GDPR Data Protection Policy

1. Introduction

Our Company GDPR Data Protection Policy refers to our commitment to treat and protect personal data of our employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights in accordance with all applicable laws and regulations:

- Directive EC/95/46/EC Data Protection
- Directive 2002/58/EC Privacy and Electronic Communications
- General Data Protection Regulation
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (UK)

This policy outlines the expected behaviour that Secom Plc Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Secom Plc for example data subject.

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data.

An organisation that handles personal data and makes decisions about its use is known as a data controller.

As a data controller, Secom Plc is responsible for ensuring compliance with data protection guidelines outlined in this policy and non-compliance may expose the business to complaints, regulatory action, fines and/or reputational damage.

2. Scope

Secom Plc employees and subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

This policy extends to all processing of personal data in electronic form or where the data is held in manual files that are structured in a way that allows ready access to information about the individual.

However, if Employees receive any personal data to their work email address this lies outside Secom Plc policy.

3. Definitions

Data Protection Principles	The fundamental rule that all who process personal data must take into consideration the right of that individual to the privacy of his or her communications.
Data Subject	The identified or identifiable natural person to which the data refers.
Process, Processed, Processing data	Any operation or set of operations performed on personal data. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection	The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.
Data Protection Authority	An independent public authority responsible for monitoring the application of the relevant data protection regulation set forth in national law.
Data Processors	A natural or legal person public authority, agency or other body which processes personal data on behalf of a data controller.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Special Categories of Data	Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data
Employees:	An individual who works part-time or full-time for Secom Plc under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
Personal Data	Any information (including opinions and intentions) which relates to an identified or identifiable natural person.
Contact	Any past, present or prospective employee, supplier, subcontractor or customer
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, by reference to an identifier such as a name an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
Encryption	The process of converting information or data into code, to prevent unauthorised access.

4. GDPR Data Protection Principles

Secom Plc has adopted the 8 GDPR data protection principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Fair & Lawful	Personal data shall be processed fairly and lawfully and shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
Principle 2: Purpose	Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
Principle 3: Adequacy	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Principle 4: Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Principle 5: Retention	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
Principle 6: Rights	Personal data shall be processed in accordance with the rights of data subjects under this Act
Principle 7: Security	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Principle 8: International	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. Policy

As part of Secom Plc operations, it is important that we obtain and process information accurately and securely. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Secom Plc ensures that information collected is carried out in a transparent way and only with the full cooperation and knowledge of interested parties. To comply with ICO Data Protection Principles the following rules apply;

- We only collect and use the personal data based on legitimate grounds
- Secom Plc will not use the data in ways that may have adverse effects on the individual concerned
- Secom Plc collects their information in a transparent way and only with the full cooperation and knowledge of interested parties by providing appropriate privacy notices at the time when we are collecting personal data
- Secom Plc will handle all personal data within its legal and moral boundaries
- Ensure controls around protecting personal data against any unauthorized or illegal access by internal or external parties are implemented

It is our responsibility and duty to ensure that data is not:

- 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

Secom Plc are committed to:

- Ensure firm controls are put in place to restrict and monitor access to sensitive data
- Implement robust procedures in line with data protection requirements
- Provide sufficient training for all Secom Plc employees around 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.)
- Ensure clear and transparent communication between us and the individuals is constant by including all data protection provisions on our website.
- Password protection also extends to confidential documents being sent from, and to, SECOM PLC.
- Wherever possible, electronic documents in a lockable format such as Microsoft Office, Adobe PDF and WinZip should be encrypted with a password which is sent separately to the underlying document.
- Hard copy documents should be, where possible, faxed and not posted.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. It is our responsibility to ensure that Secom Plc

- Reviews the length of time you keep personal data;
- Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date.

