GDPR POLICY

GDPR POLICY

Contents

GDPR POLICY

Introduction

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we always take seriously. This Data Protection Policy sets out how we handle the Personal Data of our customers, suppliers, employees, workers, and other third parties, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This Data Protection Policy applies to all Personal Data we process, regardless of the media on which it is stored or whether it relates to past or present employees, workers, customers, clients, supplier contacts, shareholders, website users, or any other Data Subject.

This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand, and comply with this Data Protection Policy when Processing Personal Data on our behalf, and attend training on its requirements. This Data Protection Policy sets out what we expect of you to ensure the Company complies with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach may result in disciplinary action, including summary dismissal.

Definitions

'Automated Decision-Making (ADM)': a decision made solely based on Automated Processing (including profiling) that has legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless specific conditions are met) but does not ban Automated Processing.

''Automated Processing'':

Any form of automated handling of Personal Data that uses it to assess personal traits of an individual, particularly to analyse or predict aspects such as that individual's job performance, financial situation, health, personal preferences, interests, reliability, behaviour, location, or movements. Profiling is an example of Automated Processing. The GDPR covers both automated processing of personal data and manual filing systems in which personal data can be accessed based on specific criteria. This could include chronologically ordered sets of manual records containing personal data.

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

"Criminal records data"

Refers to any data relating to criminal offences and convictions, which may be processed only by national authorities. National law may permit derogations provided that appropriate safeguards are in place. A comprehensive register of criminal offences can be maintained only by the responsible national authority.

GDPR POLICY

"Data Subject" is a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

''Explicit Consent'': consent which requires a very clear and specific statement (that is, not just action).

"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier. Personal data that has been pseudonymized – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

"Processing" is any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

"Sensitive Personal Data", referred to as "special categories of personal data" under the GDPR, means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, or biometric data processed to uniquely identify a person, as well as data concerning health, sex life, and sexual orientation. Processing of such data is prohibited.

The Company has appointed Dele Ogunlaru (Data Protection Officer) as the person responsible for data protection compliance within the Company. The Data Protection Officer (DPO) can be contacted at dele.ogunlaru@smartsecsolutions.com. Questions about this policy or requests for further information should be directed to him.

GDPR POLICY

Data Protection Principles

The Company processes HR-related personal data in accordance with the following data protection principles:

- The Company processes personal data lawfully, fairly and in a transparent manner.
- The Company collects personal data only for specified, explicit and legitimate purposes.
- The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Company keeps personal data only for the period necessary for processing.
- The Company adopts appropriate measures to ensure that personal data is secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
- Made available to Data Subjects, and Data Subjects allowed us to exercise certain rights in relation to their Personal Data

Legal Basis for Processing Personal Data

The Company and you may collect, process, and share Personal Data only fairly and lawfully, and for specified purposes. The GDPR restricts our processing of Personal Data to specified lawful purposes. You must identify and document the legal basis relied on for each Processing activity. Personal Data is processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Depending on the activity, we rely on the following lawful bases:

- **Performance of a contract** – where processing is necessary to deliver services or meet contractual obligations, including obligations involving TransUnion.
- **Legal obligation** – where processing is required to comply with applicable laws, regulatory requirements, or statutory obligations.
- **Legitimate interests** – where processing is necessary for legitimate business purposes such as system security, fraud prevention, risk management, audit, and compliance, and where such interests do not override the rights and freedoms of individuals. Appropriate assessments are conducted to ensure that the rights and freedoms of data subjects are protected.
- **Consent** – where required by law, and where individuals have been provided with a clear choice and the ability to withdraw consent at any time.

GDPR POLICY

The legitimate interests pursued by the controller (when processing is based on legitimate interests).

Our legitimate interests include operating our business, fulfilling contractual obligations, ensuring the security of systems and data, preventing fraud, supporting audit and compliance activities, and protecting TransUnion data. These interests are balanced against individuals' rights and freedoms, with appropriate safeguards in place.

The recipients or categories of recipients of the personal data (e.g., CRAs, partners, processors).

