Data Protection Policy

Document Reference: PRM-P-27	**Version:** N1
Revision Date: 01 May 2026	**Expiry Date:** 01 May 2027
Category: Policy	**Status:** Active

1. Introduction and Scope

In the course of business, Promont Limited collects, stores and processes personal data relating to employees, clients, customers, suppliers and other individuals. Promont Limited is committed to protecting and respecting the privacy of all individuals whose personal data it processes, in full compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

This policy applies to all personal data processed by Promont Limited, whether in electronic or paper form. It applies to:

- All employees (permanent, temporary, casual and agency workers)
- Directors and officers
- Contractors, consultants and freelancers
- Volunteers and work experience placements
- Any third party processing personal data on behalf of Promont Limited

This policy does not form part of an employee's contract of employment but it is a condition of employment that employees abide by it. Any failure to comply may result in disciplinary proceedings.

2. Data Protection Principles

Promont Limited and all employees must comply with the six data protection principles set out in Article 5 of the UK GDPR. Personal data must be:

- **Processed lawfully, fairly and transparently** – there must be a valid lawful basis for processing and individuals must be informed about how their data is used
- **Collected for specified, explicit and legitimate purposes** – data must not be processed in a manner incompatible with the purposes for which it was collected
- **Adequate, relevant and limited to what is necessary** – only data that is genuinely needed for the stated purpose should be collected and processed
- **Accurate and kept up to date** – every reasonable step must be taken to ensure personal data is corrected or deleted without delay when it is inaccurate
- **Kept for no longer than is necessary** – personal data must be retained only for as long as it is needed for the purpose it was collected, in line with Promont Limited's data retention schedule
- **Processed securely** – appropriate technical and organisational measures must be in place to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In addition, Promont Limited must be able to **demonstrate compliance** with these principles (the accountability principle).

3. Lawful Bases for Processing

Promont Limited will only process personal data where it has a valid lawful basis to do so. The lawful bases under Article 6 of the UK GDPR are:

- **Consent** – the individual has given clear, informed and unambiguous consent for processing

- **Contract** – processing is necessary for the performance of a contract with the individual or to take steps at their request prior to entering a contract
- **Legal obligation** – processing is necessary to comply with a legal obligation (e.g. employment law, tax, health and safety)
- **Vital interests** – processing is necessary to protect someone's life
- **Public task** – processing is necessary for the performance of a task carried out in the public interest
- **Legitimate interests** – processing is necessary for Promont Limited's legitimate interests or those of a third party, provided these are not overridden by the individual's rights and freedoms

For most employment-related processing, Promont Limited relies on the contractual necessity, legal obligation and legitimate interests bases. Where consent is the basis for processing, it will be obtained freely, recorded clearly, and individuals will be informed of their right to withdraw consent at any time.

4. Special Category Data

Special category data requires additional protections under Article 9 of the UK GDPR. This includes data relating to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data and biometric data (where used for identification purposes)
- Health data
- Sex life or sexual orientation

Promont Limited may process special category data where it is necessary for employment law obligations (e.g. sickness absence management, equal opportunities monitoring, health and safety) and will ensure that an appropriate lawful basis and a condition for processing under Article 9 are identified and documented before any such processing takes place.

Criminal offence data is subject to separate conditions under the UK GDPR and the Data Protection Act 2018. Promont Limited processes such data where required for employment vetting in the security industry, in accordance with applicable SIA licensing requirements.

5. Data Subject Rights

Under the UK GDPR, individuals have the following rights in relation to their personal data:

- **Right to be informed** – individuals must be told how their data is collected and used, through privacy notices
- **Right of access** – individuals may request a copy of the personal data held about them (a Subject Access Request)
- **Right to rectification** – individuals may request correction of inaccurate or incomplete data
- **Right to erasure** – individuals may request deletion of their data in certain circumstances (the "right to be forgotten")
- **Right to restrict processing** – individuals may request that processing of their data is limited in certain circumstances
- **Right to data portability** – individuals may request their data in a structured, commonly used and machine-readable format
- **Right to object** – individuals may object to processing based on legitimate interests or for direct marketing purposes
- **Rights related to automated decision-making and profiling** – individuals have the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects

6. Subject Access Requests

Any individual whose personal data is held by Promont Limited has the right to make a Subject Access Request (SAR) free of charge. Promont Limited will respond to all SARs without undue delay and within **one calendar month** of receiving the request.

In complex cases, or where a large volume of data is involved, the response period may be extended by a further two months. The individual will be informed of any extension within one month of the original request, with reasons for the

delay.

To make a Subject Access Request, the individual should contact the Data Protection Officer in writing (by email or letter). Promont Limited will verify the identity of the requester before disclosing any personal data.

Promont Limited may charge a reasonable fee or refuse to act on a request only where it is manifestly unfounded or excessive, particularly if it is repetitive. In such cases, the individual will be informed of the decision and the reasons for it.

7. Privacy Notices

Promont Limited will provide clear and accessible privacy notices to individuals at the point their data is collected. Privacy notices will include:

- The identity and contact details of Promont Limited as data controller
- Contact details of the Data Protection Officer
- The purposes and lawful basis for processing
- Categories of personal data being processed
- Any recipients or categories of recipients of the data
- Details of any international transfers
- Retention periods or criteria for determining retention
- The individual's data protection rights
- The right to lodge a complaint with the Information Commissioner's Office (ICO)

8. Data Security

Promont Limited will implement appropriate technical and organisational measures to ensure the security of personal data. These measures include:

- Access controls and password protection on all systems containing personal data
- Encryption of personal data where appropriate, particularly in transit
- Secure storage of physical records in locked cabinets with restricted access
- Regular review of access permissions to ensure only authorised personnel have access
- Secure disposal of personal data that is no longer required (shredding of paper records, secure deletion of electronic data)
- Network security measures including firewalls, anti-malware protection and regular software updates
- Regular data backups to prevent accidental loss or destruction

Only authorised employees have access to personal data held by Promont Limited. All employees are responsible for ensuring that any personal data they handle is kept securely and is not disclosed to any unauthorised person.

