

Policies & Procedures

Data Protection &. GDPR Compliance Policy v1.0

Data Protection and GDPR Policy and Procedures

Introduction 2
Data Protection Principles 2
Legal Basis for Processing Personal Data 3
Data Subject Rights 3
Data Security Measures 3
Data Processing Activities and Record-Keeping 3
Data Transfers 4
Third-Party Processors 4
Training and Awareness 4
Data Protection Impact Assessments (DPIAs) 4
Auditing and Monitoring 4
Data Protection Officer (DPO) 5
Conclusion 5

VCare Consultancy Services Ltd.

Data Protection and GDPR Policy and Procedures

Policy Lead	**Mrs. Tavleen Sharma - Registered Manager**
Version No.	1.0
Date of issue	January 2025
Date to be reviewed	January 2026

VCare Consultancy Services Ltd.

Introduction

We are committed to protecting the privacy and security of all personal data under our control. This policy outlines the measures we have taken, or will take by contract award, to ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any other relevant data protection laws

This policy applies to all processing of personal data that we undertake as part of the delivery of services related to the UK government contract.

VCare Consultancy uses All-in-One Digital Care Management Software (licensed by Carebeans) which is a comprehensive solution designed to streamline and improve the management of care services. It integrates various functions and processes necessary for the effective delivery of care, including client management, scheduling, billing, reporting, and compliance.

All-in-One Digital Care Management Software meets regulatory compliance:

- The Data Protection Act 2018.
- UK General Data Protraction regulation (UK GDPR).
- The Privacy and Electronic Communications Regulations (PECR) 2003.
- The Freedom of Information Act 2000 (FOIA).
- The Network and Information Systems (NIS) Regulations 2018.

Data Protection Principles

We adhere to the following principles in all aspects of data processing:

- **Lawfulness, fairness, and transparency**: Personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose limitation**: Personal data is collected for specified, legitimate purposes and is not processed in a manner that is incompatible with those purposes
- **Data minimisation**: We only collect personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- **Accuracy**: We ensure that personal data is accurate and, where necessary, kept up to date.
- **Storage limitation**: Personal data is not kept for longer than is necessary for the purposes for which it is processed.
- **Integrity and confidentiality**: Personal data is processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

- **Accountability**: We are accountable for compliance with these principles and have implemented measures to demonstrate our compliance.

Legal Basis for Processing Personal Data

Under UK GDPR, we process personal data based on one or more of the following legal grounds:

- Consent: Where we have obtained explicit consent from data subjects for a specific purpose.
- Contractual necessity: Where processing is necessary for the performance of a contract with the data subject.
- Legal obligation: Where processing is required to fulfill a legal obligation (e.g., compliance with a government contract).
- Legitimate interests: Where processing is necessary for our legitimate interests, provided that these interests are not overridden by the rights and freedoms of the data subject.

Data Subject Rights

We ensure that the following rights of data subjects are upheld:

- **Right to access**: Data subjects can request access to their personal data and obtain information about its processing.
- **Right to rectification**: Data subjects can request correction of inaccurate or incomplete personal data.
- **Right to erasure (Right to be forgotten)**: Data subjects can request the deletion of personal data where it is no longer necessary for processing or where consent has been withdrawn.
- **Right to restriction of processing**: Data subjects can request restrictions on the processing of their personal data in certain circumstances.
- **Right to data portability**: Data subjects can request their personal data in a structured, commonly used, and machine-readable format.
- **Right to object**: Data subjects can object to the processing of their personal data in certain circumstances, including for direct marketing purposes.

Data Security Measures

To ensure the confidentiality, integrity, availability, and resilience of personal data, we have implemented the following security measures:

- **Encryption**: All sensitive personal data is encrypted both in transit and at rest using appropriate encryption standards.
- **Access controls:** We implement robust access controls, ensuring that personal data is only accessible to authorised personnel.
- **Secure systems:** Our IT infrastructure is protected by firewalls, intrusion detection systems, and other security mechanisms to prevent unauthorized access and data breaches.
- **Regular vulnerability testing:** We regularly perform security audits, vulnerability assessments, and penetration testing to identify and address potential risks.
- **Data breach management:** We have a data breach response plan in place and will notify the Information Commissioner's Office (ICO) and affected data subjects within the legal timeframes if a data breach occurs.