We may share personal data with customers or business partners, third-party service providers, regulators, law enforcement bodies, and professional advisers where required. Where data is shared outside the UK, appropriate safeguards will apply.

Details of any international data transfers outside the UK/EU and the safeguards in place.

We may transfer personal data to recipients or service providers located outside the UK and/or the European Economic Area (EEA).

Where such transfers occur, we ensure that appropriate safeguards are in place to protect personal data in accordance with applicable data protection laws. These safeguards may include the use of approved standard contractual clauses, international data transfer agreements, or transfers to countries recognised as providing an adequate level of data protection.

GDPR POLICY

Provision of Personal Data

A statement of whether the provision of personal data is statutory or contractual, and the possible consequences of not providing it.

Is the provision of personal data statutory or contractual?

The provision of certain personal data is primarily contractual and, in some circumstances, required to meet legal and regulatory obligations.

Personal data is required to:

- enter and perform contracts with customers, suppliers, or business partners.
- process orders, manage accounts, and deliver goods and services.
- verify identity and prevent fraud; and
- comply with applicable legal, regulatory, accounting, and tax obligations.

What are the consequences of not providing personal data?

If you choose not to provide the personal data, we request:

- we may be unable to enter into a contract with you.
- we may be unable to fulfil orders, supply goods, or provide services.
- we may be unable to conduct necessary verification, compliance, or fraud prevention checks; and
- as a result, our services may be delayed, restricted, or declined.

Where personal data is requested for optional purposes, such as marketing communications, providing this data is not mandatory, and you may withdraw your consent at any time without affecting your ability to receive goods or services from us.

GDPR POLICY

Consent

Please note that the rules relating to consent may not apply to certain processing activities. Please speak to Dele Ogunlaru, Data Compliance Officer, if you are seeking to rely on consent to collect and use Personal Data in the course of your duties.

A Data Subject consents to the processing of their Personal Data if they indicate agreement clearly, either by a statement or positive action, to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document that addresses other matters, the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw consent to Processing at any time, and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different, incompatible purpose that was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data, for Automated Decision-Making and for cross-border data transfers. Usually, we rely on another legal basis (and do not require Explicit Consent) to process most Special Categories of Personal Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

Credit Reference and Affordability Checks

To help us assess applications, prevent fraud, and meet our legal and regulatory obligations, we may obtain information about you from credit reference agencies (CRAs).

We obtain this information via **Creditsafe**, which uses its data partner**, TransUnion,** to supply consumer credit and identity data.

- **Creditsafe Business Solutions Limited** is authorised and regulated by the Financial Conduct Authority
  FCA Firm Reference Number: **742313**

- **TransUnion International UK Limited** is authorised and regulated by the Financial Conduct Authority
  FCA Firm Reference Number: **805757**

The information we receive may include data relating to your identity, credit commitments, payment history, and public record information. This data is used solely for legitimate business purposes, including creditworthiness assessment, identity verification, and fraud prevention, in accordance with applicable data protection laws.

GDPR POLICY

Further information about how Creditsafe and TransUnion process your personal data can be found in their respective privacy notices:

- **Creditsafe Privacy / Transparency Notice**:
  Transparency Notice | Customers & Suppliers
- **TransUnion CRAIN (Credit Reference Agency Information Notice)**:
  https://www.transunion.co.uk/legal/privacy-centre/pc-credit-reference
- **TransUnion Bureau Privacy Notice**:
  https://www.transunion.co.uk/legal/privacy-centre/pc-bureau

Individual Responsibilities

Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if the data they provide to the Company changes, for example, if they move house or change their bank details.
Individuals may have access to others' personal data in the course of their employment, contract, internship, or apprenticeship. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff.

Individuals who have access to personal data are required:

- to access only data that they have the authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example, by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

GDPR POLICY

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or without a legitimate reason, may constitute gross misconduct and could lead to dismissal without notice.