In certain circumstances, it is permitted that personal data can be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by any rule of law

Where a data subject receives a request from a court or any regulatory or law enforcement authority for information relating to you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

6. Subject Access Request

You have the right to ask for a copy of any of your personal data held by Secom Plc as a Subject Access Request (SAR's). All requests must be in writing and addressed to the 'Data Controller', the request may include but not limited to;

- Copies of emails and letters
- Statements, references
- CCTV footage
- Call recordings
- DBS / Credit Report

Secom Plc will aim to acknowledge any Subject Access Request within 48hrs of receipt and complete the process within 40 days. In some cases, processing SAR's may take longer, and it is Secom Plc duty to keep you informed.

This is non-chargeable request; however, Secom Plc has the right to charge a 'reasonable fee' when a request is manifestly unfounded, excessive or particularly repetitive.

7. 'Right to be Forgotten'

Secom Plc employees shall have the right to obtain from the Data Protection Controller to delete personal data concerning them without undue delay.

It is the controller's obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the individual withdraws consent on which the processing is based according to **Article 6 GDPR** (1) or **Article 9 GDPR (2)**, and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to **Article 21 GDPR** (1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to **Article 21 GDPR (2)**
- the personal data have been unlawfully processed;
- the personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in **Article 8 GDPR (1)**

Where the controller has made the personal data public and is obliged pursuant to section 7 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform relevant data controllers which are processing the personal data that the individual has requested for deletion

Section 7 and 8 shall not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by a Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest around public health in accordance with points (h) and (i) of **Article 9 GDPR (2) and (3);**
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with **Article 89 GDPR (1)** in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

8. Complaints Handling

Complaints regarding the conduct of processing personal data by Secom Plc or Suppliers/Subcontractors should be in writing and forwarded to the Data Protection Officer.

An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, the Data Subject has the option to escalate the complaint further to the Information Commissioner Office (ICO).

9. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to theft or exposure must immediately notify the Data Protection Officer or Senior/Line Manager providing the description of the incident.

Notification of the incident must be made by email, calling or by using the incident reporting form which is available on the company intranet and forwarded to the Data Protection Officer who will investigate and decide whether personal data had been breach.

Where a breach is identified the Data Protection Officer has 72 hours to notify the Information Commissioner Officer (ICO).

10. Data Protection Training

All Secom Plc employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, regular data protection training and procedural guidance will be provided.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- Understanding the General Data Protection Principles.
- Establishing when to use and permit the use of personal data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security controls and other access mechanisms.
- The importance of limiting access to personal data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, print outs and electronic storage media
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of personal data outside of the internal network and physical office premises.
- Proper disposal of personal data by using secure shredding facilities.
- Any special risks associated with departmental activities or duties.

11. Disciplinary/ Legal Action

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

12. Compliance Monitoring

Adequate level of compliance that is being achieved by all Secom Plc, the Data Protection Officer will carry out an annual audit. At a minimum the audit will comprise of the following:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities.
  - Raising awareness
  - Training of Employees

- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights
  - Personal Data transfers
  - Personal Data incident management
  - Personal Data complaints handling

- The level of understanding of data protection policies and privacy notices.
- The accuracy of personal data being stored
- The adequacy of procedures for redressing poor compliance and personal data breaches.

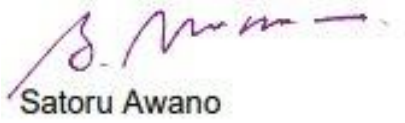
13. Related Documents and Policies

Listed below are documents that relate to this policy.

- Privacy Policy
- Privacy Policy – Staff Data
- Information Security Policy
- Whistle Blowing Policy
- DPA Breach Reporting Procedure
- Subject Access Request & Right to be Forgotten Procedure

14. Review

Formal review of this Policy will occur once a year unless deemed necessary by changes in legislation and / or need due to improved practices.



Satoru Awano

Managing Director- SECOM PLC. Revised May 2023

Version No	Amendments	By Whom	Date
3	**Update with New MD Signature**	D Jones	May 2023