StorageCraft®

GDPR FAQs

Q. Who and what does the GDPR protect?

A. The General Data Protection Regulation ("GDPR") is the European Union's new and comprehensive privacy and data protection law. Broadly speaking, the GDPR protects the "personal data" of individuals in the European Economic Area ("EEA"). An "individual" refers to a human being or natural person. It does not refer to an entity. StorageCraft is a B-to-B company and therefore most of the personal data we encounter will relate to either employees of our partner companies or personal data contained with backups we process through our cloud products and services.

Q. StorageCraft is headquartered in the U.S. Why does the GDPR apply to StorageCraft?

A. Although StorageCraft is headquartered in the U.S., whenever we provide our services to customers (or their affiliates) in the EEA, or provide services through our Irish subsidiary, then the GDPR will generally apply.

Q. What is "personal data"?

A. "Personal data" is any information that can be used to identify—either directly or indirectly—an individual. Examples of information or material that can be "personal data" include: name, telephone number, address, email address, date of birth, identification number (such as a driver's license number, national insurance numbers, or social security numbers), and photographs. Personal data also includes less obvious identifiers like IP addresses and online user names.

Q. Is someone's work email or work telephone number "personal data"?

A. Yes. It does not matter that this information is work-related. If the information can be used to directly or indirectly identify someone, then the information is "personal data" and will be protected by the GDPR.

Q. What is a "data processing agreement" (also known as a "data processing addendum")?

A. Under the GDPR, a "controller" is the party that determines the purpose and means of processing personal data and a "processor" is the party that processes personal data on behalf of a controller. The GDPR requires that the relationship between controller and processor be governed by a written agreement. It needs to specify certain minimum, mandatory terms, including "sufficient guarantees" that the processor has implemented "appropriate technical and organisational measures" around their processing of personal data. This agreement is commonly referred to a data processing agreement or addendum ("DPA"). A common misconception is that simply because personal data is transferred from one party to another, a DPA is required. That is not the case. A DPA is only required when a controller transfers personal data to a processor for the purpose of the processor "processing" personal data for and on behalf of the controller. Stated inversely, if Party A is not transferring or providing access to the personal data to Party B so that Party B can process the personal data for Party A, a DPA is not required. If the recipient of the personal data is not processing the personal data for and on behalf of the transferor but is instead processing the data for its own lawful purpose—such as Party B's performance of a contract—a DPA is not required.

Q. Which StorageCraft partner relationships require a DPA?

A. The table below summarizes the common StorageCraft partner relationships, states whether a DPA is required, and provides our reasoning:

Relationship with StorageCraft	Data Processing Agreement Necessary?	Explanation
Value-Added Reseller (VAR – selling perpetual software)	No	The only personal data that StorageCraft should receive from a VAR are the names and email addresses of employees of the VAR or employees of the end user. StorageCraft is not processing such personal data for the VAR or end user. Instead, StorageCraft is a controller of that personal data and is processing the data on its own behalf for purposes of delivering its products to the VAR and the end user, fulfilling its obligations to them and general relationship management.
Managed Service Provider (MSP – selling subscription software)	No	The only personal data that StorageCraft should receive from an MSP are the names and email addresses of employees of the MSP. StorageCraft is not processing such personal data for the MSP. Instead, it is a controller of that personal data and is processing the data on its own behalf for purposes of delivering its products and services to the MSP and fulfilling its obligations with them.
Cloud Product Agreement	Yes	A cloud customer transfers backups to StorageCraft for processing on behalf of the cloud customer. Because StorageCraft does not have knowledge of the types of data in the backups, StorageCraft assumes that backups contain personal data. In delivering its cloud products and services, StorageCraft is a processor (and/or in some cases a sub-processor if its cloud customer is itself using StorageCraft's cloud services to backup data that it processes as a processor on behalf of another controller), processing data on behalf of its cloud customer, and therefore a DPA is necessary.
Distribution Agreement	No	A distributor may transfer personal data to StorageCraft associated with companies in the chain of sale, such as its reseller or the end user. This personal data is typically comprised of the names and email addresses of people employed by the distributor, reseller, or end user. StorageCraft is not processing such personal data for the distributor or other parties in the chain of sale. Instead, StorageCraft is a controller of that personal data and is processing the data on its own behalf for purposes of delivering its products to the VAR or the end user, fulfilling its obligations to them, and general relationship management.

