Strata Service Solutions Ltd

Document Control

Creator	Strata Compliance & Security Team
Owner	Strata Data Protection Officer
Subject	Data Protection Policy
Protective Marking	OFFICIAL
Version	1.0
Version Date	May 2018
Last update	Robin Barlow – Final with DP Act 2018
File location	\\strata.local\data\Strata\Docs\Security&Compliance\Policy\Data protection

Target audience
Strata

DATA PROTECTION POLICY

Policy Statement

Strata Service Solutions Limited is committed to protecting the rights and privacy of all people with regard to the processing of personal data. It is necessary for Strata to process information about employees, service users and other individuals it has dealings with for various purposes (e.g. to recruit and pay staff). The processing is conducted fairly and lawfully in accordance with the EU General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

For clarity, from this point 'GDPR/DPA' will refer to the combination of GDPR and the Data Protection Act 2018.

This Policy applies to all employees of Strata. Any breach of GDPR/DPA or Strata's Data Protection Policy may be considered to be a breach of the staff disciplinary procedures. As a matter of good practice, contractors, other agencies and individuals working with Strata, who have access to personal information, will be expected to read and comply with this Policy.

1 Introduction

1.1 The General Data Protection Regulations (GDPR) and the Data Protection Act 2018 came into force on the 25th May 2018 and widens the scope of the Data Protection Act 1998. The updated Data Protection Act 2018 provides UK law specifics of GDPR along with other directives and specialised processing, for example the Security Services. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent. Strata will always seek to comply with the Act.

1.2 Personal Data must be processed fairly and lawfully in accordance with the provisions of the GDPR/DPA

1.3 Personal Data may only be processed for notified purposes as stated within the GDPR/DPA.

1.4 Anyone with responsibility for holding or collecting data must ensure that data kept and processed about any data subject is accurate and up to date. All due skill and care must be taken. Data collected must not be excessive to Strata's need and superfluous data must be destroyed or removed from all systems.

1.5 Strata Managers are responsible for ensuring compliance with this policy within their areas. Each Manager shall ensure their staff are aware of and compliant with the provisions of GDPR/DPA.

2 Scope

The obligations contained in this Policy apply to employees, partners and contractors of Strata who collect, hold, process or deal with personal data for or on behalf of the company.

Definitions

2.1 Personal Data:

- The GDPR/DPA 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/DPA 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 – e.g. key-coded – can fall within the scope of the GDPR/DPA depending on how difficult it is to attribute the pseudonym to a particular individual.

2.2 Special category data: (previously similar to sensitive personal data)

- Special category data is more sensitive than normal personal data and a failure to protect and manage this data correctly could result in a greater risk to an individual, and therefore needs a higher degree of rigour when processing/storing it.

  The special categories specifically include:

Race	Ethnic origin
Politics	Religion
Trade union membership	Genetics
Biometrics (where used for ID purposes)	Health
Sex life	Sexual orientation

- Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10 of GDPR/DPA).

2.3 *Processing:* in relation to information or data, means obtaining, recording or holding the information or data or carrying out set operations on it, including disclosure.

2.4 *Data Subject:* an individual who is the subject of personal data.

2.5 *Data Protection Officer (DPO)*: an individual appointed who has a level of independence, authority and knowledge of data protection to:

- monitor internal compliance, inform and advise on your data protection obligations; provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority
- help you demonstrate compliance and are part of the enhanced focus on accountability

Where it is necessary to contact the Strata DPO, there is a specific email address **dpo@strata.solutions** that should be used.

2.6 *Mobile Devices:* laptop, tablet, USB stick, mobile phone, camera.

3 Policy

3.1 Strata is committed to maintaining the strictest level of confidentiality for any personal data it is responsible for processing. Personal data will only be processed or disclosed for purposes necessary for official business and that have been notified to the ICO Commissioner. To this end Strata will adhere to the principles outlined in GDPR/DPA for the processing of such data.

3.2 Systems, both computer and manual, will be designed to comply with the principles of the Data Protection Act. Staff involved in processing personal data will have knowledge of the principles and be trained accordingly. The six principles requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR/DPA in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures."

3.3 Strata carries out its affairs in an open manner. Apart from exceptional circumstances, as outlined in GDPR/DPA, information relating to a data subject will be made available to them, upon request, in an intelligible form.

3.4 Strata will endeavour to ensure that only the minimum data necessary to perform its business is held. The data will be erased or destroyed in such a manner that confidentiality is maintained. Every effort will be made to ensure that data is accurate and up to date, and that inaccuracies are corrected without unnecessary delay.

4 Security of Data

4.1 All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

4.2 All personal data should be accessible only to those who need to use it. You should always consider keeping personal data:

4.2.1 In a lockable room with controlled access, or
4.2.2 In a locked drawer or filing cabinet, or
4.2.3 If computerised, password protected, or kept on encrypted equipment.
4.2.4 Manual records should not be left where they can be accessed by unauthorised personnel

4.3 Strata staff must adhere to the Strata Security Policies, which provide guidance on the secure protection of data including passwords and the required handling precautions of data both stored and in transit.

