2024

SSIG

SPECIALITY SECURITY INVESTIGATION GROUP

Privacy Standard (UK GDPR version)

SSIG

SPECIALITY SECURITY INVESTIGATION GROUP

Privacy Standard (UK GDPR version)

Contents

1. Interpretation

1.1 **Definitions**:

Automated Decision-Making (ADM): A decision-making process solely based on Automated Processing (including profiling) that has legal consequences or significantly affects an individual. The UK GDPR prohibits ADM unless specific conditions are met, but Automated Processing itself is not prohibited.

Automated Processing: Any automated handling of Personal Data, which involves using Personal Data to evaluate specific personal aspects of an individual, especially to analyse or predict things like their work performance, economic status, health, preferences, interests, behaviour, reliability, or movements. Profiling is a form of Automated Processing.

Company Name: Speciality Security Investigation Group Limited (SSIG-UK)

Company Personnel: Includes all employees, workers, contractors, agency workers, consultants, directors, members, and others.

Consent: A clear, freely given, specific, informed agreement, represented by a statement or a clear positive action, indicating the Data Subject's agreement to the Processing of their Personal Data.

Controller: The individual or organisation that determines the purposes and means of processing Personal Data. They are responsible for ensuring practices and policies comply with the UK GDPR. We are the Controller of all Personal Data relating to Company Personnel and data used for business purposes.

Criminal Convictions Data: Personal data related to criminal convictions and offences, including information about criminal allegations and proceedings.

Data Subject: A living, identified, or identifiable individual whose Personal Data we hold. Data Subjects may be nationals or residents of any country and may have legal rights regarding their data.

Data Privacy Impact Assessment (DPIA): Tools and assessments used to identify and mitigate risks associated with data processing activities. DPIAs should be carried out for major system or business changes involving Personal Data.

Data Protection Officer (DPO): The individual responsible for overseeing data protection compliance under the UK GDPR. In cases where a mandatory DPO is not appointed, this term refers to the data protection manager or privacy team in charge of compliance.

EEA: The EU, including Iceland, Liechtenstein, and Norway.

Explicit Consent: Consent that requires a clear and specific statement (rather than implied actions).

UK General Data Protection Regulation (UK GDPR): The Data Protection Act 2018, which provides legal safeguards for Personal Data in the UK.

Personal Data: Any information identifying a Data Subject or information about them that allows them to be identified, either directly or indirectly, from that data alone or combined with other information we hold. This includes Special Categories of Personal Data and Pseudonymised Personal Data, but excludes anonymous data or data with the individual's identity permanently removed.

Personal Data Breach: Any event that compromises the security, confidentiality, integrity, or availability of Personal Data, including unauthorised access, loss, or disclosure of data.

Privacy by Design: The practice of implementing appropriate technical and organisational measures to ensure compliance with the UK GDPR from the outset.

Privacy Guidelines: Company guidelines related to privacy and the UK GDPR to assist in implementing and interpreting this Privacy Standard and Related Policies.

Privacy Notices (also known as Fair Processing Notices): Notices provided to Data Subjects when collecting information about them. These may be general privacy statements or specific to certain groups, such as employees or website users.

Processing or Process: Any activity involving Personal Data, including obtaining, recording, holding, amending, using, disclosing, or deleting it. Processing also includes transferring data to third parties.

Pseudonymisation or Pseudonymised: Replacing information that identifies an individual with pseudonyms or artificial identifiers, ensuring the individual cannot be identified without additional separate and secure information.

Related Policies: The Company's policies and procedures that support this Privacy Standard and are designed to protect Personal Data.

Special Categories of Personal Data: Information revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life or orientation, biometric or genetic data. The Company treats these as Special Categories of Personal Data.

2. Introduction

This Privacy Standard outlines how Speciality Security Investigation Group Limited ("we", "our", "us", "the Company") manages the Personal Data of our customers, suppliers, employees, workers, and other third parties.

This Privacy Standard applies to all Personal Data we process, regardless of the medium in which it is stored, and whether it relates to current or past employees, workers, clients, customers, suppliers, shareholders, website users, or any other Data Subject.

