DATA PROTECTION POLICY

PREPARED BY	APPROVED BY	DATE
Data Protection Officer	Managing Director	03/09/2024

CONTENTS

1. INTRODUCTION

BACKGROUND TO THE GENERAL DATA PROTECTION REGULATIONS

The European Union (EU) General Data Protection Regulation (GDPR) came into effect on the 25 May 2018 replacing the EU Data Protection 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that Personal Data is not processed without their knowledge, and, wherever possible, that it is processed with the Data Subjects consent. The Data Protection Act 2018 ('DPA 2018') is the UK's implementation of the GDPR. Vertex Professional Services (the "Company") complies with the EU/ UK GDPR. This policy provides further information that support the Company's implementation of the EU/ UK GDPR (the term 'GDPR' shall be used to refer to both the UK and EU GDPR unless a key difference is noted).

Refer to Appendix A for a list of definitions used by this policy.

2. APPLICABILITY

This policy applies to any person and/or organisation affiliated with the Company and who has access to, and who in the discharge of their business activities is required to process Personal Data.

This policy applies to all the Company's Personal Data processing functions, including those performed on customers', apprenticeship programmes, clients', employees', suppliers', third parties in general, and business partners' Personal Data, and any other Personal Data the Company processes from any source (the term "staff" shall be used to refer to everyone).

3. COMPLIANCE WITH GDPR

Compliance with the GDPR is described by this policy and other relevant sub-policies, which are easily accessible on the Company's Intranet homepage, namely the Knowledge Hub under the tile 'Information Governance & Data Protection' tile.

In determining the scope for compliance with the GDPR, the Company has considered:

- A suitably qualified and experienced governance structure to ensure all applicable statutory, regulatory, and/or contractual obligations are being managed appropriately.
- Suitably trained and qualified personnel to fulfil our data protection duties.
- The external and internal issues that are relevant to the purposes of the Company's Personal Data processing activities.
- The application of an information security risk management process for managing our information and Personal Data risk – refer to document IG 1.1 Information Risk Management Policy and the Security Reliability Framework (SRF) 1.0 Information Security Policy.

The Company has developed a Privacy Information Management System (PIMS) which supports our approach to governance, risk and compliance of Personal Data.

4. POLICY STATEMENT

STATEMENT

The Senior Leadership Team (SLT), our leaders and managers are committed to compliance with, and the protection of the 'rights and freedoms' of all individuals (the "Data Subject") whose information the Company collects and processes. This is in accordance with the GDPR and Data Protection Act (DPA) 2018, and/or other applicable localised Data Laws.

The Company's Privacy Working Group (PWG) is responsible for reviewing the register of Processing activities annually in the light of any changes to the Company's activities and to any additional requirements identified by means of our IG 12.0 Data Protection Impact Assessment Policy.

Our parent company, our subsidiaries, business partners and more generally any third parties working with, or for the Company, and who have access to our staff or customer's Personal Data, are expected to have read, understood, and comply with this policy.

No Third Party may access Personal Data held by the Company without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which the Company is committed, and which gives the Company the right to audit compliance with the agreement.

5. REQUIREMENTS

PRINCIPLES

All processing activities shall be:

- Collected for specified, explicit and legitimate purposes only.
- Accurate and, where necessary, kept up to date.
- Retained only for as long as necessary.
- Processed lawfully, fairly and in a transparent manner.
- Processed securely, in an appropriate manner to maintain security.
- Adequate, relevant and limited to what is necessary.

Refer to Appendix B for a full description of the Data Protection Principles.

DATA PROTECTION OFFICER (DPO)

A Senior Leadership Team (SLT) member has been appointed as the Data Protection Officer (DPO) reporting directly to the Company's Managing Director. The DPO role requires that specific tasks are conducted. These include:

- Support the Company in upholding the rights of Data Subjects as it relates to the Company's Personal Data processing activities.
- Respond to enquiries from Data Subjects in a timely manner.
- Establish and maintain an information governance framework to monitor compliance with this policy.
- Establish and maintain a General Data Protection training and awareness programme.
- Support compliance with this policy by providing advice and guidance.
- Having timely and appropriate access to information and information systems as it relates to the discharge of the DPO duties.