4.4 Portable devices need additional consideration. Strata has a specific portable device policy. Sensitive information should not be routinely stored on mobile devices. Where sensitive data does need to be transported on a mobile device, the data should be removed immediately once it is no longer needed.

4.5 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant computers must be wiped clean before disposal.

5 Management of individual rights

5.1 Under GDPR/DPA there are various individual rights:

- Right to be informed

  Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under GDPR/DPA.

In Strata this is more likely to be a consideration in the development of IT systems, where both the principles of Data Protection by Design and Data Protection Impact Assessments (DPIA) must consider the collection of personal data, and where this is the case, identify the processes to inform those individuals of the use of the data.

Strata must regularly review, and where necessary, update your privacy information. Any new uses of an individual's personal data must be brought to their attention before starting the processing. This includes processing by previously undisclosed third parties.

Where data is obtained indirectly, privacy information must be provided within one month to the individuals.

- Right to access

  Individuals have the right to access their personal data. This is commonly referred to as subject access.

  Individuals can make a subject access request (SAR) verbally or in writing which must be *responded to within one month* of a request.

- Right to rectification

  Individuals have a right to have inaccurate personal data rectified, or completed if it is incomplete.

  Individuals can make a request for rectification verbally or in writing which must be *responded to within one month* of a request.

- Right to erasure (also known as right to be forgotten)

  Individuals have a right to have personal data erased, however this is not an absolute right and only applies in certain circumstances. Much of the data held by Strata is on behalf of the Data Controller Councils, and it is for them to respond and arrange any actions for this request.

  Individuals can make a request for erasure verbally or in writing which must be responded to within one month of a request.

- Right to restrict processing

  Individuals have the right to request the restriction or suppression of their personal data, however this is not an absolute right and only applies in certain circumstances. When processing is restricted, the data may still be stored.

  Individuals can make a request for restriction verbally or in writing which must be responded to within one month of a request.

- Right to data portability

  Individuals have a right to obtain and reuse their personal data for their own

purposes across different services, including moving, copying personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. The right only applies to information an individual has provided to a controller.

- Right to object

  Individuals have the right to object to the processing of their personal data in certain circumstances, in particular for direct marketing. Processing may continue where there is a compelling or lawful basis for this.

  Individuals can make an objection verbally or in writing which must be responded to within one month of a request.

- Rights related to automated decision making including profiling

  Individuals have the right to understand where automated decision-making with no human intervention is used where it has a legal or significant effect on them.

  In Strata this is more likely to be a consideration in the development of IT systems, where a Data Protection Impact Assessment must consider any program logic that may relate to this.

5.2 Strata will meet these rights, adopting processes where applicable for individuals to have these rights met.

5.3 Where any of these rights are for a Strata employee or an individual who has a direct relationship with Strata, this will be co-ordinated through the Strata Data Protection Officer (DPO).

5.4 Where these rights are for an employee, councillor, contractor or customer of the partner Councils then this right will be co-ordinated through the Council's own processes.

5.5 In the event that the partner Councils require assistance (a request) from Strata to deliver a right, then this will be co-ordinated through the Strata DPO. In no circumstances should any other employee of Strata directly undertake actions that are specifically to meet the Council GDPR/DPA requirements without gaining the consent of the Strata DPO.

5.6 Processes will be put in place to efficiently handle any such requests.

6 Agents, Partner Organisations and Contractors

If a contractor, partner organisation or agent is appointed or engaged to collect, hold, process or deal with personal data for or on behalf of Strata or if they will do so as part of the services they are providing to Strata, the Strata DPO must, as part of evaluation, be provided confirmation that the agent, partner organisation or contractor is able, willing and does comply with the GDPR/DPA and that an appropriate Data Protection Impact Assessment has been undertaken. There must be specific obligations in every such partnership agreement and contract requiring the partner/contractor to comply with the

GDPR/DPA.

7 Disclosure to and about Third Parties

Personal Data must not be disclosed about a Third Party except in accordance with the GDPR/DPA. If it appears absolutely necessary to disclose information about a Third Party to a person requesting data about themselves, advice must be sought from the Strata DPO.

8 Complaints

8.1 Any complaint or concern expressed by an individual in connection with the GDPR/DPA must be reported to the Strata Data Protection Officer immediately in case legal action is taken. The Data Protection Officer will work with the appropriate Strata Manager to ensure there has been no breach of the GDPR/DPA and, if there has, what action needs to be taken to remedy it, which will include a Personal Data Breach notification to the ICO, which must be lodged within 72 hours of the breach.

8.2 Where this complaint can be categorised under any of the eight specific GDPR/DPA individual rights these will be handled though these processes and be bound by any time and process stipulations for these.

9 Exemptions

There are a number of purposes which are exempt from certain provisions of the GDPR/DPA. If you are in doubt about which purposes are exempt and the scope of the exemption please contact the Strata Data Protection Officer.

10 Violations of Rules and Procedures

10.1 It is the responsibility of all employees to report any suspected breaches of the GDPR/DPA, or of this policy, to the Strata Data Protection Officer.

10.2 Failure to comply with this Policy by employees of Strata may result in disciplinary action being taken. Failure to comply by partners, agents or contractors may constitute a breach of their agreements.

10.3 A failure to comply may also open up the employee to criminal proceedings.