1 Purpose of policy

Complying with the law:
The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the EU.

Article 6(1)(c) of the GDPR provides a lawful basis for processing data where:
"processing is necessary for compliance with a legal obligation to which the controller is subject."

Following good practice:
The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Proviso Systems Ltd finds it important to follow the General Data Protection Regulations as a form of best practice and to be legally compliant.

Protecting clients, staff and other individuals:
Proviso Systems Ltd understands the requirements to protect our clients, staff and other individuals through the protection of personal data. By following the General Data Protection Regulation, the right of access and the right of erasure and data portability Proviso Systems Ltd will ensure the correct processing of personal data.

Protecting the organisation:
By keeping within the regulations of the GDPR, Proviso Systems Ltd can ensure protection from unlawful accusations and prosecution as a result of the misuse of data.

2.2 Types of data

Personal data:

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data:

The GDPR refers to sensitive personal data as "special categories of personal data".

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

2.3 Policy statement

Proviso Systems Ltd would like to state commitment to the following points.

- To comply with both the law and good practice
- To respect individuals' rights
- 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 voluntarily in the event of any breach of confidentiality.

2.4 Key Risks

To demonstrate Proviso Systems' understanding of the risks associated with GDPR non-compliances, some of the major key risks correlated with the control of personal data have been listed below.

- Personal data getting into the wrong hands, through poor security or inappropriate disclosure of information
- Individuals being harmed through data being inaccurate or insufficient
- Legal action being taken against the company. Legal action may result in fines and/or the tarnishing of the company's reputation and trustworthiness.

RESPONSIBILITIES:

3.1 The Board / Company Directors

The Company Director(s) have overall responsibility for ensuring that the organisation complies with its legal obligations.

3.2 Data Protection Officer

Data Protection Officer Chris Deakin – email: chris@proviso-systems.co.uk

The Data Protection Officer has the following responsibilities…

- Briefing the Board/ Company Director(s) on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on tricky Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification to the ICO
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

3.3 Employees & Volunteers

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers if applicable.)

SECURITY:

4.1 Scope

Proviso Systems will take necessary actions to ensure the protection of Personal Data. Reasonable actions will be taken to ensure that personal data is not sent, stored or obtained without positive consent from the data owner.

Security levels will be implemented for both soft and hard copies of data.

4.2 Setting Security Levels

Security levels will be set based on the implications of breach, likelihood of a potential breach, and the possible repercussions to the data owner and company if the data were to be unlawfully accessed or disposed.

4.3 Security Measures

Security measures for hard copy documents (these are stored in the main office within filing cabinets of folder systems).

- Office alarm/ security system
- Approved door locks and window locks
- Locking filing cabinets

Security measures for soft copy documents (these are stored on company computers, laptops or the network server).

- Office alarm/ security system
- Approved door locks and window locks
- Password protection
- Closed network
- Firewalls
- Anti-Virus and Anti-Spyware protection

Security measures for portable storage devices (these include USB sticks, laptops and company mobiles/ smartphones).

- Password protection
- Firewalls
- Anti-Virus and Anti-Spyware protection
- Individual (controller) protection and responsibility

4.4 Business Continuity

Proviso Systems ltd backs up data onto a physical hard drive which is stored with one of the company managers.

The backup storage device is not used or accessed away from the main office and would only be used in the case of office system failing.

4.5 Specific Risks

Portable devices are deemed to be a specific risk due to the difficulties in protecting a moving data storage system. Where possible data storage systems such as laptops, mobile phones ad memory sticks/drives will be kept with the employee responsible for the described item. Where available password (as well as key codes, patterns or biometrics) will be used on all devices.

Phishing emails, spyware and viruses have been deemed a specific risk because they can result in a data breach due to an employee's actions, i.e. unknowingly providing data to fraudulent individuals/ organisations. No data will be disposed without prior agreement from the data owner, this includes employee data. To protect against phishing employees will be sufficiently trained to ensure awareness, where doubt is placed on an email, website or software employees are encouraged to alert the companies data protection officer.

DATA RECORDING AND STORAGE:

5.1 Accuracy

All data provided by employees, customers, and suppliers will be checked to ensure all information held is accurate.
Individuals also have a right to access and amend all data related to the themselves, this will be actioned within 30 days maximum.

Accuracy of data taken over the phone is assured by repeating all personal information back to the provider; where applicable the NATO phonetic alphabet will be used to avoid errors. When taking email address from customers over the phone it is advised where possible to ask for the customer to email their details to us first. Alternatively, the customer should be given a time scale in which to expect contact, if contact is not received within the time scale given the customer should be advised to re-contact the company to double check the accuracy of the data taken.