It applies to all Company Personnel ("you", "your"). You must read, understand, and comply with this Privacy Standard when Processing Personal Data on behalf of the Company and attend relevant training. This Privacy Standard outlines our expectations for ensuring the Company's compliance with applicable laws. Compliance is mandatory. Related Policies and Privacy Guidelines are available to assist in interpreting and implementing this Privacy Standard. You must also adhere to these policies and guidelines. Any breach may result in disciplinary action.

If you have a specific responsibility regarding Personal Data Processing, such as obtaining Consent, reporting a Personal Data Breach, conducting a DPIA, or any other related tasks, you must follow the applicable policies and guidelines.

This Privacy Standard, along with Related Policies and Privacy Guidelines, is an internal document and cannot be shared with third parties, clients, or regulators without prior authorisation from the Data Protection Officer.

3. Scope

We recognise that correct and lawful treatment of Personal Data builds trust and supports successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility, and we take this seriously. Non-compliance with UK GDPR could expose the Company to fines of up to £17.5 million or 4% of total worldwide turnover from the previous financial year, whichever is higher.

All directors and employees are responsible for ensuring compliance with this Privacy Standard and must implement appropriate practices, processes, controls, and training to ensure adherence. The Data Protection Officer oversees this Privacy Standard and is responsible for developing related policies and guidelines.

Please contact the Data Protection Officer with any questions about this Privacy Standard, the UK GDPR, or if you believe the standard is not being followed. Specifically, you should contact the DPO in the following circumstances: (a) If you are unsure about the lawful basis for processing Personal Data (including legitimate interests) (see paragraph 5.1); (b) If you need to capture Explicit Consent (see paragraph 6); (c) If you are drafting Privacy Notices (see paragraph 7); (d) If you are unclear about retention periods for Personal Data (see paragraph 11); (e) If you need help with security measures to protect Personal Data (see paragraph 12.1); (f) If a Personal Data Breach occurs (paragraph 13); (g) If transferring Personal Data outside the UK (see paragraph 14); (h) If you need assistance with Data Subject rights (see paragraph 15); (i) If you are undertaking significant new Processing activities requiring a DPIA (see paragraph 19); (j) If engaging in Automated Processing, profiling, or ADM (see paragraph 20); (k) If carrying out direct marketing activities (see paragraph 21); (l) If sharing Personal Data with third parties (see paragraph 22).

4. Personal Data Protection Principles

We follow the principles of Personal Data Processing set out in the UK GDPR, which state that Personal Data must be:

(a) Processed lawfully, fairly, and transparently (Lawfulness, Fairness, and Transparency);

(b) Collected for specified, explicit, and legitimate purposes (Purpose Limitation);

(c) Adequate, relevant, and limited to what is necessary (Data Minimisation);

(d) Accurate and, where necessary, kept up to date (Accuracy);

(e) Not kept for longer than necessary (Storage Limitation);

(f) Processed with appropriate technical and organisational measures to protect security (Security, Integrity, and Confidentiality);

(g) Not transferred without safeguards (Transfer Limitation);

(h) Made accessible to Data Subjects to exercise their rights (Data Subject's Rights and Requests).

We are responsible for demonstrating compliance with these principles (Accountability).

5. Lawfulness, Fairness, Transparency

5.1 Lawfulness and Fairness

Personal Data must be processed lawfully, fairly, and transparently in relation to the Data Subject. You may only collect, process, and share Personal Data for specified, lawful purposes, as set out in Article 6 of the UK GDPR. The lawful bases for processing Personal Data include:

(a) **Consent**: The individual has clearly consented to processing for a specific purpose.

(b) **Contract**: Processing is necessary for a contract with the individual.

(c) **Legal obligation**: Processing is necessary to comply with the law (excluding contractual obligations).

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

(e) **Public task**: Processing is necessary for tasks in the public interest or for official functions.

(f) **Legitimate interests**: Processing is necessary for legitimate interests, unless overridden by the Data Subject's rights.

You must document the lawful basis for each processing activity.

6. Consent

A Data Controller may only process Personal Data based on lawful grounds, including Consent. Consent requires a clear affirmative statement or action from the Data Subject, and it must be separate from other matters.