Q. Does StorageCraft have a data protection officer?

A. No. A common misconception about the GDPR is that it requires all companies to appoint a data protection officer. That is not the case. The GDPR requires the appointment of a data protection officer only in three very limited circumstances: (a) the processing is done by a "public authority or body"; (b) the "core activities" of the controller or processor involve regular, systematic, and large-scale monitoring of data subjects; and/or (c) the "core activities" of controller or processor consist of large-scale processing of highly sensitive personal data. These circumstances do not apply to StorageCraft. While StorageCraft is not required to appoint a data protection officer, we take data protection very seriously. Data protection compliance is overseen by our legal and information technology departments.

Q. What are the technical and organizational security measures adopted by StorageCraft in association with its processing of personal data?

A. While StorageCraft cannot disclose all of its security processes and procedures, StorageCraft is committed to safeguarding personal data in accordance with the GDPR. A summary of StorageCraft's technical and organizational security measures is included within an addendum to StorageCraft's DPAs (where required). A copy of these measures is available upon request.

Q. What are "standard contractual clauses" and are the clauses used by StorageCraft GDPR compliant?

A. As a starting point, the GDPR prohibits any transfers of personal data outside of the EEA unless the personal data is appropriately safeguarded. The "standard contractual clauses" (also sometimes referred to as the "model clauses") are one of the methods approved by the European Commission by which personal data may be lawfully transferred outside of the EEA under appropriate safeguards. The standard contractual clauses are so standard that, in order for them to be relied upon, they must be copied verbatim from the 2010 decision by the European Commission that promulgated them. The standard contractual clauses used by StorageCraft form part of its DPA and comply with the requirements of applicable data privacy law, including the GDPR.

Q. Who are the sub-processors used by StorageCraft?

A. A list of StorageCraft's sub-processors is provided on StorageCraft's website.

Q. If a value-added reseller purchases StorageCraft products through a distributor, does it need its end user's consent to provide the distributor with personal data about employees of the end user, such as the name and email address of a contact person employed by the end user?

A. Our partners need to perform their own analysis concerning the effect of the GDPR on their business practices, including their own obligations as data controllers. We recommend that particular attention be paid to Article 6 of the GDPR, which identifies the various lawful bases for processing personal data, as well as Articles 13 and 14, which identify a controller's obligations to inform a data subject about the use of their data, which is typically accomplished through a clear and accessible privacy policy. People often assume that "consent" is required when all a controller may need to do is clearly communicate with the data subject about the use and processing of their personal data. And under Article 6, consent is only one basis on which personal data may be processed. A controller may, but need not, rely on consent when another basis for processing exists. The basis for processing should be carefully evaluated as it affects the controller's obligations under other provisions of the GDPR, such as an erasure request by the data subject.

Q. How will Brexit affect my data with StorageCraft Cloud Products?

A. Given that the UK's Brexit negotiations with the European Union are underway, the effects of Brexit are somewhat uncertain, including its impact on data protection. While no definitive pronouncements can be made today concerning post-Brexit U.K. data protection law, we believe that most indicators suggest that little will change.

The GDPR took effect in May 2018 and is currently the law of the land in the U.K. The government, concerned about negatively affecting businesses and the citizenry through excessive uncertainty, has signaled that much of existing European law will likely continue to apply in the U.K. post-Brexit. Whether a truly "soft Brexit" occurs remains to be seen, but U.K. data protection authorities have recently emphasized their continued commitment to GDPR. Indeed, in an April 2018 speech by the U.K. Information Commissioner, she stated that she continues to advise the government and parliament on "law reform that ensures high standards of data protection for U.K. citizens and consumers, wherever their data resides, uninterrupted data flows to Europe and the rest of the world; and legal certainty for business." She also emphasized that data protection is a "priority area" for the Brexit settlement, and that the Information Commissioner's Office ("ICO") continues to play a full role in creating guidance for the GDPR and engaging with the European Data Protection Board or "EDPB" (formerly the Article 29 Working Party). She also noted that Prime Minister May has recently argued for an ongoing role for the ICO in the form of a seat on the European Data Protection Board with voting rights or some similarly substantive relationship.