If applicable, data provided by third party companies should be checked for accuracy with the related individual.

5.2 Updating

Proviso Systems Ltd will update personal information during the start of each new job.

To conform with the companies obligations, financial data will be stored for 6 years from the end of the last company financial year; these records may include customer information, which can be accessed by the data owners freely upon request.

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification in writing.

5.3 Storage

The storage of data is covered by Proviso Systems' "Data Map" managed by the companies data protection officer

5.4 Retention Periods

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Where repeat work is foreseeable, personal data will be retained to aid in future jobs and services.

At any point data processed can be accessed by the related individual/ organisation. It is also a right of the data owner to be forgotten where all the data stored relating to them will be destroyed.

5.5 Archiving

All hard copies of files are archived within the main office, archiving of files does not affect the ability to be amended or destroyed upon the request of the data owner.

RIGHT OF ACCESS:

6.1 Responsibility

It is the responsibility of the Data Protection Officer to ensure access is available within the specified 30 days from request.

All request to access, amend or destroy data should be processed through the Data Protection Officer.

6.2 Procedure for making request

Right of access requests must be made in writing, either emailed or written. A standard request form is not required, as long as the initial request is clear. Where requests are not fully clear Proviso Systems may ask for further clarifications.

All employees have a responsibility to pass on any request to the Data Protection Officer without delay.

6.3 Provision for verifying identity

Where any doubt is cast on the identity of an individual trying to access data Proviso Systems ltd will ask for further verification.

Verification of identity may include formal identification such as passport or drivers licence. Verification may also be achieved through several security questions outlined below.

- What is your full name
- What is the last 5 digits of your contact number
- What is the first line of your address and postcode

Where verification is insufficient, relevant details will be passed onto the directors for review.

6.4 Charging

Proviso Systems Ltd will not charge for any request to access, amend or destroy data.

If requests become excessive, unfounded or particularly repetitive a 'reasonable fee' can be charged to cover the cost of time spent, where applicable this will be outlined before anything is carried out.

6.5 Procedure for granting access

For all written (electronic or physical) requests to access data the following procedure will be carried out by the Data Protection Officer.

First, the requesters' identity will be verified as per section 6.3 of this document.

Once identity has been verified Proviso Systems will use the companies internal data map (controlled by the Data Protection Officer) to identify all the locations where related personal data is stored.

Once the data has been identified, it will be collected into a common folder. All hard copies will be photocopied at a high resolution and stored with the electronic files.

Once the data has been collected it should then be cross checked against the original data map to ensure the information is complete.

When the data is assured to be complete the electronic folder will be shared with the individual using a file sharing software (private access only)

TRANSPARENCY:

7.1 Commitment

Proviso Systems Ltd commits fully to ensure that data subjects are aware their data is being processed, this includes the following information.

- For which purpose the data is being processed
- What data will be retained and for what period
- How to exercise their rights in relation to their data

7.2 Procedure

The procedure in which customers are made aware of this data is through this document.

Proviso Systems' GDPR policy is available to all, during new or repeat work customers can access this document through the website or through any of our staff, this will be outlined on our email footers to provide details of how to access this document.

7.3 Responsibilities

It is the responsibility of all employees to be aware of the GDPR regulations. It is also the responsibility of all employees to pass any GDPR issues onto the Data Protection Officer

It is the responsibility of the Data Protection Officer to ensure all policies and procedures are carried out as per this document.

LAWFUL BASIS:

8.1 Underlying Principles

The underlying principles are as follows:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

8.2 Opting Out

Opting out is an option available for anyone

8.3 Withdrawing Consent

Proviso Systems acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

EMPLOYEE TRAINING & ACCEPTANCE OF RESPONSIBILITIES:

9.1 Introduction

All employees who have access to any kind of personal data will have their responsibilities outlined during their induction procedures. For any existing employees, sufficient training will be provided and any required obligations will be formally accepted.

9.2 Continuing Training

If required Data Protection issues may be discussed during further employee training, team meetings, supervisions or toolbox talks.

All employees have the right to request further training or assistance in regards to the GDPR regulations.

9.3 Procedure for Staff Signifying Acceptance of Policy

All employees will be required to signify their acceptance of this policy, this can be done using a signature or with a written agreement clearly identifying any relations to this policy.

POLICY REVIEW

10.1 Responsibility

The Data Protection Officer holds responsibility for any policy amendments and future reviews.

10.2 Procedure

During any policy amendment or review all relevant employees or customers will be notified.

10.3 Timing

The maximum review date for this policy is 3 years making the date of review to be no later than 16th May 2021