You must ensure that Consent is easily withdrawable and promptly honoured. If you plan to process Personal Data for purposes other than those initially disclosed, Consent must be refreshed.
For Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis other than Consent, but if explicit Consent is required, a Privacy Notice must be provided.
You must document and maintain records of all Consents in line with Related Policies.

7. Transparency (Notifying Data Subjects)

The UK GDPR requires Controllers to provide Data Subjects with specific information, either when Personal Data is collected directly or indirectly. This information must be clear, concise, and accessible, presented in plain language.

You must provide a Privacy Notice whenever collecting Personal Data directly or indirectly, and ensure it complies with the UK GDPR and our Related Policies.

8. Purpose Limitation

Personal Data should only be collected for clear, legitimate, and specific purposes. It must not be processed in ways that are inconsistent with these original purposes.
Personal Data cannot be used for new, different, or incompatible purposes from those initially disclosed at the time of collection unless the Data Subject has been informed of the new purposes and has provided Consent, where required.

9. Data Minimisation

Personal Data must be sufficient, relevant, and limited to what is necessary for the purposes for which it is processed.

You may only process Personal Data when it is necessary for the performance of your job duties.
Personal Data cannot be processed for any reasons unrelated to your work responsibilities.
Only collect Personal Data that is necessary for your job duties; do not gather excessive information.
Ensure that any Personal Data collected is both adequate and relevant for the intended purposes.
You must ensure that when Personal Data is no longer required for the specified purposes, it is deleted or anonymised in line with the Company's data retention policies.

10. Accuracy

Personal Data must be accurate and, where required, kept up to date. Any inaccuracies must be corrected or deleted promptly.

You must ensure that the Personal Data we use and store is accurate, complete, current, and relevant to the purpose for which it was collected. You are responsible for verifying the accuracy of Personal Data at the time of collection and periodically thereafter. You must take all reasonable measures to either delete or correct inaccurate or outdated Personal Data.

11. Storage Limitation

Personal Data must not be retained in an identifiable form for longer than is necessary to fulfil the purposes for which the data was processed.

The Company will implement retention policies and procedures to ensure that Personal Data is deleted after a reasonable period, unless a legal obligation requires the data to be retained for a specified duration.
You must not retain Personal Data in a way that allows the identification of the Data Subject for longer than is necessary for the legitimate business purposes for which it was initially collected, including for any legal, accounting, or reporting obligations.

You are required to take all reasonable measures to destroy or remove from our systems any Personal Data that is no longer needed, in line with the Company's relevant records retention schedules and policies. This includes instructing third parties to delete such data where applicable.
You must ensure that Data Subjects are informed about the retention period of their data and the criteria used to determine that period in any relevant Privacy Notice.

12. Security, Integrity, and Confidentiality

12.1 Protecting Personal Data

Personal Data must be protected by suitable technical and organisational measures to prevent unauthorised or unlawful processing, as well as to safeguard against accidental loss, destruction, or damage.

We will develop, implement, and maintain appropriate safeguards that reflect our size, scope, business nature, available resources, the volume of Personal Data we control or manage on behalf of others, and identified risks (including the use of encryption and pseudonymisation where applicable). We will regularly assess and test the effectiveness of these safeguards to ensure the security of our Personal Data processing.

You are responsible for safeguarding the Personal Data we hold. You must take reasonable and appropriate security precautions to protect against unlawful or unauthorised processing and to prevent accidental loss or damage to Personal Data. Special care should be taken to protect Special Categories of Personal Data and Criminal Convictions Data from loss, unauthorised access, use, or disclosure.
You must follow all the procedures and technologies we implement to secure Personal Data from the point of collection to its eventual destruction. You may only transfer Personal Data to third-party service providers who commit to complying with the relevant policies and procedures and agree to put in place the necessary protective measures.

You are required to uphold data security by ensuring the confidentiality, integrity, and availability of Personal Data, which are defined as follows: (a) Confidentiality means that only individuals who have a legitimate need to know and are authorised to access Personal Data are able to do so; (b) Integrity means that Personal Data remains accurate and suitable for the purpose for which it is being processed; and (c) Availability means that authorised users can access the Personal Data when needed for legitimate purposes.