DPO Contact Details	
DPO:	Kenny Harkett
E-mail:	Kharkett@gov2x.eu
Tel:	+44 (0)7731987132

6. COMPLIANCE

A breach of any part of this policy may be considered a disciplinary offence, which in severe cases could lead to disciplinary action up to and including dismissal and/or criminal proceedings being undertaken. This obligation also extends to any external organisation contracted to support or access our own and our customer' Personal Data.

7. RESPONSIBILITIES AND ROLES

The Company acts as a Data Controller and a Data Processor under the GDPR. All those in the scope of this policy are responsible for adhering to the requirements of this policy:

SENIOR LEADERSHIP TEAM

- Under the auspices of the Managing Director, the SLT have overall responsibility for this policy, and for reviewing the effectiveness of actions taken in response to any concerns raised.
- SLT are responsible for making sure all Personal Data processing activities within each of their respective area of responsibility is compliant with this policy.

MANAGERS

- Senior management and leaders are responsible for developing and encouraging good information and information security handling and adequate Personal Data practices within the Company. Manager's must ensure that their staff are aware of their responsibilities and adhere to this policy.

STAFF

- All staff are responsible for ensuring that this policy and any requirements are being consistently applied to all Personal Data processing activities.
- Staff are responsible for ensuring that any Personal Data about themselves and/or supplied by them to the Company is and remains accurate and up to date.

INFORMATION ASSET OWNERS

Those described as Information Asset Owners (including System Owners) of this policy are responsible for ensuring their processes, and information systems they are responsible for meet the minimum requirements of all in-scope policies and sub-policies. Refer below.

PRIVACY WORKING GROUP

The Privacy Working Group (PWG) acts as the SLT sub-committee for all matters Privacy and ensure:

- That compliance with data protection legislation can be demonstrated through internal audit and provide the SLT with independent assurance that the Company is adhering to the requirements of this policy.
- That appropriate GDPR awareness training is readily available across the Company.

All Personal Data enquiries should be sent to - privacy.emea@gov2x.eu, or by contacting the Company's DPO directly using the contact details at section 5 to this policy.

8. DATA SUBJECT RIGHTS

Data Subjects have the following rights regarding data processing, and the data that is recorded about them:

- The right to be informed when their Personal Data is being processed.
- The right to access Personal Data held about them, including the nature of information held and to whom it has been disclosed.
- The right to have processing restricted in certain cases.
- The right to prevent processing for purposes of direct marketing.
- The right to be informed about the mechanics of automated decision-making processes that will significantly affect them.
- The right to not have significant decisions that will affect them made solely by automated process.
- The right to have Personal Data rectified or erased and to block processing of Personal Data in certain situations.
- The right to object to processing in specific instances.
- The right to request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- The right to have Personal Data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another Data Controller.
- The right to object to any automated profiling that is occurring without consent.

The subsequent section provides details with regard how you as a Data Subject can exercise these rights.

8.1 DATA SUBJECT ACCESS REQUEST (DSAR)

Data Subjects may make Data Subject access requests (DSARs) as described in the Company's IG 1.23 Data Subject Access Request Procedure.

Data Subjects have the right to complain related to the processing of their Personal Data, the handling of a request from a Data Subject and appeals from a Data Subject on how complaints have been handled in line with the IG 1.24 Complaints Procedure.

8.2 AWARENESS TRAINING

The Company will ensure relevant training is in place to assist staff in their day-to-day handling of Personal Data. All new staff must complete the Company's information security and GDPR online training courses to ensure they are aware of the risks and their responsibilities in handling Personal Data, and more generally any Company related information. Staff are required to complete refresher training annually reflecting any changes and updates in information governance best practices.