Data Processing Activities and Record-Keeping

We maintain detailed records of all personal data processing activities. These records include:

VCare Consultancy Services Ltd.

- The purpose of processing
- The categories of personal data involved
- The recipients of personal data
- The retention periods for data
- The legal basis for processing

These records are regularly updated and can be made available to regulatory authorities upon request

Data Transfers

We ensure that any transfers of personal data outside the UK are conducted in compliance with the UK GDPR. Measures include:

- **Standard Contractual Clauses (SCCs)**: For transfers to countries that do not have an adequacy decision, we implement SCCs to ensure that the recipient provides an adequate level of protection for personal data.
- **Adequacy Decisions**: We ensure that data is only transferred to countries with an adequacy decision, where applicable.

Third-Party Processors

Where we use third-party processors to handle personal data, we ensure that they are contractually bound to comply with UK GDPR. We ensure that all third-party processors provide sufficient guarantees regarding their ability to implement appropriate technical and organisational measures to protect personal data.

Training and Awareness

We provide regular training to all employees on data protection and privacy practices. This training ensures that everyone in the organisation understands their responsibilities and the importance of complying with the UK GDPR and protecting personal data.

Data Protection Impact Assessments (DPIAs)

We conduct DPIAs to assess and mitigate risks where there is a high risk to the rights and freedoms of individuals, such as when introducing new processing activities or technologies that may affect personal data.

Auditing and Monitoring

We conduct regular audits and monitor our data protection practices to ensure compliance with the UK GDPR. We evaluate the effectiveness of our data protection measures and make improvements as necessary.

V Care Consultancy Services Ltd.

Data Protection Officer (DPO)

We have appointed a Data Protection Officer (DPO) to oversee and ensure compliance with our data protection obligations. The DPO acts as a point of contact for data subjects and the Information Commissioner's Office (ICO).

- **DPO Contact Information**:
- Mr. Ashish Sharma (+44 7495785566 / support@vcareconsultancy.com)

Conclusion

This policy outlines our commitment to ensuring the protection of personal data and compliance with the UK GDPR. We take all reasonable steps to safeguard the rights of data subjects and to maintain the integrity and security of personal data throughout the processing lifecycle.

This policy and the procedures apply to employees, contractors, agency and temporary workers, suppliers, service users and carers, and anyone else with whom we come in to contact with during the course of our work.

VCare Consultancy Services Ltd.

Annex A

To ensure compliance with the **UK Data Protection Laws**, including the **UK General Data Protection Regulation (UK GDPR)**, **Data Protection Act 2018**, and related privacy regulations, **VCare Consultancy Services Limited** must implement comprehensive systems, processes, and policies to safeguard personal data. Below is an overview of how VCare Consultancy Services Limited can ensure compliance with the key principles, and the necessary steps to align with legal obligations:

Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience of Processing Systems and Services

Action Plan:

- **Data Encryption:** Ensure that all personal data is encrypted both **at rest** (on servers, databases) and **in transit**(when data is transferred over networks).
- **Access Controls:** Implement **role-based access controls (RBAC)** to restrict access to personal data to authorized personnel only.
- **Data Backups:** Regularly back up all personal data and ensure that backups are securely stored to maintain data availability.
- **Resilient IT Infrastructure:** Adopt **cloud-based solutions** or on-premise data centers with adequate disaster recovery plans to ensure system resilience and business continuity.
- **Regular Security Audits:** Conduct **regular security audits and penetration testing** to identify vulnerabilities and ensure the integrity of data processing systems.
-

Complying with the Rights of Data Subjects (Privacy Information, Access, Rectification, Deletion, and Portability of Personal Data)

Action Plan:

- **Transparency and Privacy Notices:** Ensure that clear and concise **privacy notices** are provided to all data subjects, outlining the types of personal data processed, the purpose of processing, legal basis for processing, and the rights available to individuals under UK GDPR.
- **User Access to Data:** Implement a **self-service portal** for clients and staff to easily access their personal data and review what data is being processed.
- **Data Rectification:** Establish procedures to handle requests from data subjects for correcting inaccurate or incomplete data.
- **Data Erasure (Right to be Forgotten):** Develop protocols for securely deleting personal data upon request, especially if data is no longer necessary for processing or if consent is withdrawn.
- **Data Portability:** Provide data subjects with an option to request their personal data in a **structured, commonly used, and machine-readable format** so they can transfer it to another provider.
- **Clear Communication:** Ensure communication channels are in place (e.g., email, helpdesk) to support individuals in exercising their data rights.

