GDPR requirements

Data controller vs data processor

GDPR requirements related to usage of the Commvault Cloud Offering.
DISCLAIMER
The list is by no means exhaustive nor it is intended as legal advice. It is provided without any warranty, express or implied, including as to their legal effect and completeness.

GDPR differentiates between requirements imposed on Data Controllers and Data Processors. It is important to understand the shared responsibility model introduced by GDPR and obligations imposed on parties involved in the data processing.

In the primary scenario—where you back up your data using Commvault® services—you act as a Data Controller and Commvault acts as a Data Processor.

Commvault services may support you in complying with certain requirements applicable to data controllers set forth by GDPR. The information provided below lists selected requirements of utmost relevance to any Commvault® Cloud customer.

On the other hand, Commvault acts as a Data Processor and consequentially needs to comply with data processor-specific requirements. To find out on how Commvault complies with GDPR in our role as Data Processor, refer to the following documents:

- Privacy notice
- Data Processing Addendum
- Our GDPR compliance webpage

GDPR REQUIREMENTS

Below you will find a list of requirements imposed by GDPR that are relevant from the perspective of Commvault Cloud users. For every requirement we provide a high-level description of how Commvault Cloud is able to support your GDPR compliance efforts.

Source	Requirement	How Commvault addresses/may help you address the requirement
Art. 24(1) of the GDPR—general responsibility of the Data Controller	Data controller remains responsible for implementing appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR, taking into account: • the nature, • scope, • context, and • purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.	Commvault is the Data Processor for the services it offers. Commvault services include functionalities that enable the Data Controller to remain compliant with relevant GDPR provisions. Amongst various configuration options, Commvault gives the Data Controller full control over what data is sent to Commvault Cloud for backup (data source), backup frequency, and retention periods.

Source	Requirement	How Commvault addresses/may help you address the requirement
Art. 5(1)(a) of the GDPR—lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly, and in a transparent manner concerning the data subject.	Commvault built-in security measures such as data encryption "in flight" and "at rest", RBAC controls are applied so only the users with appropriate permissions can access data—are allowing full manageability and granular control of your data, and most importantly, of how it is used. This way you can make sure that you remain aligned with all the applicable data processing principles defined by data protection laws.
Art. 5(1)(b) of the GDPR—purpose limitation	Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	Commvault can process personal data only on documented instructions from the Data Controller. Most importantly, the built-in encryption will not allow Commvault Cloud to gain access to any of your data unless you expressly decide to grant it (e.g., in customer support operations). Even in such cases, we have introduced measures that mitigate the potential risks connected with any potential further processing. For detailed instructions on: Built-in security measures applicable to purpose limitation, please refer to Commvault Cloud Documentation; How Commvault processes data as Processor, please refer to the Data Processing Addendum on commvault.com In certain scenarios (when Commvault acts as a Data Controller) connected with the marketing and sale of our services, we collect personal data based on consent and applicable opt-in rules (e.g., during sign-on and procurement). The marketing leads data is only used for contacting the customer for the exclusive business of Commvault Cloud solutions. For additional details on Commvault's privacy practices, please refer to the Commvault Privacy Policy Notice.

Source	Requirement	How Commvault addresses/may help you address the requirement
Art. 5(1)(c) of the GDPR—data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	As a Data Processor Commvault does not use personal data of customer. The Data is processed at the request of the Controller for the sole purpose of backup and eDiscovery. Role Based Access Controls provide Controller with options to control who can access the data. Marketing and Sales Customer contact information is used only for the purposes of providing information about the Commvault Cloud solution, ongoing customer engagement and support. For additional details on Commvault's privacy practices please refer to Commvault Privacy Policy Notice.
Art. 5(1)(d) of the GDPR—accuracy	Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.	Commvault—when acting as the Data Processor—does not validate the contents and accuracy of the personal data.
Art. 5(1)(e) of the GDPR—storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.	As Data Processor the Controller sets the retention period for all data processed by Commvault Cloud. It is at the discretion of the Customer/Controller to keep the data for as long as they need. Commvault will delete the data once the retention period expires. When Commvault acts as the Data Controller for Marketing and Sales leads, Commvault will keep customer sales contact info in accordance with Commvault Privacy Policy Notice.

