Exhibit C-3

Description of the Technical and Organizational Security Measures implemented by the Data Importer

"Technical and organizational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. SNI will maintain appropriate physical, administrative, technical, and organizational measures and safeguards for protection of the security, confidentiality, and integrity of the Data Exporter's Personal Information. More information on SNI's technical and organizational measures can be found in the Privacy Policy and the Data Processing Agreement. SNI will not materially decrease the overall security of the Services.

The following includes the information required by Annex II of the EU SCCs and Appendix 2 of the UK SCCs.

Technical and Organizational Security Measure	**Details**
Measures of pseudonymization and encryption of Personal Information	The transmission of Personal Information to and from the Data Processor's network is completed with the help of commonly accepted security and encryption technologies.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	The Data Processor takes – amongst other things – the following measures to guarantee that Personal Information is protected against damage by accident or loss: • Personal data is protected from accidental destruction or loss through effective retrieval systems, disaster recovery and business continuity planning. The procedures laid down for making backup copies and for recovering data ensure that they can be reconstructed in the state they were at the time they were last backed up.
Measures for ensuring the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident	The security policy contains a precise description of the steps to be taken when a security incident relating to Personal Information is detected, as well as of the persons in charge of dealing with the incident, in order to return to the normal situation as quickly as possible. The procedure for reporting and managing security incidents includes a record of each incident, the time at which it occurred, the person reporting it, to whom it was reported and the effects thereof. The circumstances of any incident are to be analyzed in order to elaborate preventive measures or make adaptations so as to avoid a repetition of this type of incident.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	A reassessment of the technical and organizational measures is performed on a regular basis in order to ensure that the initial goals and the measures taken remain up to date so that improvements can be made if necessary. In case of reorganization or modification of infrastructure, security controls are updated. The security policy will be adapted where necessary as a result of modifications or reassessment.

Technical and Organizational Security Measure	Details
Measures for user identification and authorization	The Data Processor ensures (i) that authorized users who have access to the data processing systems can only access Personal Information within their processing authorization and (ii) that the unauthorized reading, copying, changing or deletion of Personal Information is excluded during use or Processing or after the storing of Personal Information. The granting of access rights is based on the job responsibilities of the user and on a need-to-know basis and has to be authorized and granted by the corresponding supervisor of the person who makes an application for it. The authorizations are made by workflow tools. The access to productive systems is only granted to users who are periodically trained and authorized for the corresponding action. The access to productive systems is also immediately withdrawn in case of a termination of the contract of employment or in case of an assignment of a different task.
Measures for the protection of data during transmission	The Data Processor takes – amongst other things – the following measures to guarantee that Personal Information is not read, copied, altered or removed during the process of electronic transmission, or during the transport or storage of data on data carriers. • The remote access to data on the Data Processor's production machines depends on a connection to the company's network which is regulated via a double authentication. • The transmission of Personal Information to and from the Data Processor's network is completed with the help of commonly accepted security and encryption technologies. • The data processing systems are protected against the risk of intrusion with the help of suitable software and hardware whose effectiveness and updating is checked periodically. The routers are appropriately configured to secure the Data Processor's internal network from unauthorized external connections and to ensure that computer connections and data flow do not breach the logical access adjustment control of the Data Processor systems. Amendments on the hardware-based network components or on their configurations need the acceptance of the designated person in charge and are subject to a change management process.
Measures for the protection of data during storage	The Data Processor takes – amongst other things – the following measures to avoid the use by unauthorized persons of equipment by which Personal Information is processed: • Secured access connections and technologies for authentication control are implemented to regulate the access to the Data Processor's systems and internal support tools. • Techniques for encryption are used to secure user authentications. The Data Processor follows a formal process to permit the access to the Data Processor's resources or to deny such access. Unique login names, strong passwords and periodic examinations of the access lists exist to guarantee the appropriate use of user accounts. All groups which have