Information Asset Owners must complete additional training reflecting their role overseeing local procedures in relation to the management and security of Personal Data and information within their remit.

8.3 CONSENT

The Company understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed, and unambiguous indication of the Data Subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to them. The Data Subject can withdraw their consent at any time, although there are occasions where the Company must process their Personal Data to conform with, for example, a contract of employment, pay a salary etc.

The Company understands 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or based on misleading information will not be a valid basis for processing.

For sensitive data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for the processing activity exist. Further information is available in the Company's IG 14.0 Consent Procedure located on the Knowledge Hub under the Data Protection tile.

8.4 SECURITY OF PERSONAL DATA

All staff are responsible for ensuring that any Personal Data that the Company holds and for which they are responsible for is kept securely and is not under any conditions disclosed to any Third Party unless that Third Party has been specifically authorised by to receive that information and has entered a confidentiality and/or Data Sharing agreement. If you are unsure you must check with the Company's Contract department or the DPO.

All Personal Data should be accessible only to those who need to use it, and access to any Personal Data on any Information Communications Technology (ICT) or other information bearing assets such as storage devices, USB etc., may only be granted in line with the Company's SRF 1.2 Access Control Policy. All Personal Data should be treated with the highest security and must be kept:

- If hard copy, in a lockable room with controlled access (hard copy documents must be kept to a minimum and only where necessary).
- If hard copy, in a locked drawer or filing cabinet.
- If electronic, password protected in line with our Company requirements in the Access Control Policy.
- If electronic, stored on (removable) computer media that is encrypted in line with the Company's SRF 1.10 Encryption Policy (put 'Restricted document' on Knowledge Hub.
- Securely erased and/or destroyed in line with the SRF 1.19 Media Sanitisation Policy.

Hard-copy records that contain large volumes of Personal Data may not be left where they can be accessed by unauthorised personnel and may not be removed from Company premises without explicit authorisation from the relevant Information Asset Owner or System Owner. Where large amounts of Personal Data are required for a legitimate purpose and transferred outside of a secure location, be that on storage devices and/or hard copy formats, the Company's Contracts and/or DPO must be approached, and written authorisation sought. As soon as hard-copy records are no longer required for day-to-day business and client support, they must be retuned or returned and destroyed appropriately.

Personal Data may only be deleted or disposed of in line with the IG 3.0 Records Management and Retention Policy. Hardcopy records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by SRF 1.19 Media Sanitisation Policy before disposal by authorised IT support staff only.

8.5 DISCLOSURE OF PERSONAL DATA

It is essential that Personal Data is not disclosed to unauthorised staff and/or third parties, which include family members, friends, government bodies and, in certain circumstances, the police. All staff should exercise caution when being asked to disclose Personal Data to a third party. It is important to bear in mind whether disclosure of the information is relevant to, and necessary for, the conduct of the activity, actual or proposed. If in doubt always seek the advice from the DPO.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the PWG.

8.6 RETENTION AND DISPOSAL OF PERSONAL DATA

The Company does not keep Personal Data in a form that permits identification of Data Subjects for a longer period than is necessary, in relation to the purpose (s) for which the data was originally collected.

Our retention period for each category of Personal Data is set out in the IG 4.0 Records Retention Schedule along with the criteria used to determine this period, including any statutory obligations that may apply. All staff are responsible for ensuring that any Personal Data being retained meets our retention criteria and to dispose and/or delete any Personal Data in line with Company procedures.

Personal Data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the 'rights and freedoms' of Data Subjects. The relevant Information Asset Owner or System Owner remains responsible for the retention and correct disposal of Personal Data within their area of responsibility.

