Paramount Security Solutions Privacy Policy

1. Introduction

Paramount Security Solutions is committed to protecting the privacy and security of your information. This privacy policy describes how we collect and use personal information about you in accordance with UK Data Protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and section 8 of the Data Protection Act 2018.

We are required under data protection legislation to notify you of the information contained in this privacy policy.

2. Who We Are

Under Data Protection legislation, Paramount Security Solutions is a Data Processor for its clients.

The company contact details are as follows:

Website: https://www.paramountsecsolutions.com/
Email: ed.githaiga@paramountsecsolutions.com.
Tel: 01206 266789

3. Data Protection Lead

The company's data protection lead is: Ed Githaiga.

Email: ed.githaiga@paramountsecsolutions.com

4. Information We May Collect And Hold

The company collects and processes a range of information to support the functions of all business activity.

This includes:

- Information provided by filling in forms on https://www.paramountsecsolutions.com. This includes information provided at the time of registering to use this website, posting material or requesting further services. We may also ask you for information when you report a problem with this Website.

- If you contact us for any business reason, we may keep a record of your personal details you provide and any correspondence.
- If you engage in business activity, we will hold personal information relevant to the contract, such as Emergency Contact information for Keyholding Services.
- We may also use your details to complete client or employee satisfaction surveys which is used for continuous improvement purposes, although you do not have to respond to the survey.
- In some cases, we may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, financial regulated authorities and credit checks, information from criminal records checks permitted by law.

5. Criminal Offence Data

For the purposes of compliance with our Safeguarding Policy, we may ask for DBS checks or seek criminal records information in certain circumstances (we will always notify you beforehand if we require this information).This type of data is regulated under the UK GDPR and we ensure that we limit the use of any such data both in time and in scope and that we meet appropriate lawful grounds for processing such data.

6. Storage of Personal Data

Information you provide to us is stored on a secure cloud server. Data can be stored in a range of different locations on our server, including customer folders and our email folders.

The company has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused, or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the company engages third parties to process personal data on its behalf, they do so based on written instructions from our client, are under a duty of confidentiality and are obliged to implement appropriate technical and organizational measures to ensure the security of data.

Where we have given you (or where you have chosen) a password which enables you to access our systems, you are responsible for keeping this password confidential.

Once we are in receipt of your data, we will use strict procedures and security features to prevent unauthorised access.

Your information may also be stored in a third-party server, such as our Partner™ patrol verification system, on those occasions where it is necessary for the completion of our service contract with you.

7. Why We Collect and Use This Information

- To provide you with information, products, or services that you request from us or which we may feel may interest you, where you have consented to be contacted for such purposes.
- To manager our client relationship and carry out our obligations arising from any contracts entered between you and us.
- To notify you about changes to our services.
- To perform credit checks and issue invoices for services you contract into.
- To carry out client satisfaction audits, manager site visits and other company audits.

The company needs to process data to enter a contract with you and to meet its obligations under the contract. In some cases, the company needs to process data to ensure that it is complying with its legal obligations. For example, we are required to retain invoices as per the Corporate Tax Act.

8. Who Has Access To Your Data?

Your information may be shared internally, including with the Paramount Security management team if access to the data is necessary for performance of their roles. There are times where the company may share your data with third parties, for example, to obtain credit and/or financial checks, with company engaged solicitors.

9. How Long Does Paramount Security Hold Data?

The company will hold your personal data for the duration of a contract agreement or until you request for your data to be removed.

- Client contracts are retained for the duration of the contract and should the contract be terminated the contract will be retained and then destroyed after six months.
- Invoices are kept electronically and are retained for seven years for HMRC purposes.
- Any customer with a legal action claim against them and an outstanding balance payable, Paramount Security will keep the correspondence until the debt has been resolved. Once full payment is received, the letters will be deleted from the finance server.

10. Requesting Access to Your Personal Data

As a data subject, you have many rights.

- Right of access – you have a right to access to your data and to certain information about the processing of that personal data. This information must usually be provided to you free of charge within a month of receiving your request.
- Right of rectification (correction) – you have the right to ask for your personal data to be corrected if it's inaccurate and completed if it's incomplete.
- Rights to be forgotten- in certain circumstances you can ask us to erase your personal data. It's unlikely to be possible to accept your request if, for example, we have a contractual or other legal duty to retain your information.
- Right to restriction of processing – in certain circumstances you have a right to restrict the processing of your personal data. This may include when you dispute its accuracy (until the accuracy is proved); if you have objected to the processing (when it was necessary for our legitimate interest) and we are considering whether our legitimate interest overrides your own; or if we no longer need the data but you need us to keep it in order to establish, exercise or defend a legal claim.
- Right of portability – in certain circumstances, you have the right to move, copy or transfer your data to another data controller or to yourself. This right is only relevant if the data is being processed on the basis of consent or for the performance of a contract and the processing is carried out by automated means. This right is different from the right of access and the types of information you can get under the two separate rights may be different.
- Rights in relation to automated decision making – you may have the right to challenge and request a review of a decision that was made by automated means.
- Right to object – in certain circumstances, you have the right to object to the processing of your data when it is being processed on the basis of our legitimate interest. We must stop processing the data unless we can demonstrate that our legitimate interests override your own, or if the processing is necessary for legal reasons. You have an absolute right to object to processing your data for direct marketing purposes including profiling relevant to direct marketing. If you object to us processing your data for direct marketing purposes, we must accept your request and stop the processing as soon as we receive your objection.

If you would like to exercise any of these rights, please contact our DPO.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance.

Alternatively, you can contact the Information Commissioner's Office.

Ed Githaiga
Managing Director
May 25th 2026