After Brexit, businesses selling products and services into the U.K. will need to comply with both the GDPR and the U.K. version of the GDPR. We expect substantial—if not virtually universal—overlap between the two pieces of legislation. Since the GDPR is already the law in the U.K., even if Brexit ultimately transpires on the "harder" end of the hard-to-soft-Brexit spectrum, we expect that the U.K. will be an adequate country to receive data from the EEA and vice versa.

As a result, we see no need to move data from StorageCraft's Dublin or Frankfurt data centers or otherwise change product policies at this time. That said, StorageCraft is mindful of the need to ensure compliance with the GDPR and post-Brexit U.K. data-protection law. As Brexit approaches, we will be watching to see what effect, if any, it may have on our award-winning products and services. We will keep you posted.

Q. How does the "right of erasure" affect data contained in backups?

A. One of the rights given to data subjects is the right of erasure, also referred to as the "right to be forgotten." Under certain circumstances, this permits a data subject to instruct a controller to erase the data subject's personal data.

As with all legislation, there are issues that are not specifically addressed by the GDPR. These issues include the interplay between the right of erasure and computer backups. With a computer backup, it may be impossible to isolate a single data subject's personal data, delete it, and maintain the integrity of the backup. And even in circumstances where this is possible, the costs associated with such an effort may be entirely impracticable. This issue needs either legislative clarification or guidance from the EDPB, particularly given that the GDPR itself states that the ability to restore personal data from a computer backup is one of the "appropriate technical and organizational measures" that should be implemented to ensure data security. (See Art. 32(1)c.)

While there is presently no clear answer, the ICO in the U.K. is one of the few national data protection authorities to have addressed the issue. Prior to the GDPR, the ICO published guidance entitled "Deleting personal data." This guidance acknowledged the difficulty presented by an erasure request when one holds archived or backup data. The guidance states that "the ICO will adopt a realistic approach in terms of recognising that deleting information from a system is not always a straightforward matter and that it is possible to put information 'beyond use', and for data protection compliance issues to be 'suspended' provided certain safeguards are in place." For the ICO, personal data subject to an erasure request is put "beyond use," if not actually deleted, if the controller:

- Cannot or will not use the data in a way that affects the data subject;
- Does not give any other organisation access to the data;
- Applies "appropriate technical and organisational security" to the data; and
- Commits to delete the data if or when deletion becomes possible.

The ICO has continued to cite this pre-GDPR guidance, stating that it will be updated in "due course." Post-GDPR, the ICO has continued to rely on this guidance, emphasizing that, when it comes to deleting data contained in computer backups, placing the data "beyond use" in the manner described above is an acceptable approach in responding to an erasure request involving backup data. The ICO adds that a controller "must be absolutely clear with individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems." StorageCraft recommends that the data subject be informed that his or her personal data contained in the backup has not been deleted, but that the personal data has been placed "beyond use" through application of the foregoing conditions. Until the GDPR is clarified, either legislatively or through guidance from the EDPB, StorageCraft believes that the foregoing is the best solution to the quandary.

Q. Where can I learn more about StorageCraft's approach to data privacy?

A. Shortly following the GDPR's effective date, StorageCraft released an updated privacy policy, which can be found on StorageCraft's website. It is the starting point for any inquiry about the personal data StorageCraft collects and what we do with it. For additional questions on privacy-related questions and concerns please contact us at privacy@storagecraft.com.

THIS FAQ IS PREPARED BY STORAGECRAFT TECHNOLOGY AND IS AN EXPRESSION OF THE COMPANY'S OPINIONS ON THE MATTERS DISCUSSED. IT DOES NOT CONSTITUTE LEGAL ADVICE. PLEASE SEEK YOUR OWN LEGAL COUNSEL CONCERNING THE ISSUES RAISED HEREIN.

StorageCraft