8.7 DATA TRANSFERS

The flow of Personal Data within the European Economic Area (EEA) to non-EEA countries (referred to in the GDPR as 'third countries') and international organisations are necessary for several reasons such as the expansion of international trade and for divulging statistical data to our parent organisation etc. However, the GDPR deems such flows of Personal Data as unlawful unless that third country can offer an adequate level of data protection that is at least equivalent with those data protection standards of the European Union member states, including the UK. This is referred to as an adequacy decision. Where an adequacy decision on a third country has been reached, in such cases transfers of Personal Data may take place without the need to obtain any further authorisation from the supervisory authority, albeit the Company must still conduct its due diligence before Personal Data is exchanged.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union which can be accessed by pressing the link below:

DATA PROTECTION ADEQUACY FOR NON-EU COUNTRIES (EUROPA.EU)

In the absence of an adequacy decision the Company is required to take additional measures by way of making sure appropriate safeguards are in place before any Personal Data is transferred. There are different methods available to achieve this, such as the use of standard data protection clauses, and data transfer agreements.

In the absence of standard data protection clauses, a transfer of Personal Data to a third country or international organisation shall only take place on one of the following conditions:

- The Data Subject has explicitly consented to the proposed transfer, after having been informed of the risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards. A consent form must be completed.
- The transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or the implementation of pre-contractual measures taken at the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

In all cases where Personal Data will be transferred inside and out of the EEA the DPO and Contracts department must be informed before any transfer of Personal Data commences. This will ensure that the Data Subject's rights and freedoms can be consistently applied throughout any transfers taking place.

9. INTERACTION WITH OTHER POLICIES AND PROCEDURES

The Company has several existing policies and procedures that collectively make up the Information Governance Framework. These include:

- IG 1.0 Information Governance Policy
- IG 2.0 Data Protection Policy (this policy)
- IG 3.0 Records Management and Retention Policy
- IG 4.0 Records Retention Schedule
- IG 5.0 Document Management Policy
- IG 6.0 Employee Security Information Investigation Procedure
- IG 7.0 Digital Preservation Policy
- IG 8.0 Employee Monitoring Standard
- IG 9.0 Information Strategy Principles
- IG 10.0 Data Classification Standard
- IG 11.0 Personal Data Breach Procedure
- IG12.0 Data Protection Impact Assessment Policy.
- IG 13.0 Privacy Procedure
- IG 14.0 Consent Procedure
- IG 14.1 Withdraw Consent Procedure
- IG 1.23 Data Subject Access Request Procedure

Other relevant policies:

- SRF 1.0 Information Security Policy.
- SRF 1.4 Security Education Training Awareness Policy.
- SRF 1.5 Security Incident Reporting Policy.
- SRF 1.6 Acceptable Use Policy.

ANNEX A

DEFINITIONS

Information Asset Owner the Accountable owner of the system on which the Personal Data is processed.

Project Owner/ responsible person the Company's person who is responsible for the collection and processing of Personal Data.

Material scope the GDPR applies to the Processing of Personal Data wholly or partly by automated means (e.g. by computer) and to the Processing other than by automated means of Personal Data (e.g. paper records) that form part of a Filing System or are intended to form part of a Filing System.

Territorial scope the GDPR applies to all controllers and processors established in the UK and EU that process the Personal Data of Data Subjects, in the context of that establishment. It also applies to controllers and processors outside of the UK and EU that process Personal Data to offer goods and services or monitor the behaviour of Data Subjects who are resident in the UK/ EU.

Personal Data any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of Personal Data Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by UK/ EU or Member State law, the controller or the specific criteria for its nomination may be provided for by UK/ EU or Member State law.

Data processor a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

Data Subject any living individual who is the subject of Personal Data held by an organisation.

Processing Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Profiling is any form of automated Processing of Personal Data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the Data Subject to object to Profiling and a right to be informed about the existence of Profiling, of measures based on Profiling and the envisaged effects of Profiling on the individual.

Personal Data breach a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. There is an obligation on the controller to report Personal Data breaches to the supervisory authority and where the breach is likely to adversely affect the Personal Data or privacy of the Data Subject.