Source	Requirement	How Commvault addresses/may help you address the requirement
Art. 5(1)(f) of the GDPR—data security (integrity and confidentiality)	Any personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical, or organisational measures.	Under GDPR the controller and the processor "shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". Commvault products include a plethora of state of the art, built-in security measures including amongst other encryption" in flight" and "at rest", authentication using third-party identity providers, virtual air-gaps, Role Based Access Controls, etc. For details, please refer to Commvault Cloud Documentation. Properly configured and deployed Commvault Cloud services are an extremely effective mitigation measure against many risks affecting your data (e.g., ransomware attacks). As a Data Processor, Commvault is ISO and SOC 2 Type 2 certified with organisational and technical controls in place as listed in Annex 2 on Technical and Organizational Measures of Data Processing Addendum.
Art. 9 of the GDPR—processing special categories of personal data	General prohibition and exceptions for processing 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.	Commvault is a Data Processor and does not control the data being processed. Due to nature of backup services and encryption involved, the exact categories of data subjects cannot be conclusively established by the Data Processor and may vary depending on the exact use case of the Services.
Art. 10 of the GDPR—processing personal data related to criminal convictions and offences	General prohibition and exceptions for processing data related to criminal convictions and offences.	Commvault is a Data Processor and does not control the data being processed and has no ability to discriminate based on the whether the data is related to criminal convictions or offences. Due to nature of backup services and encryption involved the exact categories of data subjects cannot be conclusively established and may vary depending on the exact use case of the Services.

Source	Requirement	How Commvault addresses/may help you address the requirement
Art. 15 of the GDPR	Right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.	Commvault acts as a Data Processor and does not control the data being processed. However eDiscovery (Compliance Search) function available with selected Commvault Cloud services enables Data Controller to search for information in structured or unstructured data and may prove an effective tool when dealing with all kinds of request from data subjects. For availability, please refer to Product Documentation.
Art. 16 of the GDPR—right to rectification	Right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.	As above.
Art. 17 of the GDPR—Right to erasure ('right to be forgotten')	Right to obtain from the controller the erasure of personal data concerning him or her without undue delay.	As above.
Art. 18 of the GDPR—restriction of processing	Right to obtain from the controller restriction of processing.	As above.
Art. 20 of the GDPR—right of data portability	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.	As above.
Art. 25(1) of the GDPR—Data Protection by design	Taking into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical, and organisational measures, such as pseudonymisation, data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.	Previously mentioned technical and organizational measures built into Commvault Cloud (e.g. encryption) are designed to implement data protection principles defined by GDPR in an effective manner and to protect the rights and freedoms of data subjects.

Source	Requirement	How Commvault addresses/may help you address the requirement
Art. 25(2) of the GDPR—Data protection by default	The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	"Data protection by default" refers to the choices made by a Data Controller regarding any preexisting configuration value or processing option that has the effect of adjusting, in particular but not limited to, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. For configuration options, supported platforms and applications please refer to Product Documentation.
Art. 28 of the GDPR—Processor	The Data Controller shall use only Data Processor providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject. Processing by a processor shall be governed by a contract.	For information on how Commvault complies with this specific article—please refer to Data Processing Addendum.
Art. 30(1) and (2) of the GDPR—Records of processing activities	Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller.	Commvault maintains a record of processing activities where it acts as a Data Processor containing information required by referenced article.
Art. 32 of the GDPR—Data security	Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.	Please refer to the responses provided to Art. 5(1)(f) of the GDPR on data security (integrity and confidentiality).

Source	Requirement	How Commvault addresses/may help you address the requirement
Art. 33 of the GDPR—Data Breach notifications	In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.	Commvault will report any data breach within time-lines defined in the Data Processing Addendum.
Art. 35 of the GDPR—Data Protection Impact Assessment	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.	Upon customer's request, Commvault will assist Data Controller and provide information required to perform Data Protection Impact Assessment taking into account information available to Commvault.
Art. 38 of the GDPR	The Data Controller and the Data Processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.	Commvault appointed Global Data Governance Officer (gdgo@commvault.com).
Art. 46 of the GDPR—cross border data transfers	Any cross border data transfers may take place only if the Data Controller or Data Processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	Commvault has global data centers supporting every major region, letting our customers localize and choose where their data is backed up. For SaaS applications that are collecting and processing personal data, we recommend having data processed and stored in the same region where it's collected. In limited scenarios (such as customer support, troubleshooting), Commvault is relying on Standard Contractual Clauses which form part of our Data Processing Addendum as the mechanism enabling cross border data transfers.