VCare Consultancy Services Ltd.

Ensuring Consent-Based Processing Meets Standards of Active, Informed Consent, and That Consents Are Recorded and Auditable

Action Plan:

- **Explicit Consent:** Obtain **explicit consent** for processing personal data when required, especially for sensitive categories of data (e.g., health data). Use opt-in consent mechanisms that are **clear and unambiguous**.
- **Consent Management System:** Implement a **consent management system** that allows VCare to track, manage, and record consents in a compliant manner. Ensure that each consent record is **auditable** and time-stamped.
- **Review Mechanisms:** Periodically review existing consents to ensure they remain valid and up-to-date. Ensure that individuals can **withdraw consent** at any time, and update processing activities accordingly.
- **Transparency in Consent Requests:** Provide clear information on the data processing activities before seeking consent, including the **purpose of processing** and any third parties involved.

Ensuring Legal Safeguards Are in Place to Legitimize Transfers of Personal Data Outside the EU (if Such Transfers Will Take Place)

Action Plan:

- **Data Transfers:** If personal data needs to be transferred outside the **UK/EEA**, VCare must ensure that appropriate legal safeguards are in place:
    - **Adequacy Decisions:** Ensure that the destination country has been recognized by the UK as providing adequate protection for personal data.
    - **Standard Contractual Clauses (SCCs):** If transferring data to a non-adequate country, implement **Standard Contractual Clauses (SCCs)** or other approved mechanisms (e.g., Binding Corporate Rules) to ensure the data is protected.
    - **Data Transfer Impact Assessments (DTIAs):** Perform **Data Transfer Impact Assessments** before transferring personal data outside the UK/EEA to evaluate and mitigate any risks.
    - **Third-Party Processors:** Ensure that any third parties involved in such transfers are compliant with data protection standards and include appropriate clauses in their **Data Processing Agreements (DPAs)**.

Maintaining Records of Personal Data Processing Activities

Action Plan:

- **Records of Processing Activities (RoPA):** Develop and maintain a comprehensive **Record of Processing Activities (RoPA)** that outlines:
    - The purposes of processing.
    - Categories of personal data being processed.
    - Categories of data subjects.
    - The recipients of personal data.
    - Any international transfers.
    - Data retention periods.
    - Security measures in place to protect the data.

VCare Consultancy Services Ltd.

- **Regular Reviews:** Perform regular reviews and updates of the processing activities to ensure that the records remain accurate and reflect current data processing practices.

Regularly Testing, Assessing, and Evaluating the Effectiveness of the Above Measures

Action Plan:

- **Continuous Monitoring:** Implement continuous monitoring systems for assessing compliance with data protection laws, including regular reviews of data processing activities, security measures, and data access controls.
- **Penetration Testing & Security Audits:** Conduct regular **penetration testing** and **security audits** to evaluate the effectiveness of IT security systems and identify vulnerabilities.
- **Data Protection Impact Assessments (DPIAs):** Regularly carry out **DPIAs** for high-risk processing activities (e.g., processing sensitive data) and evaluate potential impacts on data subjects' privacy.
- **Employee Training & Awareness:** Provide regular **GDPR and data protection training** for all employees to ensure they understand the principles of data protection and how to manage personal data securely.
- **Compliance Audits:** Perform periodic internal and external **compliance audits** to verify the effectiveness of implemented measures and ensure full compliance with UK GDPR and other applicable data protection laws.

Overall Data Protection Compliance Strategy for VCare Consultancy Services Limited

- **Data Protection Officer (DPO):** Appoint a **Data Protection Officer (DPO)** if required, or an external consultant, to oversee data protection compliance and ensure adherence to the UK GDPR, Data Protection Act, and other applicable laws.
- **Data Protection Policies:** Develop and implement comprehensive **data protection policies** that cover data collection, use, storage, sharing, and retention, as well as policies for responding to data subject rights requests and data breaches.
- **Third-Party Due Diligence:** When engaging third-party vendors or service providers (e.g., cloud storage, software solutions), ensure they are compliant with the GDPR through **Data Processing Agreements (DPAs)** and regular audits.
- **Regular Reporting:** Maintain an internal reporting process for data protection issues, data breaches, and any incidents that could affect personal data security.

VCare Consultancy Services Ltd.