Data Subject consent means any freely given, specific, informed, and unambiguous indication of the Data Subjects' wishes by which they, by a statement or by a clear affirmative action, signify agreement to the Processing of Personal Data.

Child (/Children) the EU GDPR defines a child as anyone under the age of 16 years old, although the UK GDPR has lowered this age to 13 years of age. The Processing of Personal Data of a Child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the Child.

Third Party a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, processor and persons who, under the direct authority of the Data Controller or processor, are authorised to process Personal Data.

Filing System any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

ANNEX B

IG 2.0 Data Protection Policy

Dated September 2024

DATA PROTECTION PRINCIPLES

All processing of Personal Data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The Company's data protection policies and procedures help to govern and demonstrate compliance with these principles. These can be found in the Knowledge Hub under the 'Information Governance & Data Protection' tile. All employees are expected to familiarise themselves with these policies and procedures, collectively referred to as the Information Governance Framework.

The next section will examine these principles in more detail, and which apply to all our Personal Data processing activities.

PERSONAL DATA MUST BE PROCESSED LAWFULLY, FAIRLY, AND TRANSPARENTLY

Lawful - All Personal Data processing activities must be lawful. The responsible person collecting the Personal Data, must identify a lawful basis before any Personal Data is processed. These are often referred to as the "conditions for Processing", for example consent, which is covered below.

Fairly – for Processing to be fair, the Company as a Data Controller or a Data Processor must make certain information available to the Data Subjects, or to a Data Controller for who we are processing Personnel Data on behalf of, as practicable. This applies whether the Personal Data was obtained directly from the Data Subjects or from other sources.

Transparency – the GDPR includes rules on providing privacy information to Data Subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

The Company's Privacy Notice serves as a transparent communication tool providing individuals with an understanding of their privacy rights and the control they have over their Personal Data. It outlines the types of data we collect, the purpose of the data collection, the retention period, and if third parties are involved in data sharing. The Privacy Notice is available on the Knowledge Hub.

PERSONAL DATA CAN ONLY BE COLLECTED FOR SPECIFIC, EXPLICIT, AND LEGITIMATE PURPOSES

Personal Data can only be collected for specific, explicit, and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differ from those formally notified to the supervisory authority as part of the Company's register of Processing. The Company's Information Governance (IG) 13 Privacy Procedure sets out the relevant procedures, which all employees must follow.

PERSONAL DATA MUST BE ADEQUATE, RELEVANT, AND LIMITED TO WHAT IS NECESSARY FOR PROCESSING

Where a justified and purposeful reason exists for collecting Personal Data, the responsible person collecting the data) is responsible for ensuring that they do not collect information that is not strictly necessary for the purpose for which it has been originally obtained.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair Processing statement or link to a privacy statement, and be pre-approved by the PWG.

The PWG will ensure that, on an on-going basis, all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive. This is governed by using a combination of procedures and tools, which include the responsible person completing several activities including a Data Protection Impact Assessment (DPIA). The DPIA will ensure that any Personal Data risks have been considered through robust and consistent Risk Assessment. The responsible person must contact the PWG if they are unsure what activities must be completed prior to processing any Personal Data.

Refer to the following documents for further information:

- IG10.0 Data Protection Impact Assessment Policy.

PERSONAL DATA MUST BE ACCURATE AND KEPT UP TO DATE WITH EVERY EFFORT MADE TO ERASE OR RECTIFY PERSONAL DATA WITHOUT DELAY

The Company has an obligation to ensure that the Personal Data it processes is reviewed and kept up to date. No data should be kept unless it is reasonable to assume that it is accurate. This is achieved in several ways, which include:

- All employees must attend the mandatory GDPR training on induction and annually thereafter. This training emphasises the importance of collecting accurate data and maintaining it.
- For certain employees and/or departments there is a requirement to attend bespoke GDPR training. This is designed for employees and/or departments that regularly process different categories of Personal Data, for example, the HR and Finance department.
- The employee remains responsible for ensuring that their personal data remains up to date and to notify the Company of any changes in circumstance to enable personal records to be updated accordingly.
- On a minimum annual basis, the Company's Information Asset Owners, supported by system owners and other responsible person (s), will review the retention dates of all the Personal Data processed by their respective department (s), by reference to the Company's Data Retention Schedule, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed following the Company's sanitisation procedure.
- That Personal Data is kept in a form such that the Data Subject can be identified only as long as is necessary for Processing.

