PCS GROUP

TECHNICAL AND OPERATIONAL SECURITY MEASURES

Security measure	**Details**
Measures of pseudonymisation and encryption of personal data	• Data is encrypted whilst in transit. • Data is pseudonymised wherever practicable when recorded on internal systems or shared with third parties.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services, and for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures	• We conduct regular IT security reviews to ensure best practices are adopted. • Contracts with third parties requiring robust security mechanisms when processing personal data.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	• Regular back-ups made of personal data. • Mirroring of hard disks. • Uninterrupted power supply. • Firewalls. • Regularly updated disaster recovery plan.
Measures for user identification and authorisation to prevent unauthorised users from accessing data	• We adopt two-factor authentication where appropriate. • Password protection of documents containing sensitive personal data. • Automatic lockout for inaccurate passwords. • Access rights dependent on the necessity of accessing the data based on roles.
Measures for the protection of data during transmission	• We undertake penetration tests to check that data in transit is fully protected. • We ensure safeguards are in place for any international transfers of personal data to our subprocessors and other relevant parties, usually using the EU Standard Contractual Clauses with the UK Addendum.
Measures for the protection of data during storage	• We encrypt data at rest to ensure data is not written to storage in unencrypted form. • We adopt password protection and controls on user access where appropriate.
Measures for ensuring physical security of facilities at which personal data are processed	• Entry to our building is protected by physical and digital security measures including smart cards and surveillance systems. • Our servers and communications hardware are located in a secure server room. • We ensure products containing personal data are securely managed with inbound collection and reception of equipment into PCS owned and operated facilities, ensuring chain of custody.
Measures for ensuring events logging	• Our systems permit us to see an audit trail of changes to documents by personnel.
Measures for ensuring system configuration, including default	• Any new systems our assessed by our IT security team prior to implementation.

Security measure	**Details**
configuration	
Measures for internal IT and IT security governance and management	• We maintain our IT security and review our practices periodically to ensure the measures are appropriate for the size of our organisation and the type of personal data we handle.
Measures for certification/assurance of processes and products	• We seek advice from external legal counsel to ensure we are aware of our obligations under the data protection legislation. • We hold ISO certification for Quality Management Systems & Processes (ISO-9001-2015) and Environmental Management Systems & Processes (ISO-14001-2015).
Measures for ensuring data minimisation Measures for ensuring data quality	• We only collect the data needed to provide our services. • We have strict policies requiring customers using our trade-in offering to delete all personal data from devices before sharing them with us. In the event of user error, we utilise Asset Science (see below) to remove remaining data.
Measures for ensuring limited data retention	• We use a data clearing method from Asset Science, which has been ADISA certified to remove data from trade-in devices. • We adhere to an internal data retention policy reviewed by external legal counsel.
Measures for ensuring accountability	• Data that is collected for different purposes is processed separately. • We maintain separation between our business units and group entities where appropriate. • We have a robust Intra-Group Data Sharing agreement that sets out responsibilities and requirements for processing data.
Measures for allowing data portability and ensuring erasure	• We require all employees to adhere to a robust Data Protection Policy, which includes set procedures to follow in the event a data subject exercises their rights to erasure, access, portability or any other rights. • We hold up to date Article 30 Records of Processing activities that record how data is held within our business.