9. Data Breaches

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All employees must report any actual or suspected data breach to the Data Protection Officer **immediately** upon becoming aware of it. Promont Limited maintains a data breach register to record all breaches, including those that do not require notification.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, Promont Limited will notify the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of the breach, in accordance with Article 33 of the UK GDPR.

Where a breach is likely to result in a **high risk** to the rights and freedoms of individuals, Promont Limited will also notify the affected individuals without undue delay, in accordance with Article 34.

10. International Transfers

Personal data must not be transferred outside the United Kingdom unless the destination country or territory has been

deemed to provide an adequate level of data protection, or appropriate safeguards are in place. Appropriate safeguards include:

- UK adequacy regulations recognising the destination country
- Standard contractual clauses approved by the ICO
- Binding corporate rules
- The individual's explicit consent, having been informed of the risks

Any proposed international transfer of personal data must be approved by the Data Protection Officer before the transfer takes place.

11. Data Retention

Promont Limited will not retain personal data for longer than is necessary for the purpose for which it was collected. Retention periods are determined by legal, regulatory, operational and contractual requirements.

As a guide, the following retention periods apply:

- **Current employee records** – retained for the duration of employment plus six years after the employment relationship ends
- **Unsuccessful job applicants** – retained for six months after the recruitment decision unless consent is given for longer retention
- **Payroll and tax records** – retained for six years in accordance with HMRC requirements
- **Health and safety records** – retained for 40 years where relevant to workplace injury or disease
- **SIA licensing and vetting records** – retained for the duration of the licence plus 12 months
- **CCTV footage** – retained for no longer than 31 days unless required for an investigation or legal proceedings
- **Customer and supplier records** – retained for six years after the end of the business relationship

Personal data that is no longer required will be securely disposed of in accordance with Promont Limited's data disposal procedures.

12. Data Protection Impact Assessments

Promont Limited will carry out a Data Protection Impact Assessment (DPIA) before undertaking any processing that is likely to result in a high risk to the rights and freedoms of individuals. This includes:

- Large-scale processing of special category data
- Systematic monitoring of publicly accessible areas (e.g. CCTV)
- Automated decision-making, including profiling
- Processing involving new technologies or novel approaches

DPIAs will be conducted in consultation with the Data Protection Officer and will be documented and reviewed regularly.

13. Data Processors and Third Parties

Where Promont Limited engages third-party data processors to process personal data on its behalf, it will:

- Carry out due diligence to ensure the processor can provide sufficient guarantees of compliance
- Enter into a written data processing agreement setting out the subject matter, duration, nature and purpose of processing, and the obligations of both parties
- Ensure the processor acts only on documented instructions from Promont Limited
- Require the processor to implement appropriate technical and organisational security measures
- Require the processor to notify Promont Limited without undue delay of any personal data breach

14. Employee Obligations

All employees must ensure they comply with the following requirements:

- Do not disclose personal data to any unauthorised person, whether inside or outside Promont Limited
- Always verify the identity and legitimacy of any person requesting personal data before disclosing it, particularly

over the telephone or by email
- Only access personal data that you need for the performance of your duties
- Keep personal data secure at all times – lock screens when unattended, use strong passwords, and store physical documents in locked storage
- Do not transfer personal data via unsecured channels (e.g. unencrypted email) unless appropriate safeguards are in place
- Report any actual or suspected data breach to the Data Protection Officer immediately
- If you receive a Subject Access Request or any other data protection request, forward it to the Data Protection Officer without delay
- Keep your own personal information up to date and notify your line manager promptly of any changes (e.g. change of address, name or emergency contacts)

15. Data Protection Officer

Promont Limited has designated a Data Protection Officer (DPO) who is responsible for:

- Advising Promont Limited and its employees on data protection obligations
- Monitoring compliance with the UK GDPR and the Data Protection Act 2018
- Managing Subject Access Requests and other data subject rights requests
- Overseeing Data Protection Impact Assessments
- Acting as the point of contact with the Information Commissioner's Office (ICO)
- Maintaining the data breach register and managing breach notifications
- Providing data protection training to employees

Employees may contact the Data Protection Officer for any questions or concerns relating to data protection.

16. Training

Promont Limited will provide data protection awareness training to all employees as part of their induction and on a regular basis thereafter. Enhanced training will be provided to employees in roles that involve significant processing of personal data. All training will be documented and records maintained.

17. Complaints

If any individual believes that Promont Limited has not complied with this policy or has not handled their personal data in accordance with data protection legislation, they should raise the matter with the Data Protection Officer in the first instance.

If the matter is not resolved satisfactorily, employees may raise the issue through Promont Limited's formal grievance procedure. Any individual also has the right to lodge a complaint directly with the **Information Commissioner's Office (ICO)**:

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF
Telephone: 0303 123 1113
Website: www.ico.org.uk

18. Review

This policy will be reviewed at least annually, or sooner if there are changes to data protection legislation, ICO guidance, or Promont Limited's business operations that necessitate an update. Any amendments will be communicated to all employees.

Dimitar Vaglarov
Managing Director
Promont Limited
Dated: 01 May 2026