The PWG must specifically approve any data retention that exceeds the retention periods defined in the Company's IG 4.0 Records Retention Schedule and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written. It remains the responsibility of Information Asset Owners, together with the system owners, or responsible person holding the Personal Data to ensure data retention records are maintained and that Personal Data procedures are adhered to.

Refer to the following documents for further information:

- IG 18 Terms of Reference (ToR) Information Asset Owner (IAO).
- SRF 1.19 Media Sanitisation Policy.

PERSONAL DATA MUST BE PROCESSED IN A MANNER THAT ENSURES APPROPRIATE SECURITY MEASURES FOR THE PROTECTION OF THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT

The responsible person shall ensure that a risk assessment is completed, considering category of Personal Data and the circumstances of the processing operations. In determining appropriateness, the responsible person shall also consider the extent of possible damage or loss that might be caused to individuals (e.g. employees or customer Personal Data) if a security breach occurs, the effect of any

security breach on the Data Subject, and any likely reputational damage including the possible loss of customer trust.

The Company' apply a defence in depth approach to security which ensures that our technical controls are proportionate to the risk. These include (the list is not exhaustive):

Technical Measures

- SRF 1.9 Password Policy, which includes the applicable technical measures the Company deploy, such as automatic locking of idle workstations and termination of remote sessions.
- SRF 1.2 Access Control Policy, which includes the application of technical controls, access permissions and removal of access rights, onboarding, internal transfer and offboarding procedure, the management of USB and other memory media.
- SRF 1.19 Media Sanitisation Policy, which informs our employees and/or third-party organisations on the technical measures to securely dispose of Information Communications Technology (ICT) and storage media containing Personal Data.
- SRF 1.26 Configuration Management Plan, which provide the set of baseline technical control measures for secure configuration of the Company's hardware, connected network devices, file and folder locations, firmware and software controls for virus-checking and firewalls.
- SRF 1.10 Encryption Standard (this is a restricted document), which results in the application of encryption standards for the Company's ICT and storage devices containing Personal Data.
- The deployment of privacy-enhancing technologies such as pseudonymisation, anonymisation and applicable security tools to monitor for Personal Data breaches.
- The provision of a secure file transfer platform, including information security agreements, for exchanging Personal Data with external organisations and/or people.

Organisational Measures

- The SLT has established a subcommittee, namely the PWG for all privacy matters. The PWG conducts governance, risk and compliance activities, which help to ensure the Company is fulfilling its data protection obligations. The PWG Terms of Reference (ToR) can be found in the document IG 16 ToR SSC.
- Implementation towards achieving industry best practice frameworks such as ISO27001 Information Security Management System, which includes both internal and external audit regime.
- Education & Awareness Training for our employees, including bespoke GDPR training where applicable.
- Security Breach Management processes that are aligned with the Company's Human Resources disciplinary process.
- Data protection clauses in our employment contracts and Data Sharing Agreements.
- Data Protection policies, processes, and procedures.
- Supply chain security diligence measures. Refer to document SRF 1.8 Supply Chain Security Policy.

ACCOUNTABILITY

The Company demonstrates compliance with the GDPR's principles by promoting accountability and governance. This is achieved by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures as above, and adopting techniques such as data protection and security by design, DPIAs, breach notification procedures and incident response plans. These points are all covered in our policies and procedure documents – refer to the list of these documents below.

VERSION CONTROL

Version No	Date	Classification	Owner	Approver
Ver 1.3	03/0692024	Private	DPO	MD