

GDPR Compliance and Data Security

The General Data Protection Regulation (“GDPR”) takes effect on 25 May 2018. According to its opening chapter, the GDPR’s primary objective is to protect people’s fundamental rights in the security and privacy of their personal data while also ensuring the free movement of personal data within the European Union. The GDPR represents a long-awaited replacement of the old regulatory regime under the European Privacy Directive.

StorageCraft’s business provides innovative tools that help our partners and customers protect, store, safeguard, and understand their data. We therefore embrace and welcome GDPR. StorageCraft is built on the trust and confidence that our end-user customers, partners, and employees place in us. This trust is based on our long-standing record of delivering reliable and superior products and services. To meet this expectation today and in the future, the application of industry-leading data security policies and practices has been, and will continue to be, an integral part of our business conduct.

StorageCraft is committed to processing data in compliance with applicable GDPR principles, including: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. StorageCraft has already implemented wide-ranging data protection and security measures, and is again reviewing these in the context of the GDPR’s upcoming implementation. We continue to maintain internal records of all data-processing activities, and we are implementing processes to accommodate the rights of data subjects. We continue to review and update our internal data processes and systems in light of any changes made by the GDPR. We will also be releasing updated agreements and processing addenda to ensure full compliance with the GDPR prior to the time it goes into effect.

Security Practices and Procedures

A key aspect of GDPR compliance is adopting and following responsible data security practices. To consistently meet this objective, StorageCraft has implemented an Internal Information Security Program, which forms the foundation for many of our company policies, processes, practices, and procedures. It addresses StorageCraft’s corporate security principles, as well as policies and procedures related to operational, administrative, physical, and technical security controls. The Information Security Program also assists in the management of the internal security of intellectual property and sensitive employee and channel partner data, and it provides assurances to our valued partners, customers, auditors, and regulators.

Finally, StorageCraft continuously conducts independent audits to ensure its processes are working as intended. To that end, we regularly work with independent outside firms and products to conduct long-term security audits and penetration testing of our systems, including our cloud and portals. We repeat this process using independent firms and software products to ensure data integrity and confirm that StorageCraft continues to provide solid and secure solutions for our customers.

Data Centers

StorageCraft relies on industry-leading data centers rated by the Uptime Institute (or equivalent) of Tier III or better. StorageCraft's European data centers are certified to ISO/IEC 27001 and ISO 22301 standards. StorageCraft regularly confirms with its data center providers that they have multiple technical and organizational measures in place to ensure high levels of security and compliance, including robust physical security.

Cloud Solutions

Both StorageCraft and its partners expect high availability of data. Our cloud solutions employ high-end, high-availability, redundant hardware. With StorageCraft Cloud Services, in order to ensure constant data availability and integrity, StorageCraft employs the same fully distributed storage system used by leading large enterprises, including Deutsche Telekom, Bloomberg, and the CERN Large Hadron Collider in Switzerland.

The StorageCraft Cloud has achieved a consistent 99.999 percent uptime, which we continue to improve upon. StorageCraft has redundant systems to provide internal and external performance monitoring of its cloud offerings. These include implementations of industry-leading third-party monitoring solutions, as well as StorageCraft's own proprietary monitoring system. StorageCraft also employs a dedicated, global cloud operations team that monitors StorageCraft Cloud Services uninterrupted, 24/7/365.

StorageCraft software is an integral part of our approach to security. For example, StorageCraft Cloud Services only allows fully encrypted (AES-256 by default) backup images to be uploaded to the cloud or placed on a seed drive. The cloud hardware we deploy in our data centers includes enterprise-grade redundant firewalls that immediately mitigate any intrusion. Once the data is uploaded to our cloud servers, it is stored and managed by encrypted hardware and remains inaccessible to any StorageCraft employee or any other party without the customer's credentials. In short, only the client and legitimate owner of the data can read their image data.

Contact

GDPR-related questions can be addressed to privacy@storagecraft.com.