You must adhere to, and not attempt to bypass, the administrative, physical, and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

13. Reporting a Personal Data Breach

The UK GDPR requires Controllers to inform the relevant regulator of any Personal Data Breach and, in certain cases, notify the Data Subject.

We have established procedures to address any suspected Personal Data Breach and will notify Data Subjects or the relevant regulator when legally required to do so.
If you become aware of or suspect a Personal Data Breach has occurred, do not attempt to investigate the issue on your own. Immediately contact the designated person or team responsible for handling Personal Data Breaches. You should also ensure that all evidence related to the potential breach is preserved.

14. Transfer Limitation

The UK GDPR primarily applies to controllers and processors based in the United Kingdom, with certain exceptions.
Individuals may lose the protection offered by the UK GDPR if their personal data is transferred outside the UK.

As such, the UK GDPR imposes restrictions on the transfer of personal data outside the UK, or beyond the protection of the UK GDPR, unless the rights of individuals concerning their personal data are safeguarded in another way, or if one of the limited exceptions applies.

A transfer of personal data outside the scope of the UK GDPR (referred to as a ‘restricted transfer’) typically involves sending data from the UK to another country.

You may make a restricted transfer if the recipient is located in a third country or territory, or is an international organisation, that is covered by UK "adequacy regulations". These regulations define that the legal framework in the recipient country, territory, sector, or international organisation has been assessed as providing 'adequate' protection for individuals’ rights and freedoms regarding their personal data.

Provisional arrangements ensure that UK "adequacy regulations" apply to the EEA and all countries, territories, and international organisations covered by European Commission "adequacy decisions" as of 31 December 2020.

If there are no UK ‘adequacy regulations’ in place for the country, territory, or sector involved in your restricted transfer, you should then explore whether the transfer can proceed under 'appropriate safeguards'.

The UK GDPR outlines a list of appropriate safeguards, each of which ensures that both you and the recipient of the restricted transfer are legally obligated to protect individuals’ rights and freedoms in relation to their personal data.

15. Data Subject's Rights and Requests

Data Subjects have specific rights regarding the handling of their Personal Data. These include the rights to:

(a) withdraw Consent for Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to the Personal Data we hold about them;

(d) opt out of the use of their Personal Data for direct marketing purposes;

(e) request the erasure of their Personal Data if it is no longer necessary for the purposes for which it was collected or processed, or to correct inaccurate or incomplete data;

(f) restrict Processing under certain circumstances;

(g) challenge Processing based on our legitimate interests or public interest;

(h) request a copy of an agreement relating to the transfer of their Personal Data outside of the UK;

(i) object to decisions made solely through Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause harm or distress to the Data Subject or others;

(k) be notified of a Personal Data Breach that is likely to pose a high risk to their rights and freedoms;

(l) lodge a complaint with the supervisory authority;

(m) in limited circumstances, request that their Personal Data be transferred to a third party in a structured, commonly used, and machine-readable format.

You must confirm the identity of any individual making a request under the rights listed above (do not disclose Personal Data to third parties without proper authorisation).

Any Data Subject request you receive must be immediately forwarded to your supervisor.

16. Accountability

The Controller must implement appropriate technical and organisational measures effectively to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, adherence to these principles.

The Company must allocate adequate resources and establish controls to ensure and document compliance with the UK GDPR, which includes:

(a) appointing a suitably qualified Data Protection Officer (DPO) where necessary, as well as an executive who holds responsibility for data privacy;

(b) applying Privacy by Design when processing Personal Data and conducting Data Protection Impact Assessments (DPIAs) where the processing may present a high risk to the rights and freedoms of Data Subjects;

(c) integrating data protection into internal documentation, such as this Privacy Standard, Related Policies, Privacy Guidelines, and Privacy Notices;

(d) providing ongoing training for Company Personnel on the UK GDPR, this Privacy Standard, Related Policies, and Privacy Guidelines, as well as data protection topics including Data Subject rights, Consent, legal bases, DPIAs, and Personal Data Breaches. The Company must maintain records of training attendance; and

(e) regularly testing the implemented privacy measures and conducting periodic reviews and audits to assess compliance, using the results from testing to demonstrate continuous efforts to improve compliance.