Informing Data Subjects About What Data We Collect and What We Use It For (Transparency)

The GDPR requires Data Controllers to provide Data Subjects with detailed, specific information about what Personal Data is collected, how it is used, and the lawful basis for that use. This information is provided in a Privacy Notice.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR, including the identity of the Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a privacy notice. The privacy notice must be provided to the Data Subject when the Personal Data is collected.

When Personal Data is collected from a third party, you must check that the third party collected it in accordance with the GDPR and that it can be shared with us.

Personal Data Must be Collected Only for a Specified Purpose.
If the Personal Data is to be used for a purpose other than that for which it was originally collected, the Data Subject must be informed beforehand, with an explanation of our lawful basis for using it for a different purpose. This will usually mean providing an updated privacy notice. If the lawful basis is consent, fresh consent from the Data Subject will be required.

Only collect Personal Data necessary for the purpose it is needed for
You must collect only the Personal Data required for your job duties. Please ensure that when the Personal Data is no longer needed for the specific purposes of your job, it is deleted in accordance with Company procedures.

Keep Personal Data accurate, complete, up to date and relevant for the purpose it was collected for
You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Do not keep Personal Data for longer than the purpose for which it was originally collected
Please ensure you take all reasonable steps to destroy or erase all Personal Data we no longer require from our systems. You will also need to ask third parties to whom we have shared that Personal Data to delete it.

GDPR POLICY

Data Subject Access Requests

All Data Subjects have the right to submit a subject access request. All subject access requests should be sent to the HR Manager without delay.

Data Subjects' Additional Rights

Data Subjects also have the following rights in relation to how we handle their personal data:

- Right to receive certain information about how we use their Personal Data
- Right to ask us to rectify data which is inaccurate or incomplete.
- Right to require us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed
- Right to restrict processing in specific circumstances.
- Right to ask us to transfer their Personal Data to a third party.
- Right to object to processing in certain circumstances.
- Right to prevent our use of their Personal Data for direct marketing purposes.
- Right not to be subject to automated decision-making
- Make a complaint to the Information Commissioner's Office.

You must verify the identity of anyone requesting data under any of the rights listed above (do not let third parties persuade you to disclose Personal Data without proper authorisation). To request that the Company take any of these steps, the individual should send the request to Dele Ogunlaru at dele.ogunlaru@smartsecsolutions.com.

Sharing Personal Data with Third Parties

Generally, you should only share Personal Data with third parties if certain safeguards and contractual arrangements have been put in place.

You may share the Personal Data we hold with another employee, agent, or representative of our group (including our subsidiaries and our ultimate holding company and its subsidiaries) only if the recipient has a job-related need to know the information. Please refer to the section on international data transfers if the Personal Data is being transferred out of the UK.

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

- They need to know the information for the purposes of providing the contracted services.
- Sharing the Personal Data complies with the privacy notice provided to the Data Subject, and, if required, the Data Subject's consent has been obtained.

GDPR POLICY

- The third party has agreed to comply with the required data security standards, policies and procedures and to implement adequate security measures.
- the transfer complies with any applicable restrictions on cross-border transfers; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

International Data Transfers

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which we transfer Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms.
- Appropriate safeguards are in place, such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct, or a certification mechanism. A copy of any of these can be obtained from the DPO.
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Information must not be transferred to countries outside the EEA without adequate protection and unless the Data Subject has been informed in a Privacy Notice or has requested the data to be transferred.

If you have any concerns or questions regarding the processing or use of personal data, you should contact your manager or DPO as soon as possible. If in any doubt, you should cease to process the information.

Automated Processing (Including Profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) A Data Subject has Explicitly Consented.
(b) The Processing is authorised by law; or
(c) the Processing is necessary for the performance of or entering a contract.

GDPR POLICY

If certain Special Categories of Personal Data are being processed, grounds (b) or (c) will not apply, but such Special Categories of Personal Data can be processed where necessary (unless less intrusive means are available) for a substantial public interest, such as fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), Data Subjects must be informed of their right to object when you first communicate with them. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights, freedoms, and legitimate interests.

