Paramount Security Solutions Data Protection Policy

1. Introduction

This Data Protection Policy sets out the company's commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data. Paramount Security Solutions needs to gather and use personal data about individuals. This can include customers, suppliers, business contacts, and employees.

Paramount Security Solutions has an appointed Data Protection Lead. Their role is to inform and advise the company on its data protection obligations. They can be contacted at ed.githaiga@paramountsecsolutions.com and help answer questions about this policy or offer data protection guidance.

2. Definitions

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer various kinds of personal data about you which we have grouped together as follows:

- Identity Data includes name, contact details, address, username or similar identifier, marital status, title, date of birth, National Insurance number and gender.
- Financial Data includes bank account details.
- Transaction Data includes details about payments made to you.
- Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- Usage Data includes information about how you use our website, products and services.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.
- Special Categories of Personal Data includes information about your health (To provide suitable adjustments) and criminal convictions and offences (For safeguarding purposes).

3. Data Protection Principles

1. Personal data shall be processed fairly and lawfully and in a transparent manner.
2. Personal data shall be collected for a specified, explicit and legitimate purpose.
3. The company processes personal data only where it is adequate, relevant and limited to what is necessary for processing.
4. The company keeps accurate personal data and takes all reasonable steps to ensure inaccurate personal data is rectified or deleted without delay.
5. The company retains personal data only for the period necessary for processing. **6.** The company adopts appropriate measures to make sure personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
7. The company shall be responsible for and be able to demonstrate compliance with these principles.

Where the company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the UK General Data Protection Regulation (UK GDPR).

Paramount Security will update personal data promptly if an individual advises their information has changed or is inaccurate and personal data is held in:

- The individuals personal file
- People and Payroll systems, Client Management Systems, Finance Systems, Time Management systems, and other systems that the businesses uses in their service delivery activities.
- On any written contractual document, or other correspondence, as necessary.

4. Lawful Basis for Processing

Processing personal data shall be lawful only if at least one of the following applies:

- The individual has given consent to the processing of their personal data for one or more specified purposes.
- Processing is necessary for the performance of a contract to which the individual is party or to take steps at the request of the individual prior to entering into a contract. Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary to protect the vital interests of the individual or another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
- Processing is necessary for legitimate interests pursued by the data controller or by a third party.

5. Individual Rights

Under data protection law, you have rights including:

- Your right to be informed – You have the right to be informed about the collection and use of your personal data.
- Your right to rectification - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete.
- Your right to erasure - You have the right to ask us to delete your personal information.
- Your right to restriction of processing - You have the right to ask us to limit how we can use your personal information.
- Your right to object to processing - You have the right to object to the processing of your personal data.
- Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you.
- Your right to withdraw consent – When we use consent as our lawful basis, you can withdraw your consent at any time.

To enquire about these options or to ask the company to take any of these steps, the individual should send the request to ed.githaiga@paramountsecsolutions.com

We will normally respond to a request within one month of the date it is received. In some cases, such as where the company processes substantial amounts of the individual's data, we may require extra time to consider and process the request. If this is the case, we will write to the individual within one month of receiving the original request to tell them if this is the case and confirm that the request may take up to an extra two months to respond.

If a subject access request is manifestly unfounded or excessive, the company is not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the company has already responded. If an individual submits a request which is unfounded or excessive, the company will notify them this is the case and whether it will respond to it.

6. Freedom of Information

The company is subject to The Freedom of Information Act 2000 (FOI), and all requests for information which is not personal information must be treated as a FOI or EIR. These requests must be fully responded to within 20 (company) working days by law. The information will be provided unless the company can provide an exemption or exception under the FOI act.

7. Data Breaches

A personal data breach can be broadly defined as a security incident which has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever personal data is lost, destroyed, corrupted or disclosed, or if someone has access without proper authorisation.

If there is an alleged data breach you must notify our DPO immediately at ed.githaiga@paramountsecsolutions.com.

Examples of a data breach are:

- Access by an unauthorised individual or third party
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission.

If Paramount Security discovers there has been a breach of personal data which poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of becoming aware of the breach. The company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the company will inform affected individuals without undue delay there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

8. Individual Responsibilities

Individuals are responsible for helping Paramount Security keep their personal data up to date. Individuals should let the company know if the data provided to the company changes.

9. Complaints

If you believe Paramount Security has not complied with your data protection rights, you make a complaint to the Information Commissioner although we would appreciate a chance to address your concerns.

Report a concern:

• Online at https://ico.org.uk/concerns/
• Call 0303 123 1113

• Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

All complaints will be processed in accordance with the Company's Complaints Process and should be sent to: ed.githaiga@paramountsecsolutions.com

GDPR Appendix

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new candidate	Identity- Contact, Profile, Personal data	For job seeking purposes/ Maintaining your record on our databases/Necessary to comply with a legal obligation
To process payments to you	Identity- Contact / Financial / Transaction	To ensure payments are made for work undertaken/Necessary to comply with a legal obligation
To manage our relationship with you which includes; Notifying you about changes to our terms or privacy policy Asking you to leave a review or take a survey	Identity- Contact, Profile / Marketing and Communications	Performance of a contract with you/Necessary to comply with a legal obligation/Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To enable you to partake in a prize draw, competition or complete a survey	Identity- Contact / Profile / Usage / Marketing and Communications	Performance of a contract with you/Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	Identity- Contact / Technical	Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation / Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	Identity- Contact / Profile / Usage / Marketing and Communications / Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	Technical / Usage	Legitimate interests (to define types of customers, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services which may be of interest to you	Identity- Contact / Technical / Usage / Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)
To prevent fraud	Identity- Contact / Financial	Legal Obligation
To deter and to be able to report on crimes or potential crimes in and around our premises	Identity- CCTV, Photographs (This may be in some cases processed by third parties)	Vital Interests

Ed Githaiga

Managing Director

May 25th 2026