17. Record Keeping

The UK GDPR mandates that we maintain comprehensive and accurate records of all our data processing activities.

You must ensure that accurate corporate records are kept, reflecting our processing activities, including records of Data Subjects' consents and the procedures for obtaining such consents, in line with the Company’s record-keeping guidelines.

At a minimum, these records should include the name and contact details of the Controller and the DPO, clear descriptions of the types of Personal Data, Data Subject categories, processing activities, processing purposes, third-party recipients of the Personal Data, storage locations of the Personal Data, any Personal Data transfers, the retention period for the Personal Data, and details of the security measures in place. To create these records, data maps should be developed, containing the information outlined above, along with appropriate data flow details.

18. Training and Audit

We are obligated to ensure that all Company Personnel receive sufficient training to enable them to comply with data privacy laws.

You must complete all mandatory data privacy training and ensure that your team also undertakes the same compulsory training.

You must regularly assess all the systems and processes under your management to ensure they align with this Privacy Standard. Additionally, you must verify that appropriate governance controls and resources are in place to ensure the proper use and protection of Personal Data.

19. Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to incorporate Privacy by Design principles when processing Personal Data by implementing appropriate technical and organisational measures (such as Pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

You must evaluate which Privacy by Design measures can be applied to all programmes, systems, or processes that involve processing Personal Data, considering the following factors:

- the state of the art;
- the cost of implementation;
- the nature, scope, context, and purposes of the processing; and

- the potential risks, in terms of both likelihood and severity, to the rights and freedoms of Data Subjects posed by the processing.

Data controllers must also carry out Data Protection Impact Assessments (DPIAs) for high-risk processing activities.

A DPIA should be conducted (and the findings discussed with the Data Protection Officer) when implementing significant system or business changes involving Personal Data processing, including:

- the introduction of new technologies (systems, programs, or processes), or changes to existing technologies;
- Automated Processing, including profiling and Automated Decision-Making (ADM);
- large-scale processing of Special Categories of Personal Data or Criminal Convictions Data; and
- large-scale, systematic monitoring of publicly accessible areas.

A DPIA must include:

- a description of the processing, its purposes, and the Data Controller's legitimate interests, if applicable;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an evaluation of the risks to individuals; and
- the risk mitigation measures in place and a demonstration of compliance.

20. Automated Processing (Including Profiling) and Automated Decision-Making

In general, Automated Decision-Making (ADM) is prohibited when it has a legal or similarly significant effect on an individual, unless:

(a) the Data Subject has explicitly consented;

(b) the processing is authorised by law; or

(c) the processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, grounds (b) or (c) will not be applicable. However, these types of data can be processed when it is necessary (unless less intrusive alternatives are available) for substantial public interests, such as fraud prevention.

If a decision is to be made solely based on Automated Processing (including profiling), Data Subjects must be informed of their right to object at the time of the initial communication. This right must be clearly highlighted and presented separately from other information. Furthermore, appropriate measures must be implemented to protect the Data Subject's rights, freedoms, and legitimate interests.

We must also inform the Data Subject about the logic involved in the decision-making or profiling process, the significance, and the expected consequences, as well as provide them with the right to request human intervention, express their views, or challenge the decision.

A Data Protection Impact Assessment (DPIA) must be completed before initiating any Automated Processing (including profiling) or ADM activities.

21. Sharing Personal Data

As a general rule, we are not permitted to share Personal Data with third parties unless appropriate safeguards and contractual agreements have been established.

You may only share the Personal Data we hold with another employee, agent, or representative within our group (including subsidiaries, our ultimate holding company, and its subsidiaries) if the recipient requires the information for work-related purposes and the transfer complies with any relevant cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a legitimate need to know the information in order to provide the contracted services;

(b) sharing the Personal Data aligns with the Privacy Notice given to the Data Subject, and if necessary, the Data Subject's Consent has been obtained;

(c) the third party has agreed to adhere to the required data security standards, policies, and procedures, and has implemented adequate security measures;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract containing GDPR-compliant third-party clauses is in place.

22. Updates to this Privacy Standard

We regularly review this Privacy Standard. This Privacy Standard does not supersede any relevant national data privacy laws and regulations in the countries where the Company operates.