We must also inform the Data Subject of the logic underlying the decision-making or profiling, the significance and envisaged consequences, and grant the Data Subject the right to request human intervention, to express their point of view, or to challenge the decision.

Direct Marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (e.g., email, text, or automated calls). The limited exception for existing customers, known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining only enough information to ensure that marketing preferences are respected in future.

Retention Periods

Personal Data should be retained only for the period necessary and for the purpose for which it is held.

GDPR POLICY

Data Security

The Company takes the security of all personal data seriously and adopts appropriate measures to ensure that all personal data is secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

All individuals who may process personal data on behalf of the Company are required to strictly adhere to its policies and procedures from collection through to destruction. We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks. We will regularly evaluate and test the effectiveness of those safeguards to ensure the security of our Processing of Personal Data.

You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures to prevent unlawful or unauthorised Processing of Personal Data and to prevent the accidental loss of, or damage to, Personal Data. You must exercise particular care to protect Special Categories of Personal Data from loss and from unauthorised access, use or disclosure.

You must follow all procedures and technologies we implement to maintain the security of all Personal Data from collection to destruction.

You may only transfer Personal Data to third-party service providers, such as payroll providers, pension scheme providers, who agree to comply with our instructions concerning the collection and use of Personal Data, which will include having adequate security measures in place to protect the Personal Data.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data. This means you must ensure:

- only people who have a need to know and are authorised to use the Personal Data can access it.
- The Personal Data is accurate and suitable for the purpose for which it is processed.
- authorised users are only able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of this policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

Where the Company uses a third-party supplier, such as a payroll bureau, to process personal data on its behalf, the supplier does so on the basis of written instructions, is under a duty of confidentiality, and is obliged to implement appropriate technical and organisational measures to ensure the security of the data.

GDPR POLICY

Reporting a Data Breach

A breach of data protection regulations or a failure to adhere to the Company's policies could have serious repercussions for both the Company and any individual Processing Personal Data on its behalf.

Any breach, or suspected breach, must be reported immediately to your manager and/or the Appointed Person. Do not attempt to investigate the matter yourself. A data breach is any act or failure to act which results in the loss, unauthorised access, disclosure or acquisition of Personal Data. Examples of data breaches include**, but are not limited to, losing your laptop, USB stick, or mobile phone, leaving documents/files on public transport,** or sending an email containing Personal Data to the wrong recipient.

The Company will maintain a record of all data breaches and, if legally required, will report certain breaches to the Information Commissioner's Office (ICO) and, in some circumstances, to the Data Subjects.

Any breach or failure to report a breach in a timely manner will be investigated and managed in accordance with the relevant procedures. Significant or deliberate breaches of this policy, such as accessing or sharing employee or customer data without authorisation or a legitimate reason, may constitute gross misconduct and could result in your summary dismissal.

Training

The organisation will provide training to all individuals on their GDPR responsibilities as part of their induction process, including reading this document and regularly refreshing their knowledge thereafter.

Individuals whose roles involve access to and/or processing of personal data will undergo additional training to ensure a comprehensive understanding of this policy and related documents.
You must regularly review all systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure the proper use and protection of Personal Data.

GDPR POLICY

Record Keeping

The GDPR requires us to maintain full and accurate records of all our data processing activities.

You must keep and maintain accurate corporate records reflecting our processing, including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should, at a minimum, include the name and contact details of the Data Controller and the DPO/Nominated Person; clear descriptions of the types of Personal Data, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period, and a description of the security measures in place. To create such records, data maps should be prepared that include the details set out above.

Changes to this Data Protection Policy

We reserve the right to amend this Data Protection Policy at any time without giving notice to you.

This Data Protection Policy does not override any applicable national data protection laws and regulations in the countries where the Company operates.

Helmey El-Aasar,
Managing Director,
19th June 2026

Policy Owner: Compliance Manager
Policy Owner's Contact Number: 020 3002 9122
Policy Sponsor: Managing Director

Next Review Date: June 2027