Technical and Organizational Security Measure	Details
	access to the Data Processor's services are controlled by a regular examination. All named measures are described in a formalized concept of authorization. The Data Processor takes – amongst other things – the following measures to guarantee that Personal Information is not read, copied, altered or removed during the process of electronic transmission, or during the transport or storage of data on data carriers. • The remote access to data on the Data Processor's production machines depends on a connection to the company's network which is regulated via a double authentication. • The transmission of Personal Information to and from the Data Processor's network is completed with the help of commonly accepted security and encryption technologies. • The data processing systems are protected against the risk of intrusion with the help of suitable software and hardware whose effectiveness and updating is checked periodically. The routers are appropriately configured to secure the Data Processor's internal network from unauthorized external connections and to ensure that computer connections and data flow do not breach the logical access adjustment control of the Data Processor systems. Amendments on the hardware-based network components or on their configurations need the acceptance of the designated person in charge and are subject to a change management process.
Measures for ensuring physical security of locations at which Personal Information are processed	The Data Processor takes – amongst other things – the following measures to avoid the access of unauthorized persons to the carriers of Personal Information and computer systems by which the Personal Information is processed or used: • By formal/technical access procedures, the access to the involved data processing centers is regulated. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
Measures for ensuring events logging	The data processor maintains logging systems at the application and infrastructure level.
Measures for ensuring system configuration, including default configuration	The Data Processor's processes are audited under the SOC 2 Type 2 standard

Technical and Organizational Security Measure	Details
	The Data Processor undertakes – amongst other things – the following measures to separate the Processing of collected data for different purposes: • Each data Processing is made on database systems which are separated by a system of logical and physical access controls in the network. • The Personal Information Processing is only made for the purpose as further specified in the Agreement.
Measures for internal IT and IT security governance and management	The Data Processor has drawn up a written policy in relation to data security, giving a precise description of the security strategies and protection features selected for data security. The Security Policy takes into account the real risks the Personal Information are exposed to. It includes a description of how to manage security incidents, a description of the awareness-raising process for the policy within the organization and a description of the various responsibilities and organizational rules. It also specifies the measures foreseen for keeping the security system up to date after installation. The security policy has been approved by the relevant persons in charge and has been adequately disseminated within the organization. A reassessment of the technical and organizational measures is performed on a regular basis in order to ensure that the initial goals and the measures taken remain up to date so that improvements can be made if necessary. In case of reorganization or modification of infrastructure, security controls are updated. The security policy will be adapted where necessary as a result of modifications or reassessment. The Data Processor has appointed a security counsellor, who is in charge of the implementation of the security policy. The security counsellor possesses the necessary competencies, is adequately trained and will not be able to discharge any function or take up any responsibility that is incompatible with that of a security counsellor. The Data Processor has made available sufficient and adequate organizational, technical and financial resources to organize security. Information classification procedures have been elaborated. Whenever necessary, an inventory can be drawn up and all Personal Information being processed can be localized, irrespective of the type of data carrier. Guidelines on Personal Information protection have been elaborated and disseminated within the organization in order to ensure that all employees participating in the Processing of Personal Information are sufficiently informed about their duties and responsibilities during Processing operations.

Technical and Organizational Security Measure	Details
	The Data Processor has completed centralized documentation relating to security, which is complete and formalized, proportional to security needs, up to date at any time and accompanied by a directory at the disposal of properly authorized persons whenever necessary. Such documentation should at least contain the following elements: the identity of the security counsellor, the security policy, the implementation of security measures, an inventory of the personal data being processed, their localization and the operations performed on them, a nominative list of the bodies or appointees having access to the data, the system and network configuration, technical documentation about the security controls that were introduced, a schedule of planned operations, the detection policy, security control test plans, incident reports, and audit reports, if any. The Data Processor takes – amongst other things – the following measures to guarantee that the Processing of Personal Information is made in correspondence with the instructions: • The functions and obligations of every individual with access to the Personal Information are clearly defined, updated and documented. Measures are adopted to make staff familiar and periodically trained with respect to the specific rules applicable to their functions and the consequences of any breach of these rules.
Measures for certification/assurance of processes and products	The data processor's processes are audited under the SOC 2 Type 2 standard.
Measures for ensuring data minimization	The data processor operates all systems under the principle of least privilege which extends into data transfer.
Measures for ensuring data quality	Multiple data reconciliation processes are in place.
Measures for ensuring limited data retention	The data processor has automated data deletion processes backed by periodic audits.
Measures for ensuring accountability	The Data Processor takes – amongst other things – the following measures to guarantee that it can be examined and determined subsequently if and by whom Personal Information have been entered into data processing systems, altered, or removed: • Effective input control is applied to ensure that Personal Information cannot be read, copied, modified or re-modified without authorization in the course of Processing or use and after storage. All access requests are logged, and their compliance is monitored. Because detection data are also personal data, any operation performed on these data is submitted to adequate security measures.

Technical and Organizational Security Measure	Details
Measures for allowing data portability and ensuring erasure	The data controller may export their data at any time in the application using industry standard formats. Erasure is done via automated processes following the retention period.
Technical and organizational measures of Sub-Processors	Data sub-processors must pass a secure procurement process.