2024

SSIG

SPECIALITY SECURITY INVESTIGATION GROUP

DATA RETENTION POLICY

SSIG

SPECIALITY SECURITY INVESTIGATION GROUP

DATA RETENTION POLICY

Table of Contents

1.1. The corporate information, records, and data of Speciality Security Investigation Group Limited are integral to our business operations and employee management.

1.2. We are legally and regulatorily required to retain certain data for specified periods. Additionally, we keep data to ensure our business runs smoothly and to have relevant information when required. However, not all data needs to be kept indefinitely, and doing so can present risks and additional costs to the company.

1.3. This Data Retention Policy outlines the requirements for retaining and disposing of data, providing guidance on how to handle and dispose of data appropriately.

1.4. Non-compliance with this policy may result in fines, penalties, negative publicity, challenges in producing evidence when required, and difficulties in business operations.

1.5. This policy is not part of any employee's employment contract and may be modified at any time.

2. SCOPE OF POLICY

2.1. This policy applies to all data under our control, including physical records like hard copies, contracts, notebooks, letters, and invoices, as well as electronic records such as emails and digital documents. Both personal and non-personal data are covered, and we collectively refer to them as "data" in this policy.

2.2. This policy also applies to data held by third parties on our behalf, such as cloud storage providers or off-site record storage services. It also includes data owned by us but stored on employees' personal devices.

2.3. The policy distinguishes between formal or official records, disposable data, confidential information owned by third parties, personal data, and non-personal data, offering guidance on how we classify our data.

2.4. This policy is applicable across all departments and functions of Speciality Security Investigation Group Limited.

3. GUIDING PRINCIPLES

3.3 Through this policy and our data retention practices, we commit to the following:

- Complying with legal and regulatory requirements regarding data retention.
- Adhering to data protection obligations, particularly ensuring personal data is kept no longer than necessary for its intended purpose (storage limitation principle).
- Handling, storing, and disposing of data in a responsible and secure manner.

- Creating and retaining data essential for our business operations, while avoiding unnecessary data creation or retention.
- Allocating appropriate resources, roles, and responsibilities to manage data retention effectively.
- Regularly reminding employees of their data retention obligations.
- Monitoring and auditing compliance with this policy and updating it as required.

4. ROLES AND RESPONSIBILITIES

4.1. Responsibility of all employees: Compliance with the laws, regulations, and recognised best practices is essential. All employees must adhere to this policy, the Record Retention Schedule, any instructions related to data disposal, and directives from the Managing Director or Data Protection Officer. Non-compliance may result in serious civil or criminal liabilities. Employees may face disciplinary actions, including suspension or dismissal, for failing to comply.

4.2. The Managing Director has ultimate responsibility for the day-to-day management of the business.

4.3. The Data Protection Officer is responsible for identifying the data that must or should be retained and, in consultation with business leaders and external advisors, determining the appropriate retention periods.

4.4. The Data Protection Officer is also responsible for:

- Administering the data management programme.
- Assisting business leaders in implementing the programme and best practices.
- Where appropriate, overseeing the development and implementation of data disposal policies, systems, standards, and procedures.
- Providing guidance, training, and updates related to this policy.

4.5 The Data Protection Officer is the Finance Director.

5. TYPES OF DATA AND DATA CLASSIFICATIONS

1.1. **Formal or official records**: Certain data is deemed more significant and is listed in the Record Retention Schedule. This could be due to legal retention requirements, the need for

transaction evidence, or its importance to business operations. Refer to paragraph 6.1 for details on retention periods for this type of data.

1.2. **Disposable information**: This data may be deleted or discarded after serving its temporary purpose. It is not considered a formal or official record, as outlined in the Record Retention Schedule. Examples include:

- Duplicate copies of original documents that haven't been annotated.
- Drafts of letters, memoranda, reports, and informal notes that do not represent significant decisions.
- External publications like books, periodicals, and training materials retained for reference.
- Spam and junk mail.

For more information on retention periods for disposable information, see paragraph 6.2.

5.3 **Personal data**: Both formal records and disposable information may contain personal data, i.e., information identifying living individuals. Under data protection laws, we are required to keep personal data only as long as necessary for the processing purpose (storage limitation principle). See paragraph 6.2 for further details.

5.4 **Confidential information belonging to others**: Confidential information obtained from external sources, such as previous employers, must not be disclosed or used by us, as long as it remains confidential. Any unsolicited confidential information must be rejected, returned, or deleted.

5.5 **Data classifications**: The UK GDPR designates certain types of personal data as more sensitive, offering them additional protection, including:

- Personal data revealing racial or ethnic origin.
- Personal data revealing political opinions.
- Personal data revealing religious or philosophical beliefs.
- Personal data revealing trade union membership.
- Genetic data.
- Biometric data (when used for identification).

- Health data.

- Data about a person's sex life.
- Data about sexual orientation.

6. RETENTION PERIODS

6.1 **Formal or official records**: Data in the categories listed in the Record Retention Schedule must be retained for the duration specified. It should not be kept beyond this period unless there is a valid business reason, or a legal or special situation requires its retention.

6.2 **Disposable information**: The Record Retention Schedule does not specify retention periods for disposable information. This type of data should only be kept as long as needed for business purposes and securely disposed of once it is no longer necessary.

6.3 **Personal data**: As mentioned, personal data must only be retained for as long as is necessary for the purpose for which it was collected (storage limitation principle). When deciding whether to retain personal data, consider this principle.

6.4 **If data is not listed in the Record Retention Schedule**: Data not listed in the Record Retention Schedule is likely considered disposable. However, if you believe there is an omission or are uncertain, please consult the Data Protection Officer.

7. STORAGE, BACK-UP, AND DISPOSAL OF DATA

7.1. **Storage**: Data should be stored securely, ensuring it is accessible when needed. Essential documents and financial records must be backed up for emergency situations.

7.2. **Destruction**: The Data Protection Officer is responsible for overseeing the destruction of data that has reached the end of its retention period. Confidential documents, such as financial or employee records, should be shredded, while non-confidential data can be recycled. Destruction of electronic data should be coordinated with the Data Protection Officer.

7.3. Destruction must cease immediately if the Managing Director or Data Protection Officer informs that documents must be preserved due to potential litigation (litigation hold). Destruction may resume once the preservation requirement is lifted.

8. SPECIAL CIRCUMSTANCES

8.1. 8.1 **Preservation of documents for litigation and other situations**: If certain records are relevant to current or anticipated litigation, government investigation, audit, or other events, they must be preserved. This includes suspending the destruction schedule and maintaining the integrity of the records.

8.2. 8.2 If you believe this exception may apply or have questions about it, contact the Data Protection Officer.

8.3. 8.3 You may be asked to suspend routine data disposal for events such as mergers or the replacement of information technology systems.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

9.1. If you have questions about retention periods relevant to your role, please speak with your line manager. For other queries about this policy, contact the Data Protection Officer.

10. BREACH REPORTING AND AUDIT

10.1. **Reporting breaches**: We are committed to enforcing this policy. If you suspect a breach, report it immediately to your supervisor. If you are uncomfortable doing so, escalate it to their manager. Not reporting breaches may prevent corrective action.

10.2. We will not tolerate any form of retaliation or intimidation for reporting breaches, pursuing record destruction claims, or cooperating in investigations.

10.3. **Audits**: The Data Protection Officer, or external auditors, will periodically review this policy to ensure compliance with current laws, regulations, and guidelines. Audits will also be conducted to monitor ongoing compliance.

11. OTHER RELEVANT POLICIES

11.1. This policy complements our other policies and procedures and should be read alongside them.

ANNEX A – DEFINITIONS

- **Data**: All data under our control, including physical records like documents and electronic data such as emails and CCTV recordings, covering both personal and non-personal data.
- **Data Retention Policy**: This policy, which outlines our requirements for retaining and disposing of data.
- **Disposable information**: Data that can be discarded or deleted once it has served its temporary purpose.
- **Formal or official record**: Data deemed important, listed in the Record Retention Schedule, often for legal or operational reasons.
- **Non-personal data**: Data that does not identify living individuals.
- **Personal data**: Information identifying or relating to a living individual.
- **Data Protection Officer**: The individual responsible for determining which data must be retained and for how long.
- **Record Retention Schedule**: The schedule attached to this policy specifying retention periods for official records.
- **Storage limitation principle**: The principle requiring that personal data is kept only as long as necessary for its processing purpose.

ANNEX B - RECORD RETENTION SCHEDULE

Speciality Security Investigation Group Limited has established retention or destruction schedules for specific categories of data to ensure compliance with legal